KLUWER LAW INTERNATIONAL

INFORMATION LAW SERIES

DATA PROTECTION LAW

Approaching Its Rationale, Logic and Limits

Lee A. Bygrave

Wolters Kluwer
Law & Business

INFORMATION LAW SERIES – 10

DATA PROTECTION LAW

Approaching Its Rationale, Logic and Limits

International Board of Editors

EDITOR-IN-CHIEF

Prof P. Bernt Hugenholtz
Institute for Information Law
University of Amsterdam
The Netherlands

MEMBERS

Prof. Eric Barendt
University College London
England

Prof. Martin Bullinger
Albert-Ludwigs-Universität Freiburg
Germany

Dr Herbert Burkert
Institut für Medien und Kommunikationsmanagement
University of St. Gallen
Switzerland

Prof. Egbert J. Dommering
Institute for Information Law
University of Amsterdam
The Netherlands

Prof. Michael Lehmann
Max-Planck Institute for Foreign and International Patent, Copyright and Competition Law
University of Munich
Germany

Prof. André Lucas
Université de Nantes
France

Prof. Ejan Mackaay
Centre de recherche en droit public
Université de Montréal
Canada

Prof. Eli M. Noam
Columbia Institute for Tele-Information
Columbia University, New York
USA

The titles in this series are listed at the back of this volume.

INFORMATION LAW SERIES – 10

DATA PROTECTION LAW

Approaching Its Rationale, Logic and Limits

Lee A. Bygrave
B.A.(Hons.), LL.B.(Hons.), LL.D. / Dr. juris
Barrister of the Supreme Court of New South Wales

2002
KLUWER LAW INTERNATIONAL
The Hague • London • New York

Published by
Kluwer Law International,
P.O. Box 85889, 2508 CN The Hague, The Netherlands
sales@kli.wkap.nl
http://www.kluwerlaw.com

Sold and distributed in North, Central and South America by
Kluwer Law International,
101 Philip Drive, Norwell, MA 02061, USA
kluwerlaw@wkap.com

In all other countries, sold and distributed by
Kluwer Law International,
Distribution Centre, P.O. Box 322, 3300 AH Dordrecht, The Netherlands

DISCLAIMER: The material in this volume is in the nature of general comment only. It is not offered as advice on any particular matter and should not be taken as such. The editor and contributing authors expressly disclaim all liability to any person with regards to anything done or omitted to be done, and with respect to the consequences of anything done or omitted to be done wholly or partly in reliance upon the whole or any part of this volume without first obtaining professional advice regarding the particular facts and circumstances at issue. Any and all opinions expressed herein are those of the particular author and are not necessarily those of the editor or publisher of this volume.

A C.I.P. Catalogue record for this book is available from the Library of Congress.

Printed on acid-free paper

web-ISBN 978-90-411-8066-7
© 2002 Kluwer Law International

Kluwer Law International incorporates the imprint Martinus Nijhoff Publishers.

This publication is protected by international copyright law:
All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording, or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

Printed and bound in Great Britain by Antony Rowe Limited.

Table of Contents

PART III: DATA PROTECTION RIGHTS FOR PRIVATE COLLECTIVE ENTITIES

Foreword

The Hon Justice Michael Kirby AC CMG

When a completely new problem comes along, the legal mind is often paralysed for a time. Attempts are made to squeeze the problem into old familiar bottles. And when this does not work, attempts are made to create new receptacles by analogy with those that seem most suitable.

So it is with many of the contemporary problems presented to the law by genomics and the other astonishing developments of biotechnology. Just look at the puzzles that are emerging in the field of intellectual property law as it attempts to respond to the flood of applications for patents with respect to genetic sequences. Not only is the legal mind resistant to the idea of new approaches to new problems. The institutions of lawmaking are often highly inflexible. Typically, the emerging issues are complex, beyond the easy comprehension of the elected lay people who sit in the legislatures and even the overworked officials who advise them. Sometimes powerful forces of national interests or the interests of transnational corporations see advantage in delaying an effective legal response to a demonstrated problem. If nothing is done, or if any legal response is left to 'soft options', the strong and the powerful can continue to do what they want. Responses reflecting community values will then play second fiddle to the tune of unregulated power.

In recent years, I have become involved in these themes as they have been played out in the controversies that have followed the mapping of the human genome. But I was well prepared for the current debates. In 1978 I chaired the Expert Group of the Organisation for Economic Cooperation and Development (OECD) that drafted the guidelines of that organisation concerning privacy protection. Genomics would not have been possible without informatics. As Dr Bygrave points out, it was the rapid advance of information technology in the 1960s and 1970s that both diminished the scope for individual privacy and enhanced the technological capacity to respond. But what would the response be? In most of the world the legal mind seemed frozen in indecision – incapable of giving answer. In many countries of the common law, the value of individual privacy was not well protected by law. What should be done to increase protection of such values whilst at the same time avoiding undue impediments upon an amazing and useful technological breakthrough?

Fortunately, the OECD group did not come to its challenge cold. Pioneering work had already occurred in a number of the legal systems of Scandinavia. This, in

turn, had produced initiatives by the Nordic Council. These, in their turn, had prompted the Council of Europe into action. The European states saw the inherent limitations on the effectiveness of national or even European regulation of the subject. Hence the attempt to engage, first, the intercontinental OECD and later the United Nations itself.

Although later events, deeper thinking and, above all, advances in the capacity of the technology have necessitated reconsideration of the OECD Guidelines, they represented, as Dr Bygrave describes, a remarkable advance for their time. There were many of the same anxieties that now attend the debates about international regulation of biotechnology. Have we truly got the measure of the problem? Will attempts at regulation be futile, given the rapid changes in the technology? Are the values of different societies sufficiently common to permit international norms to be agreed and enforced? Do the differing constitutional requirements and legal traditions of nation states permit a common approach to regulation? Will the introduction of laws in some countries merely result in the establishment of law-free enclaves elsewhere, much as the tax havens and shipping flags of convenience developed to meet earlier economic demands? Will the big players in the technology permit the rest to call the tune when they threaten to affect the fruits of an unregulated market?

Fortunately, in the matter of informatics, and at least in respect of the countries of the OECD, there was sufficient economic and political commitment to secure agreement over at least the basic rules that should be adopted. Yet there remained important differences. They were reflected, in part, in the nomenclature that was chosen. The common law countries might conceive of themselves as protecting 'privacy'. But the civil law countries generally preferred to avoid that elusive notion and to speak of 'data protection'. Data protection over what? Data protection why? Data protection how?

The OECD group could not finally resolve these last questions. It was left to member countries to fashion their own laws after their own traditions but within an intercontinental framework set by the agreed principles. Mark this strategy well. It will become the approach of the international community to many of the issues that are presented to it by the challenges to human society occasioned by new technology, presenting in its myriad forms.

Dr Bygrave has analysed the resulting network of privacy or data protection laws that have sprung up in most developed countries of the world, and in others that aspire to that status. His is not a book of rules. Nor could it pretend to state finally the detailed law and practice of every country surveyed as they respond to a technology that continues to expand and change. However, Dr Bygrave comes to his task with an experience and training that is uniquely valuable. He has personal and intellectual links to Scandinavia where the ideas of data protection were born and nurtured. He has a deep knowledge of the legal systems of Europe, where those ideas found fertile

soil and have flourished. Yet he also understands the peculiar legal traditions of the common law.

If England is now increasingly drawn to its economic and legal connections to Europe, and influenced by the civil law and administrative traditions that lie deep in that continent, this cannot be said of the Anglophone jurisdictions of North America and Oceania. They continue to share their approach to these issues with a world-wide network of common law countries. One suspects that, to this day, the different appellations 'privacy' and 'data protection' continue to inform the response of these differing traditions. It is a great merit of this book that the author bridges this sometimes significant gulf between them. I regard this as specially valuable. The technology talks across borders. The legal traditions must also learn to do so.

Dr Bygrave emphasises the need to adopt a 'systemic' approach to the issues of privacy regulation or data protection. He advances a controversial view concerning the processing of information on corporations and other collective entities of the private sector. Much of the law has hitherto been resistant to the claim that data on corporate and collective entities deserve specific protection. The extent to which that resistance is based on human rights notions that lie deep in the very concept of 'privacy' – and can perhaps be overcome only by embracing the wider idea of 'data protection' – is a puzzle that the book helps to unfold.

A further distinctive feature of this book lies in the way in which Dr Bygrave combines his theoretical analysis with his attention to numerous questions of great practical relevance. To take one example, the book contains what must be one of the most detailed and systematic analyses, at least in the English language, of what is meant by 'personal data' and 'personal information', as those terms are used in privacy and data protection law. These are highly topical explorations given the explosion of the Internet. They are concepts central to determining whether the law applies to a given situation. The fact that Dr Bygrave examines these questions with the benefit of a systematic analysis of the 1995 European Community Directive, but also of the approaches of the law in English-speaking countries, makes this a work of large legal importance.

It is interesting for one who took part, under the chandeliers of the Chateau in Paris in which the OECD Expert Group met, to witness the growth of legal regulation that has followed. And yet informatics is but one of the challenges that come to the law from the dynamic world of technology. Other technologies, such as nuclear fission and genomics are already with us. Still others, that we do not yet know and cannot even imagine, are just around the corner. Responding to them, in effective and just ways, is a mighty challenge for the law, the rule of law, democratic institutions and international cooperation, peace and security.

When asked to explain how he perceived more than others, Isaac Newton attributed his gift to thinking deeply. In new fields, presenting new challenges, that is what lawyers must do. In this book, Dr Bygrave shows us the way. He has thought

deeply and shares with us the product of his thought. And the lessons we should draw from this book will not be confined to the issues of data protection.

High Court of Australia — Michael Kirby
Canberra — 24 May 2002

Preface

This book is closely based on a thesis for which I was awarded the degree of dr juris at the University of Oslo in May 2000. The roots of the book, however, stretch back to the penultimate year of my undergraduate law degree course at the Australian National University in 1988. It was then that my interest was awoken in law dealing specifically with the processing of information on persons. Peter Bayne at the University's Faculty of Law suggested I write an Honours thesis on a then fresh piece of Australian federal legislation: the *Privacy Act 1988*. He was sure, he told me, that the intended regulation by the Act of government agencies' data-processing practices raised a large number of challenging issues, and that I would find more than enough into which I could sink my teeth. How prescient he was!

I completed my Honours thesis with a feeling that I had only nibbled on some of the issues associated with this sort of law. Much of my work since then has been devoted to gnawing more thoroughly at more of these issues. Yet even now, after completing a doctoral research project on them, questions remain which I have scarcely touched. The number of such questions is unlikely to decrease in the near future. Technological developments coupled with socio-economic, political, legal and moral imperatives will continually throw up new dilemmas for law and policy on the processing of information on persons. This is what makes this field of research so complex and at the same time so stimulating.

It is also a field of research where I have had the fortune to meet a great many genial individuals without whose help the quality of my thinking (and much of my life) would be a great deal poorer. In this connection, I especially thank Erik Boe at the Institute for Public and International Law at the Law Faculty of Oslo University. Erik was chiefly responsible for supervising my doctoral research. He is a man of generous spirit and far-sighted vision. Our discussions have been of immense value for my work.

Similarly, I have drawn much intellectual nourishment from Knut Selmer, who functioned as assistant supervisor for my research. Knut is one of the pioneering policy makers in the field of privacy and data protection. He has been particularly helpful in showing me the intricacies of such protection from a Norwegian perspective.

Thanks go also to the Norwegian Research Centre for Computers and Law (NRCCL), of which Knut is the founding father. The NRCCL – attached to the Law Faculty of the University of Oslo – has provided the base for my doctoral research efforts. I could not have had a better environment in which to work. The NRCCL is

an inspiring place for scholarship with an excellent library. I am grateful to the Centre's director, Jon Bing, for his enthusiastic support of my studies. Thanks go too to my other fellow researchers at the NRCCL for their camaraderie and willingness to discuss ideas. In this respect, special mention should be made of Dag Wiese Schartum, Jens Petter Berg and Andreas Galtung. Other researchers who are no longer at the Centre – namely Joachim Benno, Henning Herrestad and Christen Krogh – also deserve special mention here. I am further grateful for the support and friendship of the NRCCL's administrative personnel.

Many persons outside the NRCCL have assisted my research as well. The staff of the Norwegian Data Inspectorate have been particularly helpful, cheerfully opening their archives to me and readily responding to my numerous queries about their operations. I also thank the following persons for providing me with valuable information along the way: Peter Bayne (Australia), Colin Bennett (Canada), Peter Blume (Denmark), Herbert Burkert (Germany), Roger Clarke (Australia), Walter Dohr (Austria), Stewart Dresner (England), Jacques Fauvet (France), Graham Greenleaf (Australia), Elizabeth Longworth (New Zealand), Kevin O'Connor (Australia), Thomas Pletscher (Switzerland), Yves Poullet (Belgium), Peter Seipel (Sweden), Lindy Smith (Australia), Ian Walden (England) and Jean-Philippe Walter (Switzerland).

Financial support for my doctoral research stemmed primarily from the Norwegian Research Council, which granted me a three-year research scholarship commencing in August 1993. The Council also awarded me a three-year postdoctoral fellowship commencing in October 1999. In addition, I received funding from the Anders Jahre Foundation for the latter half of 1996 and from the Law Faculty of the University of Oslo for large parts of 1997 and 1998. Thanks go to these organisations for their financial assistance.

Finally, deep gratitude goes to my wife Toril, my children Sondre and Tuva (mateys, you'll understand why soon!), my parents Fyfe and Patricia, other family members and friends for their emotional support during the time spent working on this book. It has not always been an easy period. Although I have gained much along the way, there have been losses in other respects. I therefore dedicate this book to June, for what could have been.

Sydney / Oslo

Lee Bygrave
6 June 2002

Abbreviations

A	Series A of the Publications of the European Court of Human Rights
AC	Appeal Cases (UK)
ACM	Association for Computing Machinery (USA)
AGPS	Australian Government Publishing Service
All ER	All England Law Reports
Art	Article
Bet	Betænkning (report of legislative or investigative commission, Denmark)
BGBl	Bundesgesetzblatt (Federal Law Gazette, Austria)
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Decisions of the Federal Constitutional Court, Federal Republic of Germany)
Cal App	California Appellate Reports
chapt	chapter
CLSR	*Computer Law & Security Report*
cmnd	command paper
CR	*Computer und Recht*
DuD	*Datenschutz und Datensicherung*
DPP	Data Protection Principle
DVR	*Datenverarbeitung im Recht*
ECR	European Court Reports
EIPR	*European Intellectual Property Review*
espec	especially
et seq	*et sequentia* (and what follows)
ETS	European Treaty Series
F	Federal Reporter (USA)
FFS	Finlands författningssamling (Collection of Finnish Statutes)
F Supp	Federal Supplement (USA)
HCA	High Court of Australia
HREOC	Human Rights and Equal Opportunity Commission (Australia)
HRLJ	*Human Rights Law Journal*
HMSO	Her Majesty's Stationery Office (UK)
ia	*inter alia* (amongst other things)
ibid	*ibidem* (in the same place)
id	*idem* (the same)

Innst O	Odelstingsinnstilling (Parliamentary Standing Committee Report on Legislative Proposal, Norway)
Int	International
IPP	Information Privacy Principle
J	Journal
LJ	Law Journal
L Rev	Law Review
LoR	*Lov og Rett*
NE	North Eastern Reporter (USA)
NOU	Norges Offentlige Utredninger (Official Reports to Government, Norway)
NPP	National Privacy Principle
NSWLR	New South Wales Law Reports
OJ	Official Journal of the European Communities
Ot prp	Odelstingsproposisjon (Government Bill, Norway)
P	Pacific Reporter (USA)
para	paragraph
partic	particularly
PDRA	Personal Data Registers Act (Norway)
PLPR	*Privacy Law & Policy Reporter*
RDV	*Recht der Datenverarbeitung*
rev	revised
RJD	Reports of Judgments and Decisions of the European Court of Human Rights
Rt	Norsk Retstidende (Norwegian Law Reports)
s	section
SFS	Svensk författningssamling (Collection of Swedish Statutes)
SOU	Statens Offentliga Utredningar (State Official Reports, Sweden)
St meld	Stortingsmelding (Government Parliamentary Report, Norway)
SW	South Western Reporter (USA)
TDR	*Transnational Data & Communications Report*
TfR	*Tidsskrift for Rettsvitenskap*
trans	translated
US	United States Supreme Court Reports
USC	United States Code
vol	volume

Table of Statutes and Conventions

Table of Cases

1. Introduction

1.1 Subject Matter and Aims of Book

This book deals with a class of laws that commonly go by the name of data protection law. The term 'data protection' is most commonly used in European jurisdictions; in other jurisdictions, such as the USA, Canada and Australia, the term 'privacy protection' tends to be used instead. As shown further on, both epithets are problematic. For present purposes, however, it is sufficient to refer to the type of law in question as data protection law.

The central aim of the book is to cast light on the rationale, logic and limits of this class of laws. By 'rationale' is meant data protection laws' origins, aims and purposes. By 'logic' is meant these laws' basic regulatory mechanisms (including normative framework). By 'limits' is meant (i) the points on which data protection laws differ from other types of laws, and (ii) the points at which their regulatory mechanisms are demonstrably ineffective.

Illumination of these matters is sought by focusing on three sets of issues. The first set of issues concerns the nature of the interests and values which data protection laws promote and are capable of promoting, particularly as manifest in these laws' provisions, *travaux préparatoires* (preparatory works) and application.

The second set of issues concerns the extent to which it is desirable that the processing of information on private collective entities be controlled pursuant to the regulatory regimes established by data protection laws. By 'private collective entities' is primarily meant organised groups of people in the private sector. Put briefly, an organised group is one whose members take specific, systematic measures to establish and maintain it. Such groups range from business corporations to citizen initiative groups. Some account is also taken in the book of the interests of non-organised groups. A non-organised group is constituted primarily on the basis of sets of persons being viewed as sharing one or more characteristics – eg, ethnic origin, religious belief or sexuality – and being treated as a group on the basis of these characteristics.

The third set of issues deals with the ability of data protection laws to regulate the practice of profiling. In short, profiling involves the inference of a set of characteristics (typically behavioural) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics.

The three sets of issues are described in more detail in Parts II, III and IV of the book. They are not the only issues discussed in the book but they are the main ones.

Data protection laws are recent additions to the legal landscape; the first such laws were not enacted until the early 1970s. Though a large number of legal and quasi-legal instruments on data protection are now to be found, they still tend to be an unknown or poorly known quantity for many people, lawyers included.

A preliminary description of data protection laws can be given as follows. Such laws are comprised of rules that specifically regulate all or most stages in the processing of certain kinds of information. In other words, the laws directly address the manner in which information is collected, registered, stored, used and disseminated. Only *personal* information is usually covered by data protection laws. Such information is typically defined in these laws as information relating to, and permitting identification of, individual physical/natural persons (hereinafter also termed simply 'individuals') or sometimes collective entities. The most prominent aim of the laws is to safeguard certain interests and rights of an individual when information on him/her is processed by others. These interests and rights are usually expressed in terms of privacy, autonomy and/or integrity.

The central rules of data protection laws are based upon and embody a set of principles, the core of which can be summarised in the following terms:

1) personal information should be collected by fair and lawful means;
2) the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are gathered and further processed;
3) personal information should be collected for specified, lawful or legitimate purposes, and not processed in ways that are incompatible with those purposes;
4) use and disclosure of personal information for purposes other than those specified should occur only with the consent of the person(s) to whom the information relates or by authority of law;
5) personal information should be relevant, accurate and complete in relation to the purposes for which it is processed;
6) security measures should be taken to protect personal information from unauthorised or unintended disclosure, destruction, modification or use;
7) persons should be informed of, and given access to, information relating to them held by others, and be able to rectify this information if it is inaccurate or otherwise misleading;
8) those responsible for processing information on other persons should be accountable for complying with measures giving effect to the above principles.

The principles set out above are not the only principles found in data protection laws but they are the main ones. It is arguable that another principle should also be included in the above list. This principle is that fully automated assessments of a person's character should not form the sole basis of decisions that impinge upon the person's interests. While not yet manifest in the majority of data protection laws, the

principle is attaining prominence in Europe largely on account of its embodiment in Art 15 of the 1995 European Community (EC) Directive on data protection.[1]

Elements of the above principles, and some of the rights they give rise to, are found in various formats not just in data protection laws but in other types of policy documents and legal instruments. Obvious examples of the latter are legislation on administrative decision-making procedures, legislation on public access to government-held information and legislation on civil and criminal proceedings. However, only those legal instruments embracing all or most of the above principles are commonly considered to be data protection laws, a line also taken in this book. This is not to suggest, though, that other kinds of legal instruments and policy documents have no relevance for the interpretation and application of data protection laws or for furtherance of the values and rights which such laws attempt to safeguard.

Two additional features of data protection laws are worth noting at this preliminary stage. These features are not unique to data protection laws but help to distinguish them from a large number of other legal instruments. The first feature is that most data protection laws provide for the establishment of special independent bodies to oversee their implementation. Many of these bodies (hereinafter termed 'data protection authorities') are given broad, discretionary powers to monitor and regulate the data-processing activities of organisations in both the public and private sectors. They usually have other functions as well, such as handling complaints and giving advice on data protection matters.

The creation of these authorities underscores the second feature, which is that data protection laws often take the form of so-called 'framework' laws. Instead of setting down in casuistic fashion detailed provisions on the processing of personal information, data protection laws tend to set down rather diffusely formulated, general rules for such processing and make specific allowance for the subsequent development of more detailed regulatory norms as the need arises. Primary responsibility for developing these norms is often given to the respective data protection authority.

The above two features mean that, generally speaking, data protection laws are not simply sets of fixed rules on the processing of personal information; they also contain mechanisms for monitoring their application and for generating new regulatory norms.

Why do data protection laws deserve extensive study? There are two chief reasons, each of which is inter-related. The first is data protection laws' *practical* significance (both actual and potential); the second is their *normative* importance. With regard to the first reason, data protection laws have the potential to affect the heart of organisational activity. The processing of information, particularly personal

---

1 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (OJ L 281, 23.11.1995, 31). On the Directive's influence, see Chapter 2 (section 2.2). For presentation and analysis of Art 15, see Chapter 18 (section 18.3.1).

information, is central to the tasks of public administrative agencies and private organisations. Indeed, it is basic to interactions in all spheres of human society. Because data protection laws seek to regulate directly the processing of personal information, they can interfere (positively or negatively) with fundamental organisational operations, thereby generating significant administrative, commercial and social costs (and/or gains). This potential is augmented by the establishment of data protection authorities, many of which are given considerable power to steer the data-processing activities of organisations.

As for the second reason, data protection laws and the principles and ideals they embrace, are, on the informational plane, amongst the central legal and ethical counter-weights to more technocratic imperatives, such as increased organisational efficiency and maximisation of financial profit. This is not to suggest that data protection laws are necessarily opposed to these imperatives. In some respects, data protection laws can promote their realisation. Yet such laws also emphasise that account be taken of other values, needs and interests when processing personal data. In this respect, data protection laws and the ideals enshrined in them constitute an enrichment of our normative sphere.

To some extent, the normative and practical importance of the laws is mirrored in the burgeoning focus on rights to privacy and private life, with which data protection laws are closely linked. Frowein and Peukert claim that the right to private life has constituted the major challenge for the legal systems of liberal States during the latter half of the twentieth century.[2] Although this claim is somewhat exaggerated, it is scarcely to be denied that the creation and utilisation of privacy rights over the last few decades have assumed considerable prominence in many legal systems. For instance, the right to respect for private life set down in Art 8 of the 1950 *European Convention for the Protection of Human Rights and Fundamental Freedoms*[3] has become one of the most frequently contested rights in the case law produced by the Convention. The increasing prominence of such a right is not just symptomatic of the expansive ambit of the notions of privacy and private life. It is also symptomatic of a fundamental societal development whereby the public sphere is gradually expanding into previously private domains. Privacy rights are being created and used to shield persons from the detrimental effects of this development. A similar function is carried out by data protection laws on the informational plane.

The normative and practical significance of data protection laws is also reflected in the fact that their drafting and enactment have frequently been lengthy processes fraught with controversy. For example, it has been observed that in the life of the Federal Republic of Germany scarcely any statute has had a more complicated and

---

2 JA Frowein & W Peukert, *Europäische MenschenRechtsKonvention: EMRK-Kommentar* (Kehl am Rhein: NP Engel, 1996, 2nd ed), 338.

3 ETS No 5; opened for signature 4.11.1950; in force 3.9.1953 – hereinafter termed 'European Convention on Human Rights' or 'ECHR'.

drawn out legislative history than the first *Federal Data Protection Act*, adopted in 1977.[4] Initial enactment of data protection legislation in a range of other jurisdictions, such as the United Kingdom (UK), Australia and the Netherlands, was also far from being 'short and sweet'.[5] Similarly, the drafting and adoption of the EC Directive on data protection was an extremely protracted affair marked by hefty debate and frenetic lobbying.[6] Not all data protection laws, however, have had a long or troublesome gestation. For instance, preparation and enactment of data protection legislation in Sweden occurred relatively quickly and smoothly.[7] The same can be said for Norway and Denmark, but certainly not Finland, where work on drafting the first national data protection Act took over 15 years and was frequently paralysed by political conflict.[8]

While most of the controversy surrounding the drafting and enactment of data protection laws has stemmed ultimately from the laws' perceived potential to impinge negatively upon the ways in which organisations function, other factors have sometimes played a role as well. In the UK, for instance, resistance to the initial enactment of data protection legislation was exacerbated by the fact that such legislation could not be easily accommodated within the country's constitutional system.[9] It was also exacerbated by the fact that the typical form and structure of

---

4 *Bundesdatenschutzgesetz – Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung vom 27 Januar 1977*. See S Simitis, 'Einleitung', in S Simitis, U Dammann, O Mallmann & H-J Reh, *Kommentar zum Bundesdatenschutzgesetz* (Baden-Baden: Nomos, 1981, 3rd ed), 69. The Act was replaced by the *Federal Data Protection Act* of 1990 (*Bundesdatenschutzgesetz – Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20 Dezember 1990*). The latter Act was substantially amended in 2001 (see *Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und andere Gesetze*, in force 23.05.2001) to bring German law in line with the EC Directive on data protection. Unless otherwise specified, all further references to German federal data protection legislation are to the 1990 Act as most recently amended.

5 With regard to the UK, see, eg, CJ Bennett, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992), espec 82–94, 209ff. In relation to Australia, see, eg, LA Bygrave, 'The Privacy Act 1988 (Cth): A Study in the Protection of Privacy and the Protection of Political Power' (1990) 19 *Federal L Rev*, 128, espec 137ff. Regarding the Netherlands, see, eg, VA de Pous, 'Dutch Privacy Bill Again Delayed' (1988) 11 *TDR*, no 10, 6–7.

6 For outlines of the political manoeuvres that lay behind adoption of the Directive, see N Platten, 'Background to and History of the Directive, in D Bainbridge, *EC Data Protection Directive* (London: Butterworths, 1996), chapt 2, espec 23–32; S Simitis, 'From the Market To the Polis: The EU Directive on the Protection of Personal Data' (1995) 80 *Iowa L Rev*, 445–469. For a description of the lobbying campaigns of business groups, see PM Regan, 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics', in CJ Bennett & R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999), 199–216.

7 See, eg, Bennett, *supra* n 5, 60–65, 218.

8 See, eg, J Kuopos, 'Finland', in D Campbell & J Fisher (eds), *Data Transmission and Privacy* (Dordrecht: M Nijhoff, 1994), 161, 162.

9 See espec PM Regan, 'Protecting Privacy and Controlling Bureaucracies: Constraints of British Constitutional Principles' (1990) 3 *Governance*, 33–54.

such legislation fitted uneasily with customary statutory drafting techniques in the UK.[10]

Occasionally, the controversy over legislating with respect to data protection has been channeled along the traditional, Left-Right axis of political conflict. This has been the case, for example, in Finland.[11] Yet, generally speaking, concern for privacy and data protection tends to cut across a broad range of political ideologies. In the words of Colin Bennett,

> '[t]he issue [of data protection] is so sufficiently broad that it can encompass a variety of different positions, from the civil libertarian who demands constraints on overzealous law enforcement to the conservative business group that wants tax data to be kept confidential. The issue tends to pose a dilemma for democratic socialist parties in particular; it exposes a tension between the welfare statism of the old Left, which relies on a sacrifice of individual privacy for the collective benefit, and the more antistatist individualism of the new Left. Thus below the broad liberal democratic concern for individualism and human dignity lies a complex and often contradictory set of positions. [...] The ideological foundations of the issue are inherently ambiguous because privacy and data protection do not stir partisan emotion until the debate centers on particular information in specific contexts. We then find a complexity of cross-cutting concerns.'[12]

In light of the aim of the book to cast light on the rationale, logic and limits of data protection laws, what is the justification for paying special attention to the three sets of issues described at the beginning of this introduction? More specifically, what is the point in discussing: (i) the kinds of interests and values promoted by data protection laws (hereinafter termed 'issue set 1'); (ii) the extent to which the processing of information on private collective entities should be regulated by these laws (hereinafter termed 'issue set 2'); and (iii) the ability of these laws to control profiling practices (hereinafter termed 'issue set 3')?

To begin with, the perspectives generated from analysing each of the three sets of issues are able to put traditional conceptions of these laws' rationale, logic and limits to the test. In other words, they tend to bring such conceptions into sharp relief and to encourage their rethinking.

---

10 See, eg, M Stallworthy, 'Data Protection: Regulation in a Deregulatory State' (1990) 11 *Statute L Rev*, 130, 134ff.

11 See further A Saarenpää, 'Data Protection: In Pursuit of Information. Some Background to, and Implementations of, Data Protection in Finland' (1997) 11 *Int Rev of Law Computers & Technology*, 47, 48.

12 Bennett, *supra* n 5, 147.

It is certainly not the case that such capabilities follow from analysis of these three sets of issues alone. Nevertheless, several reasons exist for focusing on issue sets 1–3 at the expense, to some extent, of other relevant issues.

Regarding issue set 1, analysis of this is indispensable to understanding the rationale, logic and limits of data protection laws. The way in which one conceptualises the interests and values served by these laws is not just of academic interest but has significant regulatory implications. It is pivotal to working out the proper ambit of the laws and, concomitantly, the proper mandate for data protection authorities. Thus, it is privotal for resolving issue set 2. It also has relevance for aspects of issue set 3 as the efficient practice of data protection is only possible if there is clarity over its goals.[13] The importance of this insight is augmented by the fact – elaborated further on in the book – that the formal goals of data protection laws tend to be expressed in diffuse terms and that data protection authorities often enjoy broad discretionary powers. More generally, when desirous of introducing legal limitations on a particular data-processing practice, one needs: (i) to have a clear idea of the reasons for these limitations; and (ii) to communicate such reasons intelligibly to the rest of society. The necessity of satisfying the two needs grows in proportion to the stringency of the desired limitations. A prerequisite for satisfying these needs is the explication of the various interests and values affected by the data-processing practice in question and the way in which the desired regulation of the practice can safeguard these interests and values.

An important reason for analysing issue sets 2 and 3 is that both sets of issues confront pressing realities of contemporary Western societies which law and policy on data protection must face. In this respect, particular mention should be made of the fact that profiling practices tend to result in the gradual extension and tightening of social control mechanisms, a process often viewed as containing the seeds for a totalitarian future. Special mention should also be made of the increasing ambit and complexity of organisational data-processing operations, affecting not just individual persons *qua* individuals but groups and organisations as well.

Indeed, all three sets of issues are complementary in terms of their potential to broaden the focus of data protection from data on individual persons to data on groups of persons, from single instances of data processing to entire data-processing systems, and from such systems as isolated units to inter-system connections. In short, all three sets of issues can involve supplementing micro- with macro-perspectives.

A further reason for focusing on the three sets of issues is the scarcity of systematic, extensive analysis of them. Of the three sets of issues, that dealing with profiling practices appears to have received the least such analysis in prior discourse on data protection. This is probably because such practices have been regarded as

---

13 See espec O Mallmann, *Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information. Mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen* (Frankfurt am Main: A Metzner, 1977), 10.

relatively peripheral to the central rules in data protection laws. A substantial number of profiling practices are not concerned directly with physical forms of data processing but with analysis/interpretation of pre-processed data. Nevertheless, profiling frequently serves to initiate various physical forms of data processing (such as data matching – ie, the comparison/cross-referencing of data), and *vice versa*. This is another reason for focusing on profiling.

As for issue sets 1 and 2, discussion of these has been quite extensive. Yet many of the contributions to this discussion appear to have been based more on each contributor's instinctive sense of what is appropriate and what is not, rather than on detached and thorough analyses of all factors involved. Evidence to support this impression is found at numerous points in Parts II and III of the book.

Writing over twenty years ago, Otto Mallmann commented that the aims and function of data protection (and, by implication, data protection laws) had been insufficiently analysed.[14] While some fine, in-depth analyses on the subject have since been published,[15] considerable uncertainty still seems to reign about exactly which interests and values are promoted by data protection laws.[16] This uncertainty is both exacerbated by and reflected in the fact – elaborated in Chapter 2 – that numerous such laws have failed to specify formally the interests and values they serve. Certainly, a fairly broad consensus exists that data protection laws are aimed primarily at safeguarding the 'privacy' of individual persons against potentially intrusive data-processing practices of large organisations. However, this depiction of the rationale of data protection laws is too often accepted without serious analysis of its adequacy, either in terms of its conceptual veracity or its ability to aid in the generation of lucid and coherent regulatory measures. As shown in Part II, a major sticking point is its focus on privacy. This focus tends to side-line or exclude detailed consideration of a range of other interests and values safeguarded by data protection laws. Moreover, the exact manner in which the rules and principles found in these laws embody or intersect with a concern for privacy (however defined) tends to be left unexplored.

As for the issue of data protection for private collective entities, debate on the issue has focused mainly on data protection for legal/juristic persons only (not all of which are collective in nature). Other types of collective entities have scarcely figured in the debate. Even with regard to legal/juristic persons, the decisions of most

---

14 *Ibid*, 9.

15 Mallmann's own analysis (*ibid*) being an example.

16 See, eg, D Korff, *Study on the Protection of the Rights and Interests of Legal Persons with regard to the Processing of Personal Data relating to such Persons*, final report to the EC Commission, October 1998, <http://europa.eu.int/comm/internal_market/en/dataprot/studies/legalen.htm>, 42 (claiming that '[t]here is a lack of clarity, of focus, over the very nature, aims and objects of data protection in the [EU] Member States which is, not surprisingly, reflected in the international data protection instruments'); B Napier, 'International Data Protection Standards and British Experience' (1992) *Informatica e diritto*, no 1–2, 83, 85 (claiming that, in Britain, 'the conceptual basis for data protection laws remains unclear').

countries' legislators on whether or not information on such entities should be directly safeguarded under data protection legislation appear to have been made without a thorough study of the issue first being undertaken. Furthermore, while governmental and data protection authorities in some of these countries have declared that such studies should and would be undertaken soon after the enactment of their data protection laws, few such studies seem to have eventuated.

Another reason for taking up the issue of data protection for collective entities is its significance beyond the field of data protection law. The issue is part of a more general problem concerning the integration of collective entities into legal systems with a conceptual apparatus based primarily on the needs and interests of individual persons. This problem is important from the perspectives of both legal science and legal policy. What makes the problem particularly vexing is that legislators and members of the judiciary have often decided on whether or not to give collective entities certain rights enjoyed by individuals, without providing detailed reasons for their decisions. The absence of such reasons has meant that the legal boundary lines marking out the extent to which collective entities are accorded the rights of individuals appear often to have been set down in an arbitrary and loosely reasoned manner. Certainly, scholars have spilled a great deal of ink on a great deal of paper in an effort to ascertain, at a conceptual level at least, the 'true' nature of various collective entities. In many legal fields, however, legislators, judges and other policy makers have not complemented this effort with systematic analyses of the actual needs and functions of collective entities, or of the actual consequences of their decisions concerning the legal rights of such entities. Data protection law is one such field.

1.2 Approach and Orientation of Book

This book is a piece of legal scholarship. It does not fit squarely, however, within any one of the traditional categories of such scholarship. The book is not a standard example of 'legal dogmatics' or what is sometimes called 'the rule-oriented approach'[17] for its main aim is not to analyse in minute detail the contents of data protection laws, provision by provision, in order to determine what is valid law. Neither is the book a standard example of jurisprudence for it is not primarily concerned with investigating the basic nature of legal reasoning, legal science or legal concepts. To describe the book as essentially a work of legal sociology would also be misleading as no attempt is made to study systematically the way in which data protection laws are actually practised.

---

17 P Westberg, 'Avhandlingsskrivande och val av forskningsansats – en idé om rättsvetenskaplig öppenhet', in L Heuman (ed), *Festskrift til Per Olof Bolding* (Stockholm: Juristförlaget, 1992), 421, 427–436 (describing 'den regelorienterade ansatsen').

At a very general level, the book is an example of what has been termed 'the problem- and interest-oriented approach'; that is, an attempt is made (by contrast to 'the rule-oriented approach') not simply to resolve the problem of what is valid law in a given field but to assess the legal rules in that field from the perspectives of other issues.[18] Such research tends to be relatively eclectic in its use of source materials and study methods. This book is no exception. Elements of all three of the traditional categories of legal scholarship listed above are present. Also present are elements from other fields of study, including those of computer and information science, sociology, philosophy and political science.

The eclectic approach of the book follows necessarily from the nature of the issues discussed. At the same time, a significant degree of eclecticism informs legal research and analysis generally in the field of data protection law.[19] To a great extent, the content of data protection laws itself tends to open for and demand a relatively wide-ranging use of perspectives and methods. As shown further on in the book, many of the central provisions of data protection laws function substantially as 'guiding standards' ('retningslinjer') in the terminology of Nils Kristian Sundby and Torstein Eckhoff,[20] or as 'principles' in Ronald Dworkin's terminology.[21] Through use of criteria, such as 'reasonable', 'fair', 'legitimate' and 'objectively justifiable', they call for a weighing up of various interests and values which rests largely upon assessment of ethical, political, technological and economic factors – a point brought home especially in Part IV. Thus, the strictly legal elements of data protection laws which can be adequately analysed using the traditional methods of legal dogmatics tend to merge with, and give way to, relatively loose policy assessments that cannot be adequately analysed without going beyond such methods. To ignore these policy assessments and focus upon purely legal matters, such as the valid competence of the

---

18 *Ibid*, 436ff (describing 'den problem- och intresseorienterade ansatsen').

19 Prominent examples are J Bing, 'Data Protection in a Time of Changes', in WFK Altes, EJ Dommering, PB Hugenholtz & JJC Kabel (eds), *Information Law Towards the 21st Century* (Deventer: Kluwer Law & Taxation, 1992), 247–259; H Burkert, 'Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws' (1981–1982) 3 *Computer/LJ*, 167–188; S Rodotà, 'Protecting Informational Privacy: Trends and Problems', in Altes *et al* (eds), *Information Law Towards the 21st Century*, *op cit*, 261–272; S Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 *University of Pennsylvania L Rev*, 707–746; and KS Selmer, 'Realising Data Protection', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 41–65. Cf P Seipel, *Computing Law* (Stockholm: Liber, 1977), chapt 7 (pointing out that computing law studies in general are inevitably multidisciplinary). Political scientists studying privacy and data protection issues have also commented on the necessity of adopting an inter-disciplinary approach in their research. See WBHJ van de Donk, CJ Bennett & CD Raab, 'The politics and policy of data protection: concluding observations' (1996) 62 *Int Rev of Administrative Sciences*, 569.

20 T Eckhoff, 'Guiding Standards in Legal Reasoning' (1976) 29 *Current Legal Problems*, 205–219; NK Sundby, *Om normer* (Oslo: Universitetsforlaget, 1974), 198ff; T Eckhoff & NK Sundby, *Rettssystemer* (Oslo: TANO, 1991, 2nd ed), 109ff.

21 R Dworkin, *Taking Rights Seriously* (London: Duckworth, 1977), espec 22ff.

respective data protection authority, would fail to come to grips with important aspects of data protection laws' regulatory dynamic.

The degree of eclecticism in the book's approach should not be overplayed. The bulk of source documentation for the book consists of conventional legal materials – treaties, statutes, regulations, preparatory works (*travaux préparatoires*), judicial decisions and legal scholars' commentaries. Moreover, a considerable amount of the book is devoted to determining the valid content of the central rules of data protection laws.

Account is taken in the book of a variety of countries' legal rules and policies on data protection. To some extent, an attempt is made also to ascertain basic similarities and differences between various national and international data protection instruments. Hence, it is tempting to describe the book as a work of comparative law. The central thrust of the book, however, is not comparative; its cross-national orientation is rather an attempt to illustrate possible conflicts, issues or legal strategies. Further, there is no extensive, systematic comparison of various national and international data protection instruments in order to determine which of them comes closest to 'best practice' in the field though some limited normative comparisons are made.

I refrain from undertaking such normative comparison in any extensive way because of its many potential pitfalls, given my lack of detailed knowledge of the totalities of many of the national legal systems studied. While normative, comparative studies in the data protection field are of great value, they are exceedingly difficult to conduct without misconstruing some element(s) of the compared national systems. The exact manner in which a particular country's system of data protection functions, tends to be tied closely not just to the formal rules of the system but also to a myriad of informal, national traditions and attitudes which can be easily overlooked or misunderstood. This is a problem besetting all kinds of cross-national analyses of legal systems though it is most acute with normative comparisons.

Some scholars claim that meaningful comparative analysis in the field of data protection law is well nigh impossible.[22] In my view, meaningful comparative analysis is not impossible but certainly difficult to execute successfully. Moreover, this difficulty increases as one goes from attempting merely to ascertain similarities and differences between national systems of data protection, to attempting to explain the origins of these similarities and differences, and, finally, to attempting to evaluate which of the systems is best.

These observations notwithstanding, persuasive grounds exist for a cross-national orientation. It enriches legal discourse and helps combat narrow-minded adherence to national dogma. Further, problems in particular jurisdictions can often be anticipated, illustrated or explained only by looking at developments in other

22 See, eg, Selmer, *supra* n 19, 41–42.

jurisdictions. This point has not been lost on the bodies that have been charged with drawing up and/or implementing national data protection laws: a tradition of close international co-operation and consultation has existed in the data protection field since the early 1970s.[23] Additionally, as data-processing operations increasingly extend across national boundaries, the way in which they are to be regulated should not occur without consideration of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation. Finally, a cross-national perspective is analytically fruitful given the fact – elaborated upon in Chapter 3 – that all countries' data protection laws are based upon and embody a set of broadly similar principles.

Despite its international orientation, references to Norwegian theory and practice on data protection figure prominently in the book and provide many of the points of departure for its discussions. This is particularly so in the analysis of the issues of the rationale for data protection laws and the regulation of profiling. The prominence of Norwegian theory and practice on data protection is due not simply to the fact that the book has been written at the Norwegian Research Centre for Computers and Law, where I have had ready access to Norwegian materials; it is due also to the fact that these materials ably illustrate many of the points I wish to make. Under the aegis of the Centre, an extensive number of studies have been carried out on data protection issues. These studies have resulted in relatively well-developed perspectives on what data protection involves.

Norwegian theory and practice on data protection should additionally be of interest to an international audience because Norway has a long-established legal regime for data protection. It is one of the very few regimes which has operated relatively extensively with a requirement that personal data registers be formally licensed (approved) by the national data protection authority before they are established. This licensing system – described more fully in Chapter 18 – has given the authority a great deal of formal power to steer the processing of personal data in both the private and public sectors. The record of the way in which the authority has treated the numerous license applications provides an instructive insight into the myriad issues connected with data protection.

Norwegian practices in this field are also interesting for an international audience because they occur in a society with arguably much potential for the undermining of data protection interests. Use of advanced information technology in both the Norwegian public and private sectors is extensive. Norway has also a long-established, comprehensive scheme whereby each member of the country's population is allocated a unique personal identification number (PIN), stored in a central population register. Furthermore, claims have been made that the country's

---

23 See generally H Seip, 'Data Protection, Privacy and National Borders', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 67–82.

cultural-political climate does little to encourage the preservation of personal privacy.[24]

The book is a product of law-reformist ambition in addition to descriptive-explanatory aims. This ambition is not so much to set out a comprehensive, fixed agenda for changing current data protection laws but to facilitate the establishment of such an agenda by challenging some of the ways in which these laws have been conceptualised. To a great extent, I seek here to air possibilities and explore perspectives. I seek also to show that arguments and distinctions which have been invoked in relation to the issues taken up in the book are not always solid or incontrovertible. As such, I am often less concerned with arguing for conclusive answers to these issues than with creating a general framework for analysing all sides of them.

1.3 Underlying Thesis of Book

While a significant aim with the book is to air possibilities, explore perspectives and challenge assumptions, it also advances a basic thesis. In very general terms, this thesis is that the rationale, logic and limits of data protection laws can only be adequately analysed in the light of increasing *electronic interpenetration* of previously distinct spheres of activity. The notion of electronic interpenetration denotes a trend towards greater dissemination, use and re-use of information across traditional organisational boundaries and a trend towards replacing or supplementing manual controls by automated controls. These processes are described in more detail in Chapter 6.

Electronic interpenetration, it is argued, necessitates expanding some traditional perspectives on data protection laws and dispensing with others. It requires that the concern of law and policy on data protection be shifted increasingly from the individual to the collective and systemic level, from the national to the inter- and supranational plane, and from the intra-organisational to the inter-organisational sphere. More specifically, greater attention will have to be given to protection of data not just on individual persons but *collective* entities. Greater attention will also have to be given to securing adequate quality not just of data and information but the *systems* used to process them.

---

24 See, eg, R Lunheim & G Sindre, 'Privacy and Computing: A Cultural Perspective', in R Sizer, L Yngström, H Kaspersen & S Fischer-Hübner (eds), *Security and Control of Information Technology in Society* (Amsterdam: North-Holland, 1994), 25, 33–37.

1.4 Source Material and Method

1.4.1 SOURCE MATERIAL

Data protection issues have generated a large amount of literature. Some idea of the enormity of this literature is gained by looking through David Flaherty's survey of some of it as of 1984.[25] His survey – mainly covering publications in the UK, USA, Germany, France, Canada and Sweden – contains close to 1900 entries. A great deal has been added to the literature since 1984, as the bibliography for this book testifies. The quantity of materials on data protection issues seems to be growing at an almost exponential rate. Accompanying this development is a steady increase in the number and spread of data protection instruments around the globe.[26]

It goes without saying that the research for this book has only canvassed a subset of the available source materials. Focus has been directed at materials that are relatively rich with information and perspectives pertinent to the issue(s) at stake.[27] These comments embrace, of course, my sampling strategy with respect to data protection legislation. Other factors, though, have also influenced my focus on certain data protection instruments at the expense of others. One factor is the normative significance of the instruments, especially in terms of their ability to determine the shape of data protection law across a range of jurisdictions. This factor largely accounts for my focus on the EC Directive on data protection, particularly in Parts I and IV. Another factor is my familiarity with the respective legal systems of which the instruments are a part. This factor largely accounts for my focus on the data protection laws of Australia, the UK and Norway at various points throughout the book.

While the subset of data protection laws upon which I have focused my research efforts *might* well be representative for all data protection regimes around the world, I am not definitely certain it is. Accordingly, many of the conclusions reached in this book as to the rationale, logic and limits of data protection laws should be treated as only *tentatively* capable of generalisation for all such laws. To borrow Patton's

---

25 DH Flaherty (ed), *Privacy and Data Protection. An International Bibliography* (London: Mansell, 1984).

26 For a reasonably current overview of the global situation with respect to data protection instruments, see Electronic Privacy Information Center (EPIC) & Privacy International (PI), *Privacy and Human Rights 2001. An International Survey of Privacy Laws and Developments* (Washington, DC: EPIC/PI, 2001).

27 In the social sciences, this sampling strategy sometimes goes under the name 'purposeful sampling'. See MQ Patton, *Qualitative Evaluation and Research Methods* (Newbury Park/London/New Delhi: Sage, 1990, 2nd ed), 169.

terminology, we can call such conclusions 'working hypotheses' or 'extrapolations'.[28]

The tentative nature of many of the conclusions in the book follows not only from the fact that I have not investigated in depth all data protection regimes around the world; it also follows from the fact that the focus and agenda of such regimes are constantly developing. The dynamic character of law and policy on data protection is demonstrated at numerous points in the book.

1.4.2 LEGAL METHOD AND DIFFICULTIES

It goes without saying that when examining legal rules in an effort to determine what is valid law, I employ the method typical of legal dogmatic analysis. Concomitantly, my point of departure for assessing what is valid law in a particular jurisdiction is the analytical method of a judge belonging to the highest court in the jurisdiction concerned. This does not mean, however, that I always accept the *actual* decisions of such courts as accurate indications of what is valid law.

I have been sensitive to the existence of some variations in legal dogmatic method from jurisdiction to jurisdiction.[29] It is, however, often difficult to make valid comparisons in this regard and relatively easy to overplay distinctions. Such variations can, though need not always, affect conclusions as to what is valid law in a given context.

Efforts to arrive at firm conclusions on the proper ambit of data protection laws are hampered by the diffuse formulation of many of these laws' provisions. Even relatively extensive and detailed laws (such as the federal *Privacy Acts* of Canada and Australia) abound with vaguely worded rules.

This difficulty is frequently compounded by sparse and/or nebulous commentary in the preparatory works and explanatory memoranda for the laws. Further aggravating the difficulty is a paucity of relevant judicial decisions. In many

---

28 *Ibid*, 489 ('Extrapolations are modest speculations on the likely applicability of findings to other situations under similar, but not identical, conditions. Extrapolations are logical, thoughtful and problem oriented rather than statistical and probabilistic').

29 Compare, eg, the approach of Norwegian courts to statutory interpretation with the approach taken by English courts. Norwegian courts tend to place greater weight on relevant *travaux préparatoires* than their English counterparts have traditionally done. Indeed, in Norway, even legislators' statements about the ambit and content of a statute which are put down in a parliamentary report *after* the statute's enactment, may be consulted by the courts when interpreting the statute: see, eg, E Boe, 'Domstolskontroll med forvaltningen: Åpne fullmakter og Høyesteretts svar i 90-årene' (1994) *LoR*, 323, espec 329–334 and references cited therein. Further, Norwegian courts tend to take a more flexible approach to precedent than has traditionally been the case with English courts. Norwegian courts appear also to place greater emphasis on so-called 'reelle hensyn' (ie, considerations of what is reasonable and practicable in the circumstances of the particular case). See generally T Eckhoff (with JE Helgesen), *Rettskildelære* (Oslo: Tano Aschehoug, 1997, 4th ed), 76ff, 173ff, 357ff; cf D Keenan, *Smith & Keenan's English Law* (London: Pitman Publishing, 1995, 11th ed), 130ff.

countries, court involvement in interpreting and applying data protection legislation has been minor if not marginal.[30]

The small amount of court involvement in applying data protection laws also makes it difficult to determine the extent to which the respective practices of data protection authorities conform with the views of the judiciary in the various countries concerned. This notwithstanding, case law shows that courts will occasionally overturn or question the lines taken by data protection authorities, even when these lines are well-established.[31] In other words, the often judicially untested views of data protection authorities will not necessarily withstand judicial scrutiny.

The latter point might seem trite but is important to spell out in a situation where data protection authorities often have ended up being able to interpret, set and apply the rules with little corrective input from the courts. In many countries, such as Australia, Denmark, New Zealand (NZ), Norway and the UK, this situation has pertained for a considerable number of years. One danger with it is that the data protection authorities begin to construe the legislation in ways that further the cause of privacy and data protection at the expense of other factors that deserve equal or greater weighting in law. The judiciary, approaching the legislation with relatively fresh eyes and formally unencumbered by a pro-privacy mandate, will tend to be better able to resist such bias. Yet we must not overlook that the courts' frequent lack of familiarity with the legislation, combined with the time pressures of litigation, can increase the likelihood of judges failing to properly appreciate the complexities of the legislation in ways that undermine the correctness of their judgments.

In light of all of the above factors, any distinction between what the law is (*lex lata*) in the field of data protection and what the law ought to be (*lex ferenda*) is more obviously difficult to draw than in many other fields.[32] This difficulty is compounded especially with respect to many of the issues taken up in the book. As subsequent chapters show, we are frequently faced with a dearth of legally authoritative opinion addressing the resolution of precisely these issues.

---

30 See further LA Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law', in P Wahlgren (ed), *IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000* (Stockholm: Jure AB, 2001), 113–125. The article is also published in (2000) 7 *PLPR*, 11–14, 33–36.

31 See, eg, the decision of 12.6.2001 by the Swedish Supreme Court (*Högsta domstolen*) in case B293-00 (overturning administrative practice in relation to application of s 7 of the *Personal Data Act* of 1998 (*Personuppgiftslagen*, SFS 1998:204)). For more detail on the decision, see Chapter 2 (section 2.4.3).

32 Such a distinction, though, is always difficult to draw (independent of the above factors) in both chronological and deontological terms. Concomitantly, it tends to underplay the dynamic realities of how law develops. See, eg, M Sandström & C Peterson, 'Lex Lata – Lex Ferenda. Fakta eller Fiktion?', in J Rosén (ed), *Lex Ferenda* (Stockholm: Juristförlaget/Norstedts Juridik, 1996), 159–177.

1.4.3 LEGAL ASPECTS OF ADMINISTRATIVE DECISION MAKING PURSUANT TO NORWEGIAN DATA PROTECTION LAW

Given the prominent place accorded in the book to the policies and experiences of Norway's data protection authority – the Data Inspectorate (Datatilsynet), it is appropriate to provide a brief description of certain legal aspects of the Inspectorate's decision making. This description pertains primarily to decision making pursuant to the *Personal Data Registers Act* of 1978 (hereinafter also termed 'PDRA')[33] as the bulk of cases referred to in the book were decided whilst that Act was in force. The PDRA has now been repealed and replaced by the *Personal Data Act* of 2000 (hereinafter also termed 'PDA').[34] However, with a couple of exceptions (noted below), the following description is also relevant for decision making pursuant to the new legislation.

The Inspectorate has been given authority to issue legally binding decisions pursuant to both Acts. These decisions may be appealed to another administrative body. Under the PDRA, this body was, as a general rule, the Ministry of Justice.[35] Under the PDA, a new quasi-judicial appeals body – the Data Protection Tribunal (*Personvernnemda*) – has taken over that role (s 43).

When exercising its discretionary powers pursuant to either Act, the Inspectorate was/is not legally bound to follow the line of its previous decisions when reaching a new decision, as long as its change of direction was/is objectively justifiable or otherwise *intra vires*.[36] The same applies with respect to both the Ministry of Justice and the Data Protection Tribunal. However, the Inspectorate was/is legally bound to implement the decisions reached by the Ministry/Tribunal on appeal. Moreover, the Inspectorate and the appeal bodies place(ed) considerable weight on their earlier decisions and tend(ed) to adopt a line consistent with these, in conformity with basic administrative law doctrines concerning legal certainty and reasonableness.[37]

To some extent, both the Inspectorate and the appeal bodies function(ed) – and were/are expected to function – as rule-generating bodies with respect to implementation of the legislation. The latter has been drafted very much as framework legislation to be built upon by rules issued by the Inspectorate (primarily through setting down conditions for the granting of licenses to establish personal data registers) and by the Ministry/Tribunal (through issuing regulations and/or handling appeals).[38]

---

33 *Lov om personregistre mm av 9 juni 1978 nr 48*.

34 *Lov om behandling av personopplysninger av 14 april 2000 nr 31*.

35 See *Forskrift om personregistre mm og om delegasjon av myndighet 21 desember 1979 nr 7*, part II.

36 See generally T Eckhoff & E Smith, *Forvaltningsrett* (Oslo: TANO, 1997, 6th ed), chapt 12, espec 303ff.

37 See generally LA Bygrave, *Personvern i praksis: Justisdepartementets behandling av klager på Datatilsynets enkeltvedtak 1980–1996* (Oslo: Cappelen, 1997), espec 24.

38 See, eg, Ot prp 2 (1977–78), *Om lov om personregistre mm*, 65–66. Note that the Inspectorate does not have competence to issue regulations under either Act.

It goes without saying that, in the context of the traditional hierarchy of legal sources, the findings of the Inspectorate and the above appeal bodies on questions of law are not as authoritative as a court's finding with respect to such matters.[39] This does not mean that a Norwegian court, when called upon to interpret either the PDRA or PDA, would discount the relevant findings and practice of the Inspectorate or the appeal bodies. In such a situation, a court would be likely to accord considerable weight to such findings and practice because of, firstly, the special expertise of the Inspectorate (and, to some extent, appeal body) in implementing the Act concerned and understanding data protection issues and, secondly, the fact that the matter in dispute would have been handled by qualified lawyers in both bodies (with assistance, where necessary, from experts on use of information technology).[40]

At the same time, certain factors could detract from the weight of the Inspectorate's decisions. For instance, such decisions tend not to be grounded on adversary procedures to the same extent as in judicial review.[41] Concomitantly, the Inspectorate's interpretation of the law might at times be biased towards promoting data protection at the expense of other factors that legally deserve equal or greater weighting.[42]

Nevertheless, the courts would be very reluctant to overturn a decision of the Inspectorate or appeal body where the matter in dispute turns on the exercise of either body's discretionary powers pursuant to the Act concerned.[43] As shown in Chapter 18 (section 18.4.7), the extent of these discretionary powers is and was considerable, especially under the PDRA.

1.4.4 LEGISLATIVE REFERENCES

Unless otherwise stated, legislative references in the book are to laws in their amended state as of 10.5.2002. The legislative picture is complicated due to an extensive process of recent reform of national laws – primarily in Europe but in other

---

39 See generally Eckhoff (with Helgesen), *supra* n 29, espec 158–159, 229.

40 *Ibid*, 229ff. This is illustrated, albeit weakly, by the judgment of the Supreme Court (*Høyesterett*) in the so-called 'snack-bar' case: Rt 1991, 616. When dealing with an issue concerning the ambit of the PDRA, the Court accorded generous place to the relevant views and practice of the Inspectorate. However, the Court refrained from addressing explicitly the weight it accorded to these views, and cast doubt over their validity.

41 See also more generally JF Bernt, 'Rettskildebruk for forskeren – En sammenligning med domstolenes og forvaltningens rettskildebruk' (1989) 102 *TfR*, 265, 276.

42 See also more generally G Holgersen, 'Den rettskildemessige vekt av praksis ved spesielle håndhevings- og kontrollorganer innen forvaltningen' (1987) 100 *TfR*, 404, 415. For a concrete example in which such bias appears to have afflicted the Inspectorate, see case 95/1193 summarised in Bygrave, *supra* n 37, 220–223. Note that the above case reference code (95/1193) is that used by the Inspectorate. The same applies to all other reference codes cited in the book in relation to cases handled by the Inspectorate.

43 See generally Eckhoff & Smith, *supra* n 36, 267–310.

countries too – which, as elaborated upon in Chapter 2 (section 2.2), has been largely occasioned by the EC Directive on data protection. The tempo of this reform process varies considerably from country to country.[44]

For English translations of European data protection legislation, I have relied where possible on the translations provided in an handbook edited by Spiros Simitis, Ulrich Dammann and Maritta Körner.[45] For English translations of non-European instruments I have relied to some extent on an (now relatively dated) handbook by Wayne Madsen.[46]

Legislative references in the following are often shortened. For instance, Australia's federal *Privacy Act 1988* is sometimes referred to simply as the 'Australian Act', the EC Directive on data protection is usually described as 'the Directive', etc.

1.5 Terminology

The book makes use of a large number of nebulous terms. In the following, an attempt is made to clarify the usage of the most prominent of these terms for the purposes of the book. These terms include 'information', 'data', 'information system', 'information technology', 'data subject', 'data controller', 'data protection', 'data security', 'privacy', 'autonomy', 'integrity', 'dignity', 'interest' and 'information quality'.

---

44 Most EU Member States have now completed changing their respective regulatory regimes with a view to meeting requirements of the Directive. France remains a laggard in this context though a Bill to amend its legislation in line with the Directive is currently before the French Parliament: see *Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (no 3250), introduced 18.7.2001. The date for final adoption of the Bill is uncertain (as of 15.4.2002). Another laggard in this context is Luxembourg which has been prosecuted for failing to transpose the Directive within the prescribed period: see judgment of 4.10.2001 by the European Court of Justice in case C-450/00, *Commission of the European Communities v Grand Duchy of Luxembourg*, unreported. A Bill for a new data protection law was issued in October 2000: see *Projet de loi relatif à la protection des personnes à l'égard du traitements des données à caractère personnel*. Again, though, the date for final adoption of the Bill is uncertain. Ireland, another laggard, has just adopted regulations to amend its data protection legislation and thereby give effect to Arts 4, 17, 25 and 26 of the Directive: see *European Communities (Data Protection) Regulations* of 2001, in force 1.4.2002. A Bill to amend the remainder of its legislation in conformity with the Directive is currently before the Irish Parliament: see *Data Protection (Amendment) Bill 2002*, introduced 25.2.2002.

45 S Simitis, U Dammann & M Körner (eds), *Data Protection in the European Community: The Statutory Provisions* (Baden-Baden: Nomos, 1992, loose-leaf, continuously updated).

46 W Madsen, *Handbook of Personal Data Protection* (London: Macmillan, 1992).

The term *information* refers to a human, cognitive product that depicts (informs us about) a set of phenomena for a given set of purposes. This is a simplified definition of what is a very complex, multi-layered concept.[47]

The term *data* is used interchangeably in the book with the term information. This is in keeping with the bulk of discourse on data protection law, though the terms are not always regarded as synonymous in other contexts.[48] Conflation of the notions of data and information tends to have little practical significance in the field of data protection law. Indeed, it is artificial and unnecessarily pedantic in most legal contexts to maintain a division between the two notions, as such a division is usually difficult to maintain in practice.[49] Nevertheless, insofar as conflation of the concepts of data and information is a result of muddled thinking, their continued conflation can do little to alleviate public confusion over their precise meanings and inter-relationship. Both concepts are complex, vague and open to a profusion of definitions. This could sometimes have unintended, if not unfortunate, regulatory consequences.

The term *information system* is employed in this book in basically the same way as it is defined by the OECD in Part III of its *Guidelines for the Security of Information Systems*. Thus, an information system encompasses computer and communication facilities and networks, and data/information processed by them, including programs, specifications and procedures for their operation. Expressed a little differently, an information system refers to the technical infrastructure that facilitates and structures the processing of data/information. Just as the distinction between data and information is difficult to draw in practice, so too are the borderlines between one information system and another such system.

---

47 For a fuller analysis upon which this definition is based, see W Steinmüller, *Informationsteknologie und Gesellschaft* (Darmstadt: Wissenschaftliche Buchgesellschaft, 1993), chapt II.

48 In the fields of computer and information science, data often refers to signs, patterns, characters or symbols which become information only when interpreted. In other words, data are treated as 'potential information', and information as 'data communicated and understood': J Bing, 'Information Law?' (1982) 2 *J of Law and Media Practice*, 219, 221–223. Cognizance of this distinction is beginning to occur in the development of security policies for information systems: see, eg, Organisation for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems* (Paris: OECD, 1992), Part III.

49 J Bing, 'En bakgrunn for analyse av informasjonsrettslige bestemmelser' (1988) *Jussens Venner*, 109, 111–112. See also Steinmüller, *supra* n 47, 353–354. Not all jurists, however, merge the two concepts: see, eg, Seipel, *supra* n 19, 345 & 348. The decision of the House of Lords in *R v Brown* [1996] 1 All ER 545 arguably demonstrates that attempts by legislators to maintain a distinction between the two concepts can sometimes be more confusing than helpful. In this case, the court was drawn into a lengthy and complicated discussion of the relationship between 'data' and 'information' in the UK *Data Protection Act* of 1984 on account of the legislation distinguishing partially between the two concepts. The case turned, though, on the meaning of the term 'use' in the Act, with the House of Lords (by a three-to-two majority) finding that a person who simply gains access to personal data by calling those data on to a computer screen and viewing them, does not 'use' the data within the meaning of s 5(2)(b) of the Act. For further detail, see, eg, J Morton, 'Data Protection and Privacy. R v Brown' [1996] 18 *EIPR*, 558–561.

Closely related to the concept of information system (as defined above) is the term *information technology*. This term is used here to denote a set of tools for the processing (including capture, storage and communication) of data/information. In this book, the tools making up information technology are viewed broadly. They embrace all of the technical infrastructure making up an information system. Accordingly, an information system is a discrete unit or set of information technology. At the same time, the latter also embraces the knowledge that facilitates the construction and operation of information systems.

Another diffuse pair of terms used frequently in the book and in data protection discourse generally, are *data subject* and *data controller*. A data subject is the person or organisation to whom/which data relate.[50] A data controller is a person or organisation who/which determines the purposes and means of data processing.[51] These are the central types of actors in relation to any set of data/information. There are at least two others as well: *data processors* and *data users*. A data processor is a person or organisation who/which actually carries out the processing (including collection, registration and storage) of data, while a data user is a person or organisation who/which receives data and applies these for various purposes.[52]

In practice, the distinction between the above categories of actors is not hard and fast. In relation to many sets of data/information, the data controller functions also as the data processor and chief data user. Further, data controllers, data processors and data users are by and large data subjects in relation to other sets of data/information. It should also be noted that, in practice, determining who or what is the controller with respect to a particular data-processing operation will not always be easy, particularly within large corporate structures and in the context of electronic communications networks.

As for the term *data protection*, this is employed in the book as the primary adjective for legislation containing all or most of the groups of principles on information processing set out above in section 1. However, I also employ the term on its own to denote a type of activity or field of operations which might or might not involve legal measures. In other words, data protection *per se* is not viewed as inextricably legal in character. Although the concept of data protection has tended to be linked primarily to a type of legislation that emerged in the 1970s, it has now achieved a level of generality in usage which goes beyond such legislation. For the

---

50 See also Art 2(a) of the 1995 EC Directive on data protection (hereinafter termed 'EC Directive') which defines 'personal data' as 'any information relating to an identified or identifiable natural person ('*data subject*') ...' (emphasis added).

51 See also Art 2(d) of the EC Directive which defines 'controller' as the 'natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'. It should be stressed that a 'controller' (or 'data controller' in my terminology) need not be in possession of personal data; the crucial criterion is control.

52 Cf Art 2(e) of the EC Directive which denotes a 'processor' as a person or organisation engaged in processing of personal data 'on behalf of' a data controller. Article 2(g) of the Directive uses the term 'recipient' to refer to a person or organisation to whom/which personal data are disclosed.

purposes of this book, a general definition of data protection is as follows: a set of measures (legal and/or non-legal) aimed at safeguarding persons from detriment resulting from the processing (computerised and/or manual) of information on them, and embodying all or most of the groups of principles on processing of personal information set out above in section 1. This does not mean that measures based on these principles are treated as *exclusively* constitutive of data protection. Rather, they are a baseline which can be expanded upon in line with technological and policy developments. As for the reference to 'persons' in the above definition, this primarily denotes individual physical/natural persons. Nevertheless, I view the notion of data protection as sufficiently broad to cover the interests of collective entities as well.[53]

The definition of data protection advanced here is not dissimilar to definitions advanced by other legal scholars.[54] Sometimes, though, the concept of data protection is defined as relating only to *legal* measures directed at *computerised* processing of personal data.[55]

A distinction is maintained in the book between data protection and *data security*. The notions are easily confused, being closely related etymologically, and touching upon overlapping issues. The term 'data protection' has its origins in the German term 'Datenschutz', which is derived in turn from the notions of 'Datensicherung' and 'Datensicherheit' (data security). A great deal of the German discourse on data protection issues was initially framed around the latter notions. However, after much discussion, the notions of 'Datensicherung' and 'Datensicherheit' were found not to capture all aspects of these issues, and the term 'Datenschutz' was consequently coined.[56] In some fields, such as database management, there is still a tendency to conflate data protection with data security.[57] Paul Schwartz and Joel Reidenberg also note that the notion of data protection in the USA often 'evokes intellectual property principles of copyright and trade secrets as well as technological security measures'.[58]

---

53 See generally Part III.

54 See, eg, Steinmüller, *supra* n 47, 467 (defining data protection as the multitude of measures for protecting data subjects from the socially undesirable effects of being made a data subject).

55 See, eg, FW Hondius, *Emerging Data Protection in Europe* (Amsterdam: North Holland, 1975), 1.

56 S Simitis, '§ 1', in S Simitis, U Dammann, H Geiger, O Mallmann & S Walz, *Kommentar zum Datenschutzgesetz* (Baden-Baden: Nomos, 1992, 4th ed, looseleaf), para 2.

57 See, eg, CJ Date, *An Introduction to Database Systems* (Reading, Massachusetts: Addison-Wesley, 1995, 6th ed), 373. Charles Raab claims that the conflation of data protection with data security is 'frequently encountered in organisational circles, including policing': CD Raab, 'Police Cooperation: The Prospects for Privacy', in M Andersen & M den Boer (eds), *Policing Across National Boundaries* (London/New York: Pinter, 1994), 121, 124.

58 PM Schwartz & JR Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Charlottesville, Virginia: Michie Law, 1996), 5. These and the immediately preceding observations highlight some of the problems involved in using 'data protection' as the primary nomenclature for the body of laws, policy and discourse with which this book is mainly concerned. For an elaboration of such problems, see LA Bygrave, 'An international data protection stocktake @ 2000 – Part 4: The issue of nomenclature' (2002) 9 *PLPR* (forthcoming).

Nevertheless, data security (and related terms, such as information security or information systems security) are viewed in this book as pertaining to a broader range of concerns than data protection. Whereas the primary goal of the latter is protection of data subjects in the name of personal privacy, freedom and integrity, data security is also very much concerned with safeguarding the interests of controllers, processors and users of all kinds of data (not just personal data) in the name of, *inter alia* (hereinafter abbreviated to 'ia'), national security, commercial profit or administrative efficiency. Data security measures are mainly directed to ensuring that data are processed in accordance with the expectations of those who steer or use a given information system.[59] The chief sub-goals for these measures are maintenance of the confidentiality, integrity/quality and availability of information in an information system as well as appropriate protection of the system itself.[60] In many instances, these measures serve to promote data protection, but they can obviously also come in conflict with the latter.

The term *privacy* is, unless otherwise stated, employed in this book to denote a condition or state in which a person (or collective entity) is more or less inaccessible to others, either on the spatial, pyschological or informational plane. This usage of privacy best accords with my own intuition as to the proper ambit of the term and it accords with definitions advanced by several other legal scholars.[61] Privacy as such is not viewed in the book as a right or claim. Neither is it viewed as a form of autonomy; eg, a person's capacity to control the flow of information about him-/herself to others. Of course, privacy can *result* from the exercise of such control, and vice-versa, but privacy and autonomy are held here as conceptually distinct.[62] Privacy is also to be distinguished from secrecy, which is best defined in Sissela Bok's terms of 'intentional concealment'.[63] Again, though, as with autonomy, secrecy can be a means of safeguarding privacy, just as privacy can help to maintain secrecy.

The reference to 'more or less' in my definition of privacy is to underline that privacy is always a matter of degree. As Ruth Gavison notes, '[t]he possession or enjoyment of privacy is not an all or nothing concept ... and the total loss of privacy is as impossible as perfect privacy'.[64]

---

59 See also Steinmüller, *supra* n 47, 472. Cf Steinmüller's more simplistic formulation that whereas data protection protects *against* data processing, data security simply *protects* data processing: *id*.

60 See, eg, Nordic Council of Ministers, *Information Security in Nordic Countries*, Nordiske Seminar- og Arbejdsrapporter 1993:613 (Copenhagen: Nordic Council of Ministers, 1994), 12.

61 See further *infra* n 494 and references cited therein.

62 In much discourse on data protection, though, the notion of privacy is defined in terms of informational control: see further Chapter 7 (section 7.2.1).

63 S Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Pantheon, 1982), 5ff.

64 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale LJ*, 421, 428. In this regard, O'Brien distinguishes between 'inevitable' and 'contingent' privacy. Inevitable privacy arises from an ontological limitation on the ability of humans to communicate or disclose *all* aspects of themselves; it is this limitation that prevents total loss of privacy. Contingent privacy, however, 'relates to what

It should also be emphasised that, unlike some scholars, I do not limit my usage of privacy to apply only to those aspects of persons' lives that are considered as intimate. Thus, for the purposes of this book, the disclosure of any type of information about a person will constitute a reduction in that person's privacy. Nevertheless, the nature of the information disclosed will determine, at least in part, the *significance* of the reduction in privacy for the person concerned. It may, for instance, partially determine whether we talk of 'violating' privacy or its mere 'loss'.

As indicated above, a distinction is maintained in the book between privacy and *autonomy*. The latter notion is treated here as broadly synonymous with self-determination. Thus, unless otherwise stated, autonomy is to be understood as denoting a person's capacity to live his/her life in accordance with his/her own wishes. An autonomous person is one who is the instrument of his/her own will, not the will(s) of others. Autonomy works not just at the level of action but at the level of reflection and motivation. It involves a person's capacity to reflect independently upon his/her motivational structure and to change that structure.[65]

Closely connected with both privacy and autonomy is the notion of *integrity*. The latter notion is used in the book to denote a person's state of intact, harmonious functionality based on other persons' respect for him/her. Thus, a breach of integrity involves disruption of this functionality by the disrespectful behaviour of others.[66] Just as there are different degrees of autonomy and privacy, so too are there various degrees of integrity (as defined here).

The term *dignity* is used here to denote the intrinsic worth of a person. The adjective 'intrinsic' is intended to connote a worth which inheres in a person on the basis of his/her humanity and which thus arises partially independent of the attitudes of either that person or others. At the same time, the notion of 'worth' (like that of 'quality' – see below) has a subjective dimension; ie, worthiness is partly a product of persons' attitudes even though, once established, it can stand as a kind of 'fact' relatively unaffected by personal whim.[67] Because of this subjective dimension, there is the possibility that dignity can increase and decrease in accordance with persons' attitudes (though the criterion for its impartation cannot).[68] Nevertheless, dignity has

---

(Cont.)
individuals choose to disclose (or not to disclose) about themselves ... and to the circumstances that impose limits on access to individuals'. See DM O'Brien, *Privacy, Law, and Public Policy* (New York: Praeger, 1979), 17. It is, of course, with contingent privacy that this book, and law and social policy generally, are concerned.

65 G Dworkin, *The Theory and Practice of Autonomy* (Cambridge: Cambridge University Press, 1988), 108.

66 This understanding of integrity builds upon the term's etymological roots in Latin: the prefix 'in' negating the verb 'tangere' (touch).

67 See also M Hailer & D Ritschl, 'The General Notion of Human Dignity and the Specific Arguments in Medical Ethics', in K Bayertz (ed), *Sanctity of Life and Human Dignity* (Dordrecht/Boston/London: Kluwer Academic, 1996), 91, 103–104.

68 See also A Kolnai, 'Dignity', in RS Dillon (ed), *Dignity, Character, and Self-Respect* (New York/London: Routledge, 1995), 53, 61–62, 75.

the potential of being prescribed as an irreducible constant within the confines of one agreed, normative system.[69]

Regarding the term *interest*, this is used to denote a concern (desire) to achieve a particular (valued) state of affairs. As such, an interest is rooted in needs (physiological and/or psychological),[70] though it is not the same as them. In my view, needs give stimulus to an interest or set of interests; put crudely and somewhat misleadingly, needs 'push' interests. If interests can be said to be pushed by needs then the 'pulling' is done by *values*, which constitute the focal point of interests.[71] Values here are defined as objects or conditions to which satisfaction is attached.[72] Under this terminological set-up, privacy *per se*, for instance, is an example of a value as opposed to an interest. When the book refers to an interest in privacy, it refers to a concern or desire to bring about a state of privacy (ie, limited accessibility). At the same time, though, this distinction between interests and values has little practical significance for the discussion in the book.

The final term in special need of clarification is *information quality*. For the purposes of the book, information quality refers to various characteristics or attributes of information which bear on the worth of the latter for given purposes and given persons. This notion of quality encompasses also attributes or characteristics of the relationship between various sets of data, information and information systems. However, the notion of quality *per se* is not employed here to express a judgement about the actual value, worth or utility of information relative to other information.[73]

---

69 See, eg, Art 1(1) of Germany's *Basic Law* (*Grundgesetz*) of 1949: 'Human dignity ['Die Menschenwürde'] shall be inviolable. To respect and protect it shall be the duty of all State authority'. Cf Art 1 of the *Universal Declaration of Human Rights* of 1948: 'All human beings are born free and equal in dignity and rights …'.

70 See also A Ross, *On Law and Justice*, trans M Dutton (London: Stevens & Sons Ltd, 1958), 358; originally published as *Om ret og retfærdighed: en indførelse i den analytiske retsfilosofi* (Copenhagen: Nyt Nordisk Forlag, 1953).

71 Cf the analytical framework drawn up by Kaarlo Tuori, who sees values as 'transforming' needs into interests: K Tuori, 'Interests and the Legitimacy of Law', in A Aarnio *et al* (eds), *Rechtsnorm und Rechtswirklichkeit. Festschrift für Werner Krawietz zum 60. Geburtstag* (Berlin: Duncker & Humblot, 1993), 625.

72 See also V Aubert, *Sosiologi 1. Sosialt samspill* (Oslo: Universitetsforlaget, 1981, 2nd ed), 62.

73 Further on the concept of information quality, see LA Bygrave, 'Ensuring Right Information on the Right Person(s): Legal Controls of the Quality of Personal Information – Part I', Manuscript Series on Information Technology and Administrative Systems, University of Oslo, 1996, vol 4, no 4.

PART I
OVERVIEW OF DATA PROTECTION LAWS

2. Aims and Scope of Data Protection Laws

2.1 Introduction

This part surveys the content of legal (and some non-legal) instruments on data protection on both international and domestic planes. The presentation here is aimed at fleshing out the short description of data protection laws' distinguishing features given in Chapter 1. It is not intended to provide an exhaustive analysis of data protection laws; rather, it is intended to sketch these laws' central, primarily *formal* characteristics so as to create a platform for closer analysis of their rationale, logic and limits in the remainder of the book.

Part I leaves largely unexamined the now considerable number of data protection instruments that are of sectoral application only.[74] This is because their basic principles are broadly similar to, and largely derived from, the principles set down in the generally applicable instruments. Also left unexamined are the rules governing national data protection laws' territorial reach and concomitant choice-of-law problems as such issues are marginal to the focus of the book.[75]

This chapter surveys the aims and ambits of data protection laws, using three international instruments on data protection as primary points of reference (see section 2.2). It looks first at data protection laws' respective aims (section 2.3), then at their respective ambits (section 2.4).

---

74 See, eg, *Directive 97/66/EC of the European Parliament and of the Council of 15.12.1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector* (OJ L 24, 30.01.1998, 1) – hereinafter termed 'EC Directive on telecommunications privacy'; the code of practice issued by the International Labour Organisation (ILO) on protection of workers' personal data – ILO, *Protection of Workers' Personal Data* (Geneva: ILO, 1997); and the various sectoral recommendations of the Council of Europe (CoE) some of which are listed in the Bibliography (part B).

75 For more detailed analysis of these issues, see, eg, R Ellger, *Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisions-rechtliche Untersuchung* (Baden-Baden: Nomos, 1990), chapt IV; ACM Nugter, *Transborder Flow of Personal Data within the EC* (Deventer: Kluwer Law and Taxation, 1990), chapt VII; M Bergmann, *Grenzüberschreitende Datenschutz* (Baden-Baden: Nomos, 1985), chapt 7; LA Bygrave, 'Determining Applicable Law pursuant to European Data Protection Legislation' (2000) 16 *CLSR*, 252–257.

2.2 Primary Points of Reference

The emergence of data protection laws is recent. The first pieces of legislation in the field were not enacted until the early 1970s. At present, however, a large range of legal and quasi-legal instruments on data protection are to be found. There are now well over thirty countries which have enacted data protection statutes at national or federal level, and the number of such countries is steadily growing. Various legal instruments on data protection have also been introduced at the international plane and provincial and municipal levels.

To describe even briefly each of these instruments one after the other would make for an exceedingly long exegesis. It would also be tedious since, as shown further on, these instruments are broadly similar on a large number of points. Hence, three international data protection instruments are used as primary points of reference in this chapter and the other chapters in Part I. These instruments are:

1) the CoE *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (hereinafter termed 'CoE Convention'),[76] adopted by the CoE Committee of Ministers on 28.1.1981;
2) the EC *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (hereinafter termed 'EC Directive'),[77] adopted by the European Parliament and the Council on 24.10.1995; and
3) the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (hereinafter termed 'OECD Guidelines'),[78] adopted by the OECD Council on 23.9.1980.

These instruments are focused upon for two main reasons. First, they contain relatively clear distillations of the basic principles of data protection which are present (though not always obvious) in domestic data protection laws. Secondly, they serve as influential models for national and international initiatives on data protection.

The EC Directive is the most comprehensive and complex of the instruments. It constitutes also the most important point of departure for new data protection initiatives, both in and outside the EU. Member States of the EU were given until 24.10.1998 to bring their respective legal systems into conformity with the provisions of the Directive (see Art 32(1) of the latter).[79] Although the Directive's scope is

---

76 ETS No 108.

77 Directive 95/46/EC (OJ L 281, 23.11.1995, 31).

78 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980).

79 Some types of data processing, however, do not have to be regulated in conformity with the Directive until after this date. Data processing already underway at the time when a Member State adopts new legislation to comply with the Directive, need not be subject to this legislation until 24.10.2001

delimited in several major respects,[80] its general thrust is to establish a set of rules capable of broad application and impact. The Directive and later EC legislation on data protection also apply to the processing of personal data by the Community's own institutions as of 1.1.1999.[81] Further, the Directive was incorporated on 25.6.1999 into the 1992 *Agreement on the European Economic Area* (EEA) such that States which are not members of the EU but party to the EEA Agreement (ie, Norway, Iceland and Liechtenstein) are legally bound to bring their respective laws into conformity with the Directive. The Directive exercises additionally some political and legal influence over other countries outside the EU not least because it prohibits (with some qualifications) the transfer of personal data to these countries unless they provide 'adequate' levels of data protection (Arts 25–26).[82] Accordingly, the following presentation treats the Directive in considerably more detail than the other international instruments.

Despite adoption of the Directive, study of the CoE Convention and OECD Guidelines remains important as they have influenced and embody the basic principles of most countries' current data protection laws along with the Directive

---

(Cont.)

(Art 32(2)). With respect to personal data already held in manual filing systems at the time the new legislation is adopted, the processing of such data need not be brought into conformity with Arts 6–8 in the Directive until 24.10.2007, though this is not to prevent data subjects from exercising their rights set down in other provisions of the Directive, with respect to such data (Art 32(2)). The processing of data kept solely for the purpose of historical research need never be brought into conformity with Arts 6–8 of the Directive, as long as 'suitable safeguards' are in place (Art 32(3)).

80 Most importantly, the Directive does not apply to data processing carried out as part of activities falling beyond the ambit of EC law – eg, 'processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law' (Art 3(2)). This delimitation is reinforced in Art 13(1) which permits Member States to restrict the scope of some of the central rights and obligations laid down by the Directive insofar as the restriction is necessary to safeguard, ia, 'national security', 'defence', 'public security' or 'the prevention, investigation, detection and prosecution of criminal offences …': see further Chapter 18 (section 18.4.6). Moreover, none of the Directive applies to data processing by a natural person 'in the course of a purely personal or household activity' (Art 3(2)): see further section 2.4.3 below. Finally, Art 9 of the Directive requires Member States to lay down exemptions from the central provisions of the Directive with respect to data processing 'carried out solely for journalistic purposes or the purpose of artistic or literary expression', insofar as is 'necessary to reconcile the right to privacy with the rules governing freedom of expression': see further Chapters 2 (section 2.4.3) and 18 (section 18.4.6).

81 See Art 286(1) of the 1957 *Treaty establishing the European Community* (hereinafter termed 'EC Treaty'). See also Art 286(2) which requires the Council to have established by 1.1.1999 an independent agency to monitor application of this legislation to EC institutions. The requirements of Art 286 are given effect by *Regulation (EC) 45/2001 of the European Parliament and of the Council of 18.12.2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data* (OJ L 8, 12.1.2001, 1).

82 See further Chapter 4 (section 4.4).

itself.[83] The Convention is the hereto sole international treaty dealing specifically with data protection. It entered into force on 1.10.1985. As of 23.5.2002, it had been ratified by 27 CoE Member States.[84] The Convention is potentially open for ratification by States that are not members of the CoE (Art 23); concomitantly, it is also envisaged to be potentially more than an agreement between European States.[85] As yet, though, it has not been ratified by any non-Member State. While accession to the Convention is presently open only for States proper,[86] the EC itself has signalled a wish to accede to the Convention in the near future, and moves are underway to amend the Convention so that the wish may be met.[87]

As for the OECD Guidelines, while not legally binding on OECD Member States,[88] they have been highly influential on the enactment and content of data protection legislation in non-European jurisdictions, particularly Japan, Australia, NZ and Hong Kong.[89] In North America, the Guidelines have been formally endorsed by

---

83 Regarding the latter, see, eg, recital 11 of the Directive which states that the data protection principles in the Directive 'give substance to and amplify' the principles of the Convention.

84 See <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=>.

85 Hence, the Convention is not entitled 'European Convention': see *Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (hereinafter 'Explanatory Report')(Strasbourg: CoE, 1981), para 24.

86 See further F Henke, *Die Datenschutzkonvention des Europarates* (Frankfurt am Main: P Lang, 1986), 66 and references cited therein.

87 Appropriate amendments to the Convention were adopted on 15.6.1999 by the CoE Committee of Ministers (see *Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede*) and will enter into force on the thirtieth day after approval by all of the Convention Parties (Art 21(6) of the Convention). As of 23.5.2002, 20 Parties had registered their approval. The competence of the EC to accede to the Convention is questionable given that the European Court of Justice (ECJ) has held that the EC does not have the competence to accede to the European Convention on Human Rights on the basis of Art 308 (formerly 235) of the EC Treaty. According to the Court, '[a]ccession to the Convention [ECHR] would ... entail a substantial change in the present Community system for the protection of human rights in that it would entail the entry of the Community into a distinct international institutional system as well as integration of all the provisions of the Convention into the Community legal order. Such a modification ... with equally fundamental institutional implications for the Community and for the Member States would be of constitutional significance and would therefore be such as to go beyond the scope of Article 235 [now 308]': Opinion 2/94 of 28.3.1996, reported in [1996] ECR I-1759, paras 34–35. However, the impact of this ruling on the legal viability of accession to the CoE Convention is lessened by the fact that the institutional framework set up by that Convention, along with its institutional implications for the EC, are extremely modest in comparison with the framework established by the ECHR.

88 The Recommendation of 23.9.1980 issued by the OECD Council in tandem with the Guidelines' adoption states simply that Member States are to take account of the Guidelines when developing domestic legislation on privacy and data protection.

89 For example, the Preamble to Australia's federal *Privacy Act* of 1988 lists the Guidelines and the accompanying OECD Council Recommendation as part of the reasons for the passing of the Act. Similarly, the Preamble to New Zealand's *Privacy Act* of 1993 states that the Act is to 'promote and protect individual privacy in general accordance with the Recommendation [of the OECD Council] ...'.

numerous companies and trade associations.[90] They have additionally constituted the basis for the first comprehensive set of data protection standards to be developed by a national standards association: the Model Code for the Protection of Personal Information, adopted by the Canadian Standards Association (CSA) in March 1996.[91]

Some account is also taken in this and the following chapters of a fourth international instrument: the United Nations' (UN) *Guidelines Concerning Computerized Personal Data Files* (hereinafter termed 'UN Guidelines'),[92] adopted by the UN General Assembly on 14.12.1990. The Guidelines are intended to encourage those UN Member States without data protection legislation in place to take steps to enact such legislation based on the Guidelines. The Guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal data in a responsible, fair and privacy-friendly manner. The Guidelines are not legally binding and seem to have had little practical effect relative to the other three international instruments on data protection canvassed in this chapter. Indeed, the Guidelines tend to be overlooked in much data protection discourse, at least in Scandinavia.[93] This is unfortunate as their adoption demonstrates that concern for data protection can no longer be assumed as confined to the Western democracies of the so-called First World. Moreover, as shown further on, the UN Guidelines do not merely repeat what is set out in other international instruments on data protection but supplement some of these instruments in several respects.

When considering both the descriptive and prescriptive character of the above instruments with respect to domestic data protection laws, two related points need to be kept in mind. First, all of the above instruments give the States to which they are addressed a significant amount of leeway in terms of how their rules are to be implemented in national legislation. This is obviously the case with the two sets of

---

90 See, eg, RM Gellman, 'Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions' (1993) VI *Software LJ*, 199, 230. Gellman notes, though, evidence suggesting that few of these corporations had (at the time of writing his paper) actually put into practice policies implementing the Guidelines: *ibid*, 232–233.

91 CSA, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (Rexdale, Ontario: CSA, 1996). The Model Code has been incorporated into Canadian legislation as Schedule 1 to the *Personal Information Protection and Electronic Documents Act* of 2000.

92 Doc E/CN.4/1990/72, 20.2.1990. On the background to the Guidelines, see, eg, J Michael, *Privacy and Human Rights. An International and Comparative Study, with Special Reference to Developments in Information Technology* (Paris/Aldershot: UNESCO/Dartmouth Publishing Company, 1994), 21–26.

93 A case in point is the tome produced by Sweden's Data Act Committee (Datalagskommittén): see *Integritet – Offentlighet – Informationsteknik*, SOU 1997:39. No reference is made to the UN Guidelines in this report despite analysis of other international data protection instruments in its chapters 3 and 4. Similar omissions occur in Peter Blume's standard Danish works on data protection: see P Blume, *Personregistrering* (Denmark: Akademisk forlag, 1996, 3rd ed), particularly chapter 4; *Databeskyttelsesret* (Copenhagen: Jurist- og Økonomforbundets Forlag, 2000).

Guidelines since neither are legally binding. Yet also the two other instruments allow for flexibility. The CoE wanted its data protection Convention to be a catalyst and guide for States' legislative initiatives rather than to short-circuit these initiatives by providing a completed package of directly applicable, material rules.[94] Thus, the Convention is not intended to be self-executing. Article 4(1) of the Convention simply obliges Contracting States to incorporate the Convention's principles into their domestic legislation; 'individual rights cannot be derived from it'.[95] It should also be noted that the Convention does not establish a body to enforce its implementation. Moreover, it allows for derogations on significant points (see, eg, Arts 3, 6 and 9 described further below). This seriously hampers its ability to harmonise the data protection regimes of the Contracting States.[96]

Similarly, in accordance with the principle of subsidiarity, EU Member States have been allowed a margin for manoeuvre in implementing the Directive. This follows partly from the status of the Directive *qua* directive (as opposed to regulation).[97] Directives are legally binding only in terms of result; how the result is to be reached is up to the Member States to determine. In practice, though, the amount of such discretion is dependent on each directive's objective and level of detail.[98] Regarding the data protection Directive, its aim of bringing about harmonisation of national data protection regimes[99] should narrow the amount of discretion accorded Member States in terms of how it is to be implemented. Nevertheless, key provisions in the Directive expressly provide States a considerable margin for manoeuvre.[100] As a result of this margin, recital 9 in the Directive's preamble recognises that 'disparities could arise in the implementation of the Directive'.[101] This is despite the assumption (also expressed in recital 9) that the

---

94 S Simitis, 'Datenschutz und Europäischer Gemeinschaft' (1990) 6 *RDV*, 3, 9–10; Henke, *supra* n 86, 57–60.

95 Paragraph 38 of the Convention's Explanatory Report; see also para 60. Cf Rainer Schweizer's argument that substantial elements of the Convention (particularly in Arts 5 & 8) can and should be treated as self-executing given that they are formulated sufficiently clearly to function as directly applicable rights and duties, and given the objects clause in Art 1: see R Schweizer, 'Europäisches Datenschutzrecht – Was zu tun bleibt' (1989) *DuD*, 542, 543. The argument has much to commend it in terms of *lex ferenda* but in light of Art 4(1) and the Convention's Explanatory Report, its validity in *lex lata* terms is doubtful.

96 See generally Nugter, *supra* n 75, chapt VIII.

97 On the status of directives and regulations, see generally TC Hartley, *The Foundations of European Community Law* (Oxford: Clarendon Press, 1998, 4th ed), 196ff.

98 *Ibid*, 204–205 and references cited therein.

99 See especially recital 8. See further section 2.3.

100 See particularly Art 5 which provides that 'Member States shall, within the limits of the provisions of [Chapt II] determine more precisely the circumstances in which the processing of personal data is lawful'. See also recital 9. Examples of points in Chapt II of the Directive where Member States are given an obvious margin for manoeuvre are Arts 7(f), 8(4), 10, 11, 13 and 14(a). The provisions are described in Chapters 3 and 18.

101 It might be more accurate to describe such disparities as not merely possible but probable. See Simitis, *supra* n 6, 449 ('Experience has shown that the primary interest of the Member States is not

Directive's implementation will bring about an 'approximation' of national laws resulting in 'equivalent' levels of data protection across the Member States.

The second point is that many of the provisions in the international data protection instruments are diffuse with little authoritative guidance on how they are to be interpreted. The substantive provisions of the EC Directive have yet to be analysed by the ECJ. Case law of the European Court of Human Rights (ECtHR) and of the now abolished European Commission of Human Rights (ECommHR) has scarcely touched specifically upon the provisions of the CoE Convention, though breaches of the Convention's core principles could constitute in many cases interference with the 'right to respect for private life' provided under Art 8 of the ECHR.[102] That same case law will also play a part in determining the meaning of the provisions in the EC Directive, given that the ECHR provides much of the Directive's normative basis.[103]

Only the OECD Guidelines and CoE Convention have been issued with explanatory memoranda but these are thin at numerous points. Moreover, the memorandum ('Explanatory Report') for the Convention is prefaced with a disclaimer stating that '[t]he report does not constitute an instrument providing an authoritative interpretation of the text of the Convention, though it might be of such nature as to facilitate the understanding of the provisions contained therein'. Thus, caution needs to be exercised when using that report to resolve ambiguities in the Convention's text.

The same applies when attempting to resolve such ambiguities through recourse to the various sectoral recommendations on data protection which have been adopted by the CoE Committee of Ministers in the wake of the Convention. This is not to say that these recommendations are without *any* relevance for interpreting the Convention. One of their express aims is to provide guidance on how to apply the

---

(Cont.)
to achieve new, union-wide principles, but rather to preserve their own, familiar rules. A [*sic*] harmonization of the regulatory regimes is, therefore, perfectly tolerable to a Member State as long as it amounts to a reproduction of the State's specific national approach').

102 Some of the language used in the CoE Convention (see espec Art 1 of the CoE Convention, set out in section 2.3), as well as some of the case law developed by the ECtHR and ECommHR (see LA Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *Int J of Law and Information Technology*, 247, 254ff) give solid grounds for treating the main principles of the CoE Convention as a detailed enumeration of the protection provided by Art 8 of the ECHR: see also Chapter 6 (section 6.4.1). At the same time, in light of the case law on Art 8, one cannot be certain that *all* breaches of the CoE Convention's core principles would necessarily be regarded by the ECtHR as breaches of the ECHR. This point applies especially with respect to the data-processing practices of private (as opposed to State) bodies since the ECtHR has yet to conclusively decide that such practices fall within the ambit of Art 8: see Bygrave, *ibid*, 257–259.

103 See further *infra* nn 133–135 and accompanying text. The influence of ECtHR case law is evidenced in the decision of 12.6.2001 by the Swedish Supreme Court in case B293-00. The Swedish Court drew heavily upon that case law when determining the ambit of s 7 of Sweden's *Personal Data Act* which transposes Art 9 of the EC Directive: see *infra* n 200 and accompanying text.

Convention's provisions in specific contexts. In providing such guidance, they aim also to take account of technological developments. They are drafted by experts in the field, with participation from all CoE Member States. While implementation of the recommendations is not legally required, Member States tend to attribute considerable authority to their provisions.[104] Accordingly, the recommendations may be considered as having more than marginal weight when resolving ambiguities in the text of the Convention. Nevertheless, they can hardly be said to have an absolute determinative weight; they are just one of several relevant interpretative factors.

Also relevant, of course, are the basic principles of treaty interpretation set down in Arts 31–33 of the 1969 *Vienna Convention on the Law of Treaties*. The central principle here is that '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose' (Art 31(1)).

While these principles are not formally binding on the ECJ when it interprets EC legal instruments, contextual and purposive methods of interpretation do play a key role in the Court's jurisprudence. In practice, the ECJ not uncommonly places most weight on what it sees as provisions' object and purpose, giving relatively little attention to the literal meaning of the words used[105] or to the drafters' actual intentions as found in the *travaux préparatoires*.[106] Hence, if called upon to interpret the EC Directive, the Court is likely to devote most energy to ascertaining the Directive's policy thrust and then reading the Directive in the light of this. The Court may have regard to the recitals in this process. As for the Directive's *travaux préparatoires*, despite the Court's minor use of such documents generally, these can be taken into account insofar as they help to clarify textual ambiguity that the recitals otherwise are unable to resolve conclusively,[107] and insofar as they are publicly accessible.[108]

---

104 The authority of the Recommendations is reflected in the fact that when they are adopted, individual Member States frequently issue reservations on contentious points. The recommendations are also highly influential on the policies and practices of national data protection authorities.

105 This proportioning of emphasis is due partly to the multilingual nature of EC legal instruments. The Directive has been issued in the various working languages of the EU, with each version being equally authentic. This means that one cannot look to one single version of the Directive in the event of interpretative difficulties. In the following, I use the English version of the Directive as a point of departure for analysis but take into account also French, German, Danish and Swedish versions as the need arises.

106 See generally Hartley, *supra* n 97, 77ff and references cited therein. See also F Arnesen, *Introduksjon til rettskildelæren i EF* (Oslo: Universitetsforlaget, 1995, 3rd ed), 14, 25ff.

107 Arnesen, *supra* n 106, 14, 44–46.

108 In light of the latter criterion, the Court is unlikely to place weight on the unpublished Council minutes relating to the adoption of the Common Position on the Directive (hereinafter termed 'Council minutes'), despite the inclusion in these minutes of declarations by various Member States, together with the Commission and Council, on how they respectively understand particular provisions of the Common Position. An edited version of the minutes has been made publicly available in Sweden. This version is in Swedish and in a format whereby declarations of Member States other

2.3 Aims

Data protection laws typically express as one of their primary aims the safeguarding of individual persons' right to privacy. The main object of the CoE Convention, for example, is set out in Art 1 as follows:

> 'to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').'

Article 1(1) of the EC Directive is formulated similarly:

> 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.'

On a national plane, the objects clauses and/or titles of the data protection laws (both past and present) of several European countries expressly point to privacy as a fundamental value to be protected by the laws.[109] The privacy protection rationale also figures prominently in the data protection laws of non-European countries. For instance, Australian, Canadian, NZ and United States' (US) data protection statutes enacted at the federal/national level all bear the titles 'Privacy Act' and set down the safeguarding of privacy as one of their basic objects.[110]

However, many European data protection statutes (both past and present) make no explicit reference to the safeguarding of privacy. Of these, some refer instead to other related concepts, such as protection of 'personality',[111] or protection of 'personal integrity'.[112] Other statutes, though, do not contain objects clauses formally specifying a particular abstract interest or value which they are intended to serve.

(Cont.)
than Sweden are anonymised. A Danish version of the declarations disclosed in Sweden has since been published by Peter Blume: see Blume, *Personregistrering*, *supra* n 93, 430ff. To my knowledge, an English version has not been made publicly available.

109 See, eg, Art 2 of Belgium's *Act of 8.12.1992 Concerning the Protection of Personal Privacy in Relation to the Processing of Personal Data* (*Wet van 8 December 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerkung van persoonsgegevens / Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*); and Art 2 of Portugal's *Act no 67/98 of 26.10.1998 on the Protection of Personal Data* (*Lei no 67/98 de 26 de Outubro 1998, da Proteccão de Dados Pessoais*).

110 See the preambles to the Australian and New Zealand Acts, s 2 of the Canadian *Privacy Act* of 1982, and s 2(b) of the US *Privacy Act* of 1974.

111 See Art 1 of Switzerland's *Federal Law of 19.6.1992 on the Protection of Data* (*Loi fédérale du 19 juin 1992 sur la protection des données / Bundesgesetz vom 19 Juni 1992 über den Datenschutz*). Cf Art 1(1) of Germany's *Federal Data Protection Act* (stipulating the purpose of the Act as safeguarding the individual from interference with his/her 'personality right' ('Persönlichkeitsrecht')).

112 See s 1 of Sweden's *Personal Data Act* of 1998 (*Personuppgiftslagen*, SFS 1998:204).

This is the case, for instance, with the national data protection statutes of Denmark and the UK.[113] It is also the case with the first data protection statutes of Sweden, Norway and Iceland.[114] Nevertheless, references to such interests or values emerge in other provisions of some of the Scandinavian countries' data protection laws,[115] and/or in some of the preparatory works to these laws.[116]

It is apparent from the above that the objects clauses of data protection laws frequently point to other values than just privacy. At the same time, these values are often left relatively unspecified. Article 1 of the CoE Convention, for instance, refers merely to 'rights and fundamental freedoms'. Article 1(1) of the EC Directive is pitched at a similar level of generality. Such a broad formulation of goals not only provides data protection laws with an extremely large register of values upon which their formal rationale may be grounded, it also serves to strengthen their normative links with the corpus of human rights law. Somewhat paradoxically, though, such broad goal formulation might also belie uncertainty about exactly which interests data protection laws are to serve, other than privacy. A closer analysis of such interests is undertaken in Part II.

The broadest and boldest expression of basic objects at national level is arguably found in s 1 of France's *Law of 6.1.1978 Regarding Data Processing, Files and Individual Liberties*.[117] This provision reads:

> 'Data processing shall be at the service of every citizen. It shall develop in the context of international co-operation. It shall infringe neither human identity, nor the rights of man, nor privacy, nor individual or public liberties.'

---

113 For Denmark, see the *Private Registers Act* of 1978 (*Lov nr 293 af 8 juni 1978 om private registre mv*) and the *Public Authorities' Registers Act* of 1978 (*Lov nr 294 af 8 juni 1978 om offentlige myndigheders registre*) – both of which have been replaced and repealed by the *Personal Data Act* of 2000 (*Lov nr 429 af 31 maj 2000 om behandling af personoplysninger*). The latter statute also lacks an objects clause. For the UK, see both the *Data Protection Act* of 1984 (repealed) and the *Data Protection Act* of 1998. Note that, unless otherwise specified, future references to the UK legislation are to the 1998 Act.

114 For Sweden, see the *Data Act* of 1973 (*Datalagen* (SFS 1973:289)), now repealed. For Iceland, see the *Protection of Personal Records Act* of 1989 (*Lög nr 121 28 desember 1989 um skráningu og medferd persónuupplýsinga*), now repealed. For Norway, see the *Personal Data Registers Act* (PDRA) of 1978, now repealed. Cf the new Norwegian *Personal Data Act* of 2000 which contains an objects clause (s 1) stipulating that the purpose of the legislation is to protect individuals from violation of their 'privacy protection' ('personvernet') through the processing of personal data. The clause further states that the legislation shall help to ensure that personal data are processed in accordance with 'fundamental privacy concerns' ('grunnleggende personvernhensyn'), including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

115 See, eg, s 3 of Sweden's *Data Act* of 1973 (stipulating that personal files shall only be established if these do not unduly encroach upon the 'personal integrity' of registered persons).

116 See, eg, in relation to Norway's PDRA, Innst O 47 (1977–78), 1 (stating that the legislation is aimed at safeguarding 'personal integrity' ('den personlige integritet')).

117 *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Another relatively comprehensive objects clause was s 1 of Finland's *Personal Data Registers Act* of 1987.[118] This set out the Act's purposes as being '... to protect the privacy, interests and rights of the person, to ensure the security of the State and to maintain good data file practice ...'. The reference to protecting not just the interests of individuals but also those of the State is rare. It has been dropped from the objects clause of the Finnish *Personal Data Act* of 1999[119] which replaced the 1987 legislation.

Express concern for safeguarding interests directly connected with the State is also found in some of the data protection Acts of the German *Länder*. One aim of these Acts is to to preserve State order based on the principle of separation of powers. For example, s 1(2) of the Hessian *Data Protection Act* of 1999[120] sets down as one of its purposes

> 'to safeguard the constitutional structure of the State, in particular the relationship between the constitutional organs of the *Land* and those of local government, based on the principle of separation of powers, against all risks entailed by automatic data processing.'

This declaration is followed up by provisions aimed at maintaining a so-called 'Informationsgleichgewicht' ('informational equilibrium')[121] between the legislature and other State organs in Hesse.[122] Similar provisions are found in the data protection statutes of Rhineland-Palatinate, Berlin and, to a lesser extent, Thuringia.[123]

A major formal aim of *international* data protection instruments is to stimulate the creation of adequate national data protection regimes and to prevent divergence between them. Thus, Art 1 of the CoE Convention ('... to secure in the territory of each Party for every individual, whatever his nationality or residence ...': see above), together with the Convention's Preamble ('Considering that the aim of the Council of Europe is to achieve greater unity between its members...') indicate that the Convention is intended to harmonise Contracting States' respective data protection regimes so that processing of personal data is subject to basically the same rules in all

---

118 *Henkilörekisterilaki / Personregisterlag* (FFS 471/87), now repealed.

119 *Henkilötietolaki / Personuppgiftslag* (FFS 523/99).

120 *Hessisches Datenschutzgesetz vom 7 Januar 1999*.

121 See, eg, Simitis, *supra* n 56, para 17. This 'equilibrium' refers principally to a situation in which the legislature is able to get access to information (personal and/or non-personal) that is available to the executive.

122 See ss 24(2), 38 & 39. This concern has also been present in the earlier data protection legislation of Hesse.

123 For Rhineland-Palatinate, see *Landesdatenschutzgesetz vom 5 Juli 1994*, ss 1(2), 24(6) & 34. For Berlin, see *Datenschutzgesetz vom 17 Dezember 1990*, ss 1(1)(2), 20 & 24(3). For Thuringia, see *Datenschutzgesetz vom 29 Oktober 1991*, s 40(5). Similar provisions were included in the early data protection statutes of Bremen (see *Gesetz zum Schutz vor Misbrauch personbezogener Daten bei der Datenverarbeitung vom 19 Dezember 1977*) and Lower Saxony (see *Datenschutzgesetz vom 17 Juni 1993*) but have since been taken out.

countries concerned.[124] This harmonisation is not only to strengthen data protection and thereby the right 'to respect for private life' pursuant to Art 8 of the ECHR but, somewhat paradoxically, to ensure also the free flow of personal data across national borders and thereby safeguard the right in Art 10 of the ECHR 'to receive and impart information and ideas without interference by public authority and regardless of frontiers'.[125] The latter concern is actualised by the existence in many countries' data protection laws of rules providing for the restriction of data flow to countries without equivalent or adequate levels of data protection.[126]

Similar concerns are manifest in both the OECD and UN Guidelines.[127] However, the concern of the OECD Guidelines in maintaining transborder data flows is specifically linked not so much to a human right in freedom of expression but to the factors of 'economic and social development'.[128] This is in contrast to the CoE Convention and UN Guidelines.[129]

Factors related to economic and social development also figure centrally in the aims of the EC Directive. The Directive's recitals (especially recitals 3, 5 & 7) register a concern to promote realisation of the EU's internal market, in which goods, persons, capital, services and, concomitantly, personal data are able to flow freely between Member States. The need to ensure free flow of personal data is not rooted exclusively in commercial considerations; recital 5 indicates that the pan-EU ambit of government administration plays a role too.

In furtherance of the concern to promote realisation of the internal market, the main function of the Directive is to secure, pursuant to Art 95 of the EC Treaty,[130] harmonisation of Member States' respective data protection laws. It is assumed in recitals 8 and 9 that implementation of the Directive will lead to an 'approximation' of national laws, resulting in 'equivalent' levels of data protection across the EU. With implicit reference to Art 12(3)(a) of the CoE Convention,[131] recital 9 states that the achievement of such equivalency will make it legally impossible for Member States to restrict the free flow of personal data to other Member States 'on grounds

---

124 See too the Convention's Explanatory Report, para 21.

125 See the Convention's Preamble. See further Art 12 of the Convention, described in Chapter 4 (section 4.4).

126 See further Chapter 4 (section 4.4).

127 See paras 17–18 of the OECD Guidelines and Principle 9 of the UN Guidelines each of which seek to minimise restrictions on transborder data flows along broadly similar lines to the CoE Convention. See further Chapter 4 (section 4.4).

128 See the preamble to the OECD Council Recommendation of 23.9.1980 concerning the Guidelines.

129 Work on the UN Guidelines appears to have been inspired mainly by a concern to protect and strengthen human rights in the face of technological advances; purely economic concerns seem to have played a relatively minor role. See generally Michael, *supra* n 92.

130 See the first clause of the Directive's preamble.

131 In essence, this provision allows State Parties to the Convention to restrict, for the purposes of privacy protection, flows of personal data to other State Parties when the latter do not provide 'equivalent' protection for the data concerned. See further Chapters 4 (section 4.4) and 11 (section 11.2.3).

relating to protection of the rights and freedoms of individuals, and in particular the right to privacy'.[132]

At the same time, though, the recitals emphasise the importance of protecting basic human rights, notably that of privacy, in the face of technological and economic developments.[133] Indeed, the Directive is amongst the first Directives to expressly accord a prominent place to the protection of human rights. As such, it reflects and reinforces the gradual incorporation of law and doctrine on human rights into the EU legal system.[134] Also noteworthy here is that the Directive strives to bring about a 'high' level of data protection across the EU.[135] Accordingly, it would be wrong to see the Directive as attempting merely to constitute the 'lowest common denominator' of rules found in Member States' pre-existing laws. Concomitantly, particularly in view of recitals 9 and 10, the Directive leaves open the possibility for Member States to establish or maintain a higher level of data protection than the Directive seeks to establish, as long as this does not derogate from any of the Directive's mandatory requirements.

2.4 Ambit

2.4.1 COVERAGE WITH REGARD TO TYPE OF DATA

Data protection laws' regulatory focus is centred upon 'personal' data or information. Article 2(a) of the CoE Convention defines 'personal data' as 'any information relating to an identified or identifiable individual'. Exactly the same definition is given in para 1(b) of the OECD Guidelines.[136] A similar but more comprehensive

---

132 See further the prohibition on such restrictions in Art 1(2), set out in Chapter 4 (section 4.4).

133 See, eg, recitals 2, 3, 10 & 11.

134 For an overview of this process of incorporation, see, eg, P Craig & G de Búrca, *EU Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 1998, 2nd ed), chapt 7. Note especially the *Treaty on European Union* of 1992, Title I, Art F(1) & (2). Note too the *Charter of Fundamental Rights of the European Union*, adopted 7.12.2000 (OJ C 364, 18.12.2000, 1). Article 7 of the Charter provides for the right to respect for private and family life, while Art 8 provides for a right to protection of personal data.

135 See recital 10 ('Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Fundamental Rights and Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community'). Note also recital 11 (stating that the Directive's data protection principles not only 'give substance to' but also 'amplify' the principles of the CoE Convention) and recital 9 (providing that Member States 'shall strive to improve the protection currently provided by their legislation').

136 Cf the UN Guidelines which surprisingly omit to define their key terms, such as 'personal data' and 'personal data file'. It is safe to assume, though, that these terms are to be defined in much the same way as in the other main international data protection instruments.

definition is provided by Art 2(a) of the EC Directive which defines 'personal data' as

> 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'

Broadly similar definitions of 'personal data' or 'personal information' are found in domestic data protection legislation.[137]

One can read into these definitions two cumulative conditions for data or information to be 'personal': first, the data must relate to or concern a person; secondly, the data must facilitate the identification of such a person. Regarding the first condition, however, there is usually no requirement that the data relate to a particular (eg, private, intimate) sphere of a person's activity. Hence, in most cases, it may not be appropriate to talk of two separate (though cumulative) conditions for making data 'personal'; the first condition can be embraced by the second in the sense that information will normally relate to, or concern, a person if it facilitates that person's identification. In other words, the basic criterion appearing in these definitions is that of identifiability; ie, the potential of information to enable identification of a person.

Six further issues are relevant for determining what is 'personal information' pursuant to data protection laws:

1) What exactly is meant by the concept(s) of identification/identifiability?
2) How easily or practicably must a person be identified from information in order for the latter to be regarded as 'personal'?
3) Who is the legally relevant agent of identification (ie, the person who is to carry out identification)?
4) To what extent must the link between a set of data and a person be objectively valid?
5) To what extent is the use of auxiliary information permitted in the identification process? Is information 'personal' if it allows a person to be identified only in combination with other (auxiliary) information?
6) To what extent must data be linkable to just *one* person in order to be 'personal'?

These issues tend to be inter-related, the answer to one partly determining the answers to the others.

---

137 See, eg, s 6(1) of Australia's federal *Privacy Act* and s 3(1) of the German *Federal Data Protection Act*.

Concept of identification/identifiability

There is little doubt that the ability to identify a person is essentially the ability to distinguish that person from others by linking him/her to pre-collected information of some kind. As such, identification does not require knowledge of a person's name but it does require knowledge of some unique characteristics of the person relative to a set of other persons.[138]

Ease of identification

Few answers are given by the international data protection instruments regarding the issue of requisite ease or practicability of identification. Paragraph 28 of the CoE Convention's Explanatory Report states that an 'identifiable person' pursuant to Art 2(a) of the Convention is one 'who can be *easily* identified: it does not cover identification of persons by means of *very sophisticated* methods' (emphasis added). It is not clear if this statement should be read as introducing two separate criteria (ease and sophistication of methods) or just one (ie, the reference to 'very sophisticated methods' being simply an elaboration of the ease criterion). In any case, the focus on 'sophistication' of methods is problematic as it rests on a misguided perception that as sophistication increases, ease of identification decreases. In reality, enhanced sophistication often results in greater ease of identification. Thus, it is welcome to find that subsequent elaborations of the ease criterion in relation to the CoE's various sectoral recommendations on data protection introduce (more appropriately) the factors of reasonableness, time, resources and, to a decreasing extent, cost.[139]

Recital 26 of the EC Directive lays down a relatively broad and flexible criterion for identifiability:

> 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.'

---

138 See also the following commentary by the EC Commission (COM(92) 422 final – SYN 287, 15.10.1992, 9): 'A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc)'.

139 See, eg, para 1.3 of *Recommendation R (89) 2 on Protection of Personal Data used for Employment Purposes* (adopted 18.1.1989): '…[a]n individual shall not be regarded as 'identifiable' if the identification requires an unreasonable amount of time, cost and manpower'. More recent Recommendations have dropped the reference to 'cost' on account of technological developments. See para 36 of the Explanatory Memorandum to *Recommendation R (97) 5 on the Protection of Medical Data* (adopted 13.2.1997): '… in view of the developments in computer technology, the aspect of 'costs' was no longer a reliable criterion for determining whether an individual was identifiable or not'.

The phrase 'likely reasonably' could be read as introducing two criteria for identifiability: the term 'likely' pointing to an assessment of *probability* of identification; the term 'reasonably' pointing to an assessment of the *difficulty* (eg, in terms of time and resource utilisation) of identification. In practice, however, the two criteria will tend to be interlinked. The French, German and Swedish versions of recital 26 formulate the criteria for identifiability in terms of those means for identification which are *reasonably capable* (as opposed to likely) of being put to use.[140] Nevertheless, it is doubtful that these differences between the recital versions are of real significance as a probability criterion can be read into the notion of reasonableness. It is also doubtful that the Directive's criteria for identifiability are in effect substantially at variance with the criteria laid down in the CoE Recommendations.

As for the OECD Guidelines, these are relatively non-committal on the issue,[141] as are the UN Guidelines.[142] However, both sets of Guidelines most probably embrace criteria for identifiability similar to those read into the EC Directive and CoE Recommendations. Some national laws which expressly qualify degree of identifiability have employed similar criteria as well.[143]

Finally, it should be emphasised that at least for some laws – particularly the Directive – what is of legal importance is the *capability* or *potentiality* of identification rather than the actual achievement of identification. Hence, data will not fail to be personal merely because the data controller refrains from linking them to a particular person.[144]

Legally relevant agent of identification

Closely related to the issue of ease/probability of identification is the issue of who is the legally relevant agent of identification. Most data protection instruments refrain

---

140 The French version refers to '… l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre …'; the German version refers to '… alle Mittel … die vernüftigerweise … eingesetzt werden könnten'); and the Swedish version to 'alla hjälpmedel som … rimligen kan komma att användas …'. Cf the Danish version which expresses the relevant criteria in terms of the means that can reasonably be *thought* to be used ('… alle de hjælpemidler … der med rimelighed kan tænkes bragt i anvendelse …'). The Danish version is probably much the same in effect as the other versions.

141 See para 41 of the OECD Guidelines' Explanatory Memorandum.

142 As noted above, the UN Guidelines fail to define their key terms, such as 'personal data'. It seems safe to assume, though, that these are to be defined in basically the same way as they are defined in the other major international data protection instruments.

143 For instance, a criterion of proportionality applies with respect to the identification process envisaged by Germany's *Federal Data Protection Act* so as to exclude cases where identification is only possible through a data controller making an effort that is 'disproportionate' in relation to his/her/its 'normal' means and activities. This proportionality criterion is derived from s 3(6) of the Act which defines anonymised data in terms of information which 'can no longer or only with a disproportionately great expenditure of time, money and labour be attributed to an identified or identifiable natural person'. See further E Dörr & D Schmidt, *Neues Bundesdatenschutzgesetz: Handkommentar* (Köln: Datakontext-Verlag, 1997, 3rd ed), 26.

144 See further Chapter 18 (section 18.2.1). Cf case law described *infra* nn 168 & 170.

from broaching the latter issue. A notable exception is recital 26 of the EC Directive which indicates that *any* person may be the legally relevant agent for identification. In other words, legally decisive for the Directive is not just the ability of the data controller to link a person to the data but any person's ability to do so.[145] This lowers the threshold for determining the circumstances under which data are personal.

Nevertheless, the criteria for ease/practicability of identification discussed in the preceding paragraphs exclude from consideration any persons who do not employ means that are reasonably capable of being used for identification. The notion of reasonableness implies that account ordinarily should not be taken of persons who are only able to carry out identification by *illegal* means (eg, unauthorised computer hacking).[146] Given that the notion of reasonableness also connotes a probability criterion, account should also not be taken of persons who are only able to carry out identification by (objectively) *unexpected* or *unusual* means. In most cases, illegal means will be unexpected or unusual means but not always. Thus, a situation of conflicting standards might arise (stemming from the one concept!). It goes without saying that neither the Directive nor its *travaux préparatoires* provide guidance on how to resolve this potential conflict. In light of the intention behind the Directive (as manifest in, eg, recital 26) to encourage a broad and flexible approach to the issue of identification and thereby a broad basis for data protection, the probability criterion should be given priority over the legality criterion in the event of conflict; ie, account should be allowed of persons who are able to carry out identification by illegal yet probable means. In practice, assessment of probability here will involve analysing security measures for the data concerned in light of the history of attempts at gaining unauthorised access to these data. At the same time, the criterion of probability might need to be construed more stringently if the means are illegal.

---

145 This stance is expressly embraced in the *travaux préparatoires* for the new Danish and Belgian data protection laws: see *Behandling af personoplysninger*, Bet 1345 (Copenhagen: Statens Information, 1997), 432; Chambre des Représentants de Belgique, Session ordinaire 1997–1998, 20.5.1998, 1566/1 – 97/98, 12. Cf s 1(3) of the UK Act which defines 'personal data' as 'data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'. The equivalent definition in s 1(1) of the Irish Act is similar. Both definitions might be read as indicating that account is only to be taken of the data controller's ability to carry out identification. However, they do not have to be read this way and are, accordingly, not necessarily in conflict with the Directive.

146 For a similar view, see L Coll, *Innsyn i personopplysninger i elektroniske markedsplasser*, CompLex 3/2000 (Oslo: Universitetsforlaget, 2000), 60. Cf Austria's new data protection law which operates with a sub-category of personal data termed 'only indirectly person-related' ('nur indirekt personenbezogen'). This sub-category is defined as data that the controller or processor cannot link (on his/her/its own) to a specific person using '*legally permitted* means' ('rechtlich zulässigen Mitteln'; emphasis added): see § 4(1) of the *Data Protection Act* of 2000 (*Datenschutzgesetz 2000* (DSG 2000), BGBl I Nr 165/1999). Processing of this category of data is subjected under the Act to less stringent controls than the processing of other personal data.

Accuracy of link between data set and individual

The issue of the accuracy of the connection between a set of data and an individual has rarely been raised in data protection discourse. The issue comes to a head in cases where a set of data (eg, about a company) are incorrectly perceived to relate to an individual. Does this lack of objective validity mean that the data are not properly to be regarded as 'personal' pursuant to data protection laws? In support of a negative answer to this question, one could point to the rules in data protection laws on rectification of incorrect or misleading data:[147] such rules would seem not to make sense if an affirmative answer were adopted. However, by and large, these rules seem to operate only once data are established as being 'personal'; ie, they do not relate to the quality (accuracy) of the way in which a set of data are initially connected to an individual.

It could be argued that the manner of such connection must be objectively valid in the sense that data, in order to be 'personal', must be capable, in truth, of being linked to one person; concomitantly, it is not possible under data protection law for data to become 'personal' primarily on the basis of a *mis*perception that the data are so capable. This argument works best with respect to those data protection laws whose definitions of 'personal data' (or 'personal information') do not embrace mere opinions. However, some national data protection laws allow for opinions to qualify as personal data;[148] some even allow for *false* opinions to qualify as such.[149] It is not entirely clear if the definition of 'personal data' in Art 2(a) of the EC Directive embraces opinions, let alone false ones. It has been intimated that mere opinions fall outside the scope of the definition.[150] However, neither the Directive nor its *travaux préparatoires* specifically exclude opinions from coverage. Indeed, the *travaux préparatoires* indicate an intention to make the definition of 'personal data' in the Directive 'as general as possible, so as to include all information concerning an identifiable individual'.[151] In light of this intention, together with the Directive's express aim of providing for a high level of data protection,[152] solid grounds exist for including opinions – even false ones – within the ambit of Art 2(a). Such an inclusion, though, brings with it a risk of regulatory overreaching. This risk could be mitigated by limiting inclusion to those opinions that are socially significant; ie, are shared by many people and harbour possibly adverse consequences for the individual concerned.

---

147 See further Chapter 3 (section 3.5) and Chapter 18 (section 18.4.4).

148 See, eg, s 6(1) of the Australian Act, s 1(3) of the UK Act and s 2(1) of Norway's PDA.

149 The case with, eg, the Australian Act.

150 See K Davey, 'Privacy Protection for Internet E-mail in Australia' (1998) *Computers & Law*, no 35, 21, 28.

151 COM(92) 422 final – SYN 287, 15.10.1992, 9.

152 See recitals 9–11, *supra* n 135.

Use of auxiliary information

The issue of auxiliary information[153] is not specifically addressed by the CoE Convention, OECD Guidelines or UN Guidelines. However, the inclusion of the term 'identifiable' in their definitions of 'personal data' would seem to open up for the use of some such information. Article 2(a) of the EC Directive is more helpful in this respect, providing that

> '… an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[154]

On the national plane, many data protection laws open up for the use of certain auxiliary information, either by making specific mention of such information,[155] or by providing that identification may occur 'indirectly'.[156] Inclusion of the adjective 'identifiable' in the definition of 'personal data' has also been interpreted as allowing for the use of some auxiliary information in identifying a person.[157] The same applies with respect to the phrase 'can reasonably be ascertained' in s 6(1) of Australia's federal *Privacy Act*.[158]

Requirement of individuation

The sixth and final issue concerns the extent to which data must allow for individuation; ie, be linkable to *one* person as opposed to an aggregate of persons. Data protection laws typically require that data must allow for individuation in order to qualify as 'personal'. However, some uncertainty and variation exist from jurisdiction to jurisdiction as to how stringent the requirement of individuation is applied. Swedish data protection law has operated with a very stringent individuation requirement.[159] Finnish data protection law, by contrast, expressly opens up for some

---

153 Usually termed 'Zusatzwissen' in German.

154 See also the elaboration of these criteria in the commentary by the EC Commission, *supra* n 138.

155 See, eg, s 1(3) of the UK Act, *supra* n 145.

156 See, eg, s 2(1) of Iceland's *Act on the Protection of Individuals with Regard to Processing of Personal Data* of 2000 (*Lög nr 77 23 mai 2000 um persónvernd og medferd persónuupplýsninga*).

157 This is the case, for example, in relation to the definition of 'personal data' in s 3(1) of Germany's *Federal Data Protection Act*: see U Dammann, '§ 3', in Simitis *et al*, *supra* n 56, paras 21, 28ff.

158 The office of the Australian federal Privacy Commissioner takes the view that if one can ascertain 'fairly easily' the identity of a person from one set of information using another set of information then the former set of information is 'personal': according to David Thorp (Senior Advisor to the Commissioner and Director of the Commissioner's Privacy Complaints and Enquiries Unit) in a personal interview of 16.12.1997. The same view was taken by the Australian Law Reform Commission (ALRC) in respect of clause 8(1) of its Draft Privacy Bill upon which the present s 6(1) of the *Privacy Act 1988* is based: see Australian Law Reform Commission (ALRC), *Privacy*, Report No 22 (AGPS, 1983), vol 2, 82. Graham Greenleaf embraces a similar line: see, eg, G Greenleaf, 'Privacy principles – irrelevant to cyberspace?' (1996) 3 *PLPR*, 114, 114.

159 See further Chapter 18 (section 18.2).

relaxation of the requirement by providing that data may be 'personal' even if they can be linked only to a 'family' or 'household' unit.[160] Such provision is rare. Nevertheless, relaxation of the individuation requirement would seem to be possible under some other national data protection laws. Under German law, for instance, it seems that data may be 'personal' even if they can be linked to two individuals, though not to three or more individuals.[161] A similar position is possible with respect to Norwegian data protection law, though the latter traditionally has not operated with any predetermined number of persons when setting the boundaries for the individuation criterion. What is crucial is whether the group data can be 'indirectly linked to an individual' (presumably without an extreme amount of effort).[162]

Restricting expansive potential

From the analysis above, it is clear that many of the definitions of personal data are capable in theory of embracing a great deal of data, including geographical and environmental data, which *prima facie* have little direct relationship to a particular person.[163] At the same time as this capability has obvious benefits from a data protection perspective, it threatens the semantic viability of the notion of 'personal data/information' and incurs a practical-regulatory risk that data protection laws will overreach themselves. Thus, in some jurisdictions, attempts have been made to limit this capability. For example, Ulrich Dammann claims that, as a general rule in German data protection law, data over, say, material goods are 'personal' only insofar as the data identify the goods and are able to relate them to the 'life context' of a particular person.[164] A broadly similar, though perhaps more restrictive, line has been taken by Australia's federal Privacy Commissioner.[165] Moreover, the *travaux*

---

160 See the definitions of 'personal data' in s 2(1) of the 1987 Act and s 3(1) of the 1999 Act.

161 Dörr & Schmidt, *supra* n 143, 26; Dammann, *supra* n 157, para 42.

162 See statement of the Norwegian Data Inspectorate in its letter of 10.9.1980 (ref 80/580-2 AF/NM) to Schibsted-gruppen. The Inspectorate did not spell out what it meant by 'indirectly identified'. However, its statement has been cited – somewhat presumptuously – as showing that it viewed the *Personal Data Registers Act* as applicable when information could be linked to a 'smaller group of, eg, 2–3 persons': M Borchgrevink, *Ny teknologi i arbeidslivet: rettslige aspekter* (Oslo: Universitetsforlaget, 1985), 240; Coll, *supra* n 146, 63. Some commentary on the new *Personal Data Act* takes a similar line though suggests that the possibility of information being personal when it can only be linked to a group of two or three persons, depends somewhat on the existence of a pronounced threat to data protection interests: see M Wiik Johansen, K-B Kasperson & ÅM Bergseng Skullerud, *Personopplysningsloven. Kommentarutgave* (Oslo: Universitetsforlaget, 2001), 69. See further *infra* n 166.

163 For examples, see J Bing, 'From footprints to electronic trails: Some current issues of data protection policy', in *Proceedings of the 17th International Conference on Data Protection, Copenhagen 1995* (Registertilsynet/Data Protection Agency, 1995), 3.

164 Dammann, *supra* n 157, para 57. Cf the apparently less restrictive line in J Taeger, 'Umweltschutz und Datenschutz' (1991) CR, 681, 686 ('Jede Information, die in irgendeiner Weise einen Personenbezug hat, fällt zunächst in den Anwendungsbereich des Datenschutzrechts').

165 According to David Thorp (Senior Advisor to the Privacy Commissioner and Director of the Commissioner's Privacy Complaints and Enquiries Unit), in a personal interview of 16.12.1997. As

préparatoires to the Norwegian *Personal Data Act* suggest that some data that would fit within the Act's literal definition of 'personal information' (in s 2(1)) may not warrant protection in light of the Act's objects clause.[166] As Dammann makes clear, such delimitations are not fixed along abstract logical or semantic lines; rather, they are reached pragmatically.[167]

Alternatively, the UK *Data Protection Act* of 1984 (repealed) only applied to the processing of personal data when the processing occurs 'by reference to the data subject' (s 1(7)). The UK Data Protection Tribunal (now 'Information Tribunal') read the latter phrase as excluding from the purview of the Act processing operations in which the data subject is not intended to be in focus.[168] However, there is no corresponding phrase into which this delimitation can be read on the face of the new UK Act of 1998 – at least with regard to *automated* processing.[169] The same can be said with respect to the EC Directive along with the other data protection laws I have perused.

Nevertheless, a majority judgment of the Hong Kong Court of Appeal has read down the scope of Hong Kong's *Personal Data (Privacy) Ordinance* of 1995 by taking a similar line to that of the UK Data Protection Tribunal.[170] The Court

---

(Cont.)

an example, Thorp mentioned a case from 1992/93 (archive reference not found) in which basic information about an old house (its structure, number of rooms, type of garden, name, suburban location – but not its street address nor the identity of its current owner) which was registered in a Heritage Listing, was held by the Commissioner not to constitute personal information pursuant to the *Privacy Act* even though the information could be linked to a particular person (the house owner).

166 NOU 1997:19, 131; Ot prp 92 (1998–99), 101. The objects clause of the Act is summarised *supra* n 114.

167 Dammann, *supra* n 157, para 57.

168 See *Equifax Europe Ltd v Data Protection Registrar* (1991) Case DA/90 25/49/7, para 49 ('using the Land Registry's computer to change the boundaries of a plot of land, or perhaps to extract a copy of a restrictive covenant, would in no way concern the individual identity or attributes of a data subject, and need not attract the control over processing'). The Tribunal contrasted such a processing operation with a situation in which 'the object of the exercise is to learn something about the individual [data subject], not about the land': *ibid*, para 50.

169 It *might* be possible to read in some such limitation with respect to non-automated (manual) processing of data: see the definition of 'relevant filing system' in s 1(1) of the 1998 Act ('any set of information relating to individuals to the extent that … the set is structured, either by reference to individuals or by reference to criteria relating to individuals …'). The definition of 'personal data filing system' in Art 2(c) of the EC Directive is more open-ended ('any structured set of personal data which are accessible according to specific criteria …'), though this open-endedness is undercut by recital 27 in the Directive's preamble which states that 'the content of a filing system must be structured according to specific criteria relating to individuals …'.

170 See *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* [2000] 1 HKC 692 (per Ribeiro JA and Godfrey VP; Wong JA dissenting). The case concerned the non-consensual publication by a magazine of a photograph taken at long range by one of its journalists of a woman in a public place without her knowledge. The photograph was one of a series published in a feature article on the fashion sense of Hong Kong women. In the article, derisive comments were made about the dress style of the photographed woman though no additional information was supplied as to her

majority held that the collection of data falls within the scope of the Ordinance only if the 'data user' is 'thereby … compiling information about an *identified* person or about a person *whom the data user intends or seeks to identify*.'[171]

Also noteworthy are *obiter dicta* in a recent majority judgment of the NZ Court of Appeal which express scepticism towards an 'unqualified approach' to what constitutes personal information under the country's *Privacy Act*.[172] The *obiter dicta* signal perhaps a future preparedness on the part of the NZ judiciary to read down the literal scope of the concept of personal information. However, the reasoning of the court majority on the point at issue is somewhat dubious, further undermining the authority of the *dicta* as precedent.[173]

2.4.2 COVERAGE WITH REGARD TO TYPE OF DATA PROCESSING

Data protection laws typically regulate all or most stages of the data-processing cycle, including registration, storage, retrieval and dissemination of personal data. Thus, Art 2(b) of the EC Directive broadly defines 'processing' as

---

(Cont.)
identity, which was immaterial for and unknown to the magazine. The woman was embarrassed by the article and lodged a complaint with the Privacy Commissioner. The main issue before the Court was whether the publisher of the magazine had breached DPP 1 of the Ordinance which requires personal data to be collected fairly and lawfully. The Court majority found that there had been no breach as the magazine had neither sought nor intended to identify the woman. Although this finding formally relates to the meaning of 'collection' under the Ordinance, it implicitly rests on a view of the meaning of 'personal data'. For further detail on the case, see R Wacks, 'What has data protection to do with privacy?' (2000) 6 *PLPR*, 143–146.

171 *Ibid*, 700 (emphasis added). The conclusion was grounded partly in a concern not to unduly restrict photojournalistic activity and thereby freedom of expression (*ibid*, 701) and partly in the assumption underlying several of the basic rules of the Ordinance (eg, data access and rectification rights) that a data controller is able to readily identify the data subject (*ibid*, 702–703).

172 See judgment of Tipping J (with whom Elias CJ and Thomas J agreed) in *Harder v Proceedings Commissioner* [2000] 3 NZLR 80, 89–90. Here the court majority doubted that tape recordings of telephone conversations between a woman and a barrister contained personal information related to the woman for the purposes of the *Privacy Act*. The recordings appear to have dealt with largely procedural matters on the handling of a proposed settlement between the woman and her former partner (whom the barrister represented) in connection with the partner's breach of a non-violence order. The recordings also revealed whether the woman was in possession of certain unspecified goods.

173 The court majority derived support for its view on what constitutes 'personal information' from s 14(a) of the Act. That provision requires the Privacy Commissioner, when carrying out his/her functions, 'to have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of the free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way'. It is at the very least questionable whether s 14(a) is legally relevant for determining the scope of the concept of 'personal information' in the Act. See further the casenote by P Roth in (2000) 7 *PLPR*, 134, 135. See also P Gunning, 'Central features of Australia's private sector privacy law' (2001) 7 *PLPR*, 189, 192.

> 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'

The concept of 'processing' used in the CoE Convention is a little narrower: it does not cover collection of data, nor data processing carried out by entirely manual (non-automated) means.[174] However, Art 3 allows Contracting States to apply the rules laid down in the Convention to data processed manually. Moreover, some of the Convention's provisions (notably Art 5(a)) pertain directly to the collection of data.

Some national data protection laws have focused mainly on the registration, as opposed to collection, of personal data. This was the case, for instance, with Norway's PDRA. This focus was part of a more general focus on the creation and use of personal data *registers*; ie, files, records and the like in which 'personal information is systematically stored so that information concerning an individual person may be retrieved' (PDRA, s 1(2)). The focus on registers is shared by some other data protection instruments, including the CoE Convention and UN Guidelines.

This regulatory focus on registers and files is typical for data protection instruments drafted in the 1970s and early 1980s. It reflects a belief from those times that systematically structured collections of personal data pose the principal risks for data subjects' interests in privacy, integrity and the like.[175] It further reflects the character of computerised data processing which predominated in that period – personal computers and distributed computer networks were then in their infancy. To some extent, such a focus is also symptomatic of a concern to limit the ambit of data protection laws so as to prevent regulatory overreaching and collision with other laws.[176]

The regulatory focus of the EC Directive is on the 'processing' of personal data regardless (almost) of the way in which the data are organised. This is also the case with the OECD Guidelines, along with many recently enacted national data protection laws.[177] Future laws are likely to dispense largely with the register/file concept, partly in order to avoid their marginalisation in a world of distributed computer networks and partly in order to conform with the EC Directive. The move

---

174 See Art 2(c) along with para 31 of the Convention's Explanatory Report.

175 See, eg, Ot prp 2 (1977–78), 69 ('Som hovedregel antar [Justis-]departementet at det bare er når personopplysninger er tatt inn i registre at det er behov for særlige lovregler for å sikre personvernet').

176 See, eg, *ibid*, 22 ('Noen generell regulering spesielt for personopplysninger ville antakelig være vanskelig å koordinere med de reglene som gjelder for forvaltningens saksbehandling generelt').

177 See, eg, Hungary's *Act No LXIII of 27.10.1992 on the Protection of Personal Data and on the Publicity of Data of Public Interest* (*1992 evi LXIII torveny a szemelyes adatok vedelmerol es a kozerdeku adatok nyilvanossagarol*); and Italy's *Law no 675 of 31.12.1996 on Protection of Individuals and Other Subjects with Regard to Processing of Personal Data* (*Legge 31 dicembre 1996, n. 675 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*).

is not only sensible in view of technological developments; it also makes for increased flexibility of the laws' application. It enhances their ability to embrace forms of data processing, such as video surveillance, which can fit uncomfortably within the register/file concept. Further, it allows for easier avoidance of complex and arbitrary line-drawing exercises in evaluating what constitutes a register and where the boundaries between one register and other registers should be fixed.

Nevertheless, the register/file concept has not been totally ditched by the Directive; it lives on with respect to manually processed data. Pursuant to the Directive, purely manual data processing is to be regulated insofar as the data form or are intended to form part of a 'filing system' (Art 3(1)). By 'filing system' is meant 'any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis' (Art 2(c)). As this definition suggests, retainment of the register/file concept here is essentially a consequence of a concern (noted in section 2.4.1) to limit the application of data protection laws to data that can be linked to a particular person without great difficulty,[178] as it is in relation to this sort of data the risk to data protection interests primarily lies.[179] Retainment is also symptomatic of a concern to prevent data protection laws from overreaching themselves in a practical, regulatory sense.[180]

Otherwise, the provisions of the Directive are largely technology-neutral. This is in contrast to the CoE Convention and UN Guidelines which cover automated data-processing practices to the almost total exclusion of manual (non-automated) processing.[181] The data protection legislation of a large number of countries, such as Austria, Ireland, Japan, Luxembourg, Sweden and the UK, also cover or initially covered automated data-processing practices only. This focus on automation is symptomatic of a belief that the increasing usage of computers, particularly for decision-making purposes, represents the main threat to data protection interests.[182]

However, due to the requirements of the EC Directive, data protection laws will increasingly extend to both manual and computerised processing of personal data. This broadening of focus is partly grounded on a desire to prevent the circumvention

178 Recital 27 qualifies the notion of accessibility in Art 2(c) with the adjective 'easy'; ie, in order to fall within the scope of the Directive, the filing system 'must be structured according to specific criteria relating to individuals allowing easy access to the personal data'. See also recital 15.

179 On the latter point, see, eg, the Explanatory Memorandum to the Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final – SYN 287, 15.10.1992), 10.

180 *Id*.

181 Cf the OECD Guidelines which apply to both manual and automated processing of personal data. Both the CoE Convention and UN Guidelines, however, provide for the optional extension of their principles to cover non-automated data files: see Art 3(2)(c) of the Convention and para 10 of the UN Guidelines.

182 See, eg, para 1 of the CoE Convention's Explanatory Report.

of laws that govern automated processing only.[183] It is also partly grounded on the realisation that manually processed data can have significant implications for the privacy, autonomy and integrity interests of data subjects – indeed, often the most sensitive personal data (eg, on persons' mental and physical health) are to be found in manual record systems. And it is partly technology-induced insofar as data in modern information systems tend to be processed using a mixture of automated, semi-automated and manual techniques, the line between which can often be difficult to draw.[184] This does not mean that manual and automated techniques will be uniformly regulated in all respects. The EC Directive allows for some discrimination here. For instance, Art 18 of the Directive does not require national data protection authorities to be notified of purely manual data-processing operations.[185]

2.4.3 COVERAGE WITH REGARD TO SECTORS

All of the international data protection instruments are intended to apply to the processing of personal data in both the public and private sectors. Not surprisingly, a majority of national data protection laws have a similar ambit. In some of these laws, however, differentiated regulation for each sector has occurred,[186] with the processing practices of public sector bodies sometimes being subjected to more stringent regulation than those of private sector bodies.[187] Such differentiation is expected to diminish considerably in the future national legislation of EU Member States given its absence from the EC Directive.

A handful of countries – USA, Japan and the Republic of Korea (South Korea) – have national/federal data protection laws which largely regulate the data-processing activities of national/federal government agencies only. A similar situation pertained up until very recently with Australia and Canada. Constitutional limitations on the

183 See, eg, recital 27 of the EC Directive.

184 A point duly noted in, eg, para 35 of the OECD Guidelines' Explanatory Memorandum.

185 See further Chapter 4 (section 4.2). Note, though, that Art 18(5) gives EU Member States the option of stipulating such a requirement.

186 Cf Denmark which previously regulated each sector with separate Acts; ie, the *Public Authorities' Registers Act* and the *Private Registers Act*. The new Danish data protection legislation largely dispenses with such differentiated regulation: see the *Personal Data Act* of 2000.

187 See, eg, s 15 of the French data protection law which subjects automatic processing of personal data by public sector bodies to prior authorisation by the country's data protection authority, unless the processing is already authorised by law. In contrast, private bodies may undertake automated processing of personal data simply upon notifying the authority of the basic details of their processing plans (s 16). Cf s 17 which provides for a simplified notification procedure for both public and private bodies in the case of 'the most common types' of data processing 'which manifestly do not infringe upon privacy or liberties'. The above sectoral differentiation is set to disappear under recently proposed amendments to the Act: see *Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (no 3250), introduced 18.7.2001.

legislative powers of federal governments have partly accounted for the restricted ambit of the laws in question but other factors are often more significant. In the USA, for instance, there reigns general distrust of State dirigism, accompanied by scepticism towards legislative regulation of the private sector except where there are proven to exist flagrant imbalances of power between private parties which cannot be corrected otherwise than by legislative intervention.[188] In the field of privacy/data protection, this scepticism has resulted in the eschewal of 'omnibus' legislative solutions in favour of *ad hoc* enactment of sectoral laws dealing with, in the words of Joel Reidenberg, 'narrowly identified' problems.[189] The coverage these laws offer with respect to processing of personal data by private sector bodies remains haphazard and incomplete.[190]

Much the same could be said of the coverage previously offered by equivalent legislative regimes for data protection with respect to the private sector in Australia and Canada.[191] Now, though, federal data protection legislation has been passed in both countries giving considerably more comprehensive coverage of the private sector.[192] Some significant gaps remain, however, particularly under Australian law.[193]

With adoption of the EC Directive and the resultant threat that EU countries will prevent, pursuant to Art 25 of the Directive, transfers of personal data to countries without 'adequate' levels of data protection,[194] greater legal (and economic) pressure is now upon countries like the USA, Japan and Australia to enact comprehensive data protection laws to regulate the private sector. At the same time, one should not overlook the possibility of one or more of the latter countries' governments (particularly that of the USA) thumbing their noses at the EU in defiance of the 'adequacy' criterion laid down in the Directive.[195] The extent to which this might occur is likely to depend on how stringently and consistently the 'adequacy' criterion is applied, together with the extent to which implementation of Art 25 (and Art 26) is

---

188 See further JH Yurow, 'National Perspectives on Data Protection' (1983) 6 *TDR*, no 6, 337–339; Schwartz & Reidenberg, *supra* n 58, 6ff.

189 JR Reidenberg, 'Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?' (1992) 44 *Federal Communications LJ*, 195, 201.

190 For detailed analysis of these laws, see Schwartz & Reidenberg, *supra* n 58, chapts 9–14.

191 However, a comprehensive, 'European-style' data protection regime has long been established in Quebec pursuant to the 1993 *Act on Protection of Personal Information in the Private Sector*.

192 For Australia, see *Privacy Amendment (Private Sector) Act 2000* (in force 21.12.2001); for Canada, see *Personal Information Protection and Electronic Documents Act* of 2000. The latter Act is being implemented in three stages, from 1.1.2001 to 1.1.2004.

193 For example, with a few exceptions, the Australian legislation does not apply to so-called 'small business operators'; ie, businesses with an annual turnover of AUS$3 million or less (see federal *Privacy Act*, ss 6C(1), 6D, 6DA & 6E)). Another major gap is that the legislation does not cover the processing of data by employers about their present and past employees (as long as the processing is directly related to the employment relationship) (s 7B(3)).

194 See further Chapter 4 (section 4.4).

195 See further Chapter 4 (section 4.4).

found to conflict with international trade law.[196] Other factors might also prove significant, not least the extent to which business enterprises in, say, the USA tire of having to cope with the patchy, sometimes uncertain and inconsistent legal regimes for data protection in that country.

It should be emphasised that data protection laws covering the private and/or public sectors rarely regulate all processing of personal data. For example, exemptions from the laws in their entirety or from their central provisions are often made with respect to data-processing operations of national security services,[197] data-processing operations of the mass media for journalistic purposes,[198] and/or data processing for purely personal or domestic purposes.[199] Considerable uncertainty surrounds the exact ambit of many of these exemptions, though some authoritative guidance is beginning to emerge.

One of the most significant instances of recent authority is the decision of 12.6.2001 by the Swedish Supreme Court in case B293-00 (as yet unreported) which casts light on the meaning of the expression 'solely for journalistic purposes' in Art 9 of the EC Directive and s 7 of Sweden's *Personal Data Act* (the latter provision transposing Art 9). Using as a major point of departure case law of the ECtHR on the right to freedom of expression pursuant to Art 10 of the ECHR – particularly the principle of proportionality developed therein – the Supreme Court ruled that the expression is not intended to cover just the established mass media. Concomitantly, the exemption to which the expression attaches, may cover communication that fails to meet the standards of professional journalism. It may also apply to communication that is defamatory. As for the reference to 'solely' ('uteslutande' in s 7 of the Swedish Act), the Court held that this is intended to clarify that data processing by journalists and the mass media for other than 'editorial' purposes (eg, for the purposes of invoicing, direct marketing or production of consumer profiles) is not encompassed by the exemption. The Court was unable to find support for construing 'solely' such that publishing activity which has a journalistic purpose but which also

196 See further Chapter 4 (section 4.4).

197 See, eg, Art 3(3) of the Belgian Act; s 1(4)(a) of the Irish *Data Protection Act* of 1988. Cf Arts 3(2) & 13(1) of the EC Directive, set out *supra* n 80.

198 See, eg, s 7 of Sweden's *Personal Data Act*; Art 3(1) of the Netherlands' *Personal Data Protection Act* of 2000 (*Wet bescherming persoonsgegevens*). Article 9 of the EC Directive requires EU Member States to lay down exemptions from the central provisions of the Directive with respect to data processing 'carried out solely for journalistic purposes or the purpose of artistic or literary expression', insofar as is 'necessary to reconcile the right to privacy with the rules governing freedom of expression'. See also recitals 17 and 37. For brief consideration of the impact of Art 9 on profiling practices, see Chapter 18 (section 18.4.6). Further on the ambit of Art 9, see *infra* n 200 and accompanying text.

199 See, eg, Art 3(2) of the EC Directive which exempts coverage of data processing 'by a natural person in the course of a purely personal or household activity'. Cf declaration 9 of the Council minutes in which the Commission and Council infer that the phrase 'purely personal or household activity' should not be taken to embrace an individual's communication of personal data to an indeterminate circle of persons: see Blume, *Personregistrering*, *supra* n 93, 432.

involves spreading derogatory information about persons, may be penalised under the data protection legislation. At the same time, the Court made clear that its judgment did not prevent possible prosecution for defamation under other legislation.[200]

200 For further detail on the decision, see LA Bygrave, 'Balancing data protection and freedom of expression in the context of website publishing – recent Swedish case law' (2001) 8 *PLPR*, 83–85.

3. Core Principles of Data Protection Laws

3.1 Introduction

This chapter provides an overview of the basic principles applied by data protection laws to the processing of personal data. These principles are summed up in terms of 'fair and lawful processing' (see section 3.2), 'minimality' (section 3.3), 'purpose specification' (section 3.4), 'information quality' (section 3.5), 'data subject participation and control' (section 3.6), 'disclosure limitation' (section 3.7), 'information security' (section 3.8) and 'sensitivity' (section 3.9). As shown in the following, these categories are not always hard and fast; considerable overlap exists between them. Further, each of them is in reality a constellation of multiple principles.

The purpose of the chapter is to present the constituent elements of these principles, along with the main similarities and differences in their formal manifestation in the various data protection instruments. The chapter does not attempt to analyse in detail the scope and content of the principles nor the range of legal exemptions to their implementation. Such analysis is undertaken in Chapter 18 insofar as is relevant for the regulation of profiling practices.

The following principles are primarily abstractions that denote the pith and basic thrust of a set of legal rules. At the same time, they have a normative force of their own. This force is achieved in several ways. First, the principles (or a selection of them) have been expressly incorporated in certain data protection laws as fully-fledged legal rules in their own right (though not always using exactly the same formulations as given in this chapter). Examples of such incorporation are found throughout the following sections. Secondly, the principles function as guiding standards during interest-balancing processes carried out by, for instance, data protection authorities in the exercise of their discretionary powers. Examples of such a function are found in Chapter 18 (section 18.4.7). Finally, and closely related to the latter function, the principles help to shape the drafting of new data protection laws. This is most obviously exemplified in the impact of the OECD Guidelines (which, as shown below, contain most of the principles) on the drafting of Australian and NZ data protection legislation.[201]

---

201 See *supra* n 89.

3.2 Fair and Lawful Processing

The primary principle of data protection laws is that personal data shall be 'processed fairly and lawfully'.[202] This principle is 'primary' because, as demonstrated in the following, it embraces and generates the other core principles of data protection laws presented below.[203] Concomitantly, the twin criteria of fairness and lawfulness are manifest in all of these principles even if, in some instruments, they are expressly linked only to the means for collection of personal data,[204] or not specifically mentioned at all.[205]

Of the two notions 'fairly' and 'lawfully', the latter is relatively self-explanatory. Less obvious in meaning but potentially broader is the notion of fairness. An exhaustive explication of the fairness notion cannot be achieved in the abstract.[206] Moreover, general agreement on what is fair will inevitably change over time. Nevertheless, at a very general level, the notion of fairness undoubtedly means that, in striving to achieve their data-processing goals, data controllers must take account of the interests and reasonable expectations of data subjects; controllers cannot ride roughshod over the latter. This means that the collection and further processing of personal data must be carried out in a manner that does not in the circumstances intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity. In other words, the notion of fairness brings with it requirements of balance and proportionality. These requirements are applicable not just at the level of individual data-processing operations; they speak equally to the way in which the *information systems* supporting such operations are designed and structured. This is an important point which is revisited in Chapter 19.

In light of these requirements, fairness also implies that a person is not unduly pressured into supplying data on him-/herself to a data controller or accepting that the data are used by the latter for particular purposes. From this, it arguably follows that fairness implies a certain protection from abuse by data controllers of their monopoly position. While very few data protection instruments expressly address the latter issue,[207] some protection from abuse of monopoly can be read into the relatively

---

202 See, eg, Art 5(a) of the CoE Convention, Art 6(1)(a) of the EC Directive, Art 9 of the Italian Act and DPP 1 in Part 1 of Schedule 1 to the UK Act. For what is, in effect, the same norm, see, eg, Principle 1 of the UN Guidelines, Art 3 of the Hungarian Act and Art 4(2) of the Swiss Act.

203 See further Chapter 18 (section 18.4.1) particularly with respect to the EC Directive.

204 The case, for instance, with the OECD Guidelines (see para 7).

205 The case, for instance, with the Norwegian PDA.

206 See also comments of the UK Data Protection Registrar (now 'Information Commissioner') in *The Guidelines on the Data Protection Act 1984*, Fourth Series (Wilmslow: Data Protection Registrar, 1997), 53; *Thirteenth Report of the Data Protection Registrar, June 1997* (London: The Stationery Office, 1997), 22.

207 The most notable exception is s 3(4) of the German *Teleservices Data Protection Act* of 1997 (*Gesetz über den Datenschutz bei Telediensten*) which seeks to restrict a teleservice provider exploiting its service monopoly by forcing users to consent to the processing of their data for purposes other than

common provisions on data subject consent, particularly the requirement that such consent be 'freely given'.[208]

The notion of fairness further implies that the processing of personal data be transparent for the data subject(s).[209] Fairness not only militates against surreptitious collection and further processing of personal data, it also militates against deception of the data subject as to the nature of, and purposes for, the data processing.[210] Arguably, another requirement flowing from the link between fairness and transparency is that, as a point of departure, personal data shall be collected directly from the data subject, not from third parties. This requirement is expressly laid down in some but not the majority of data protection instruments.[211]

As mentioned above, fairness implies that data controllers must take some account of the reasonable expectations of data subjects. This implication has direct consequences for the purposes for which data may be processed. It helps to ground rules embracing the purpose specification principle (dealt with more fully below). Concomitantly, it sets limits on the secondary purposes to which personal data may be put. More specifically, it arguably means that when personal data obtained for one purpose are subsequently used for another purpose, which the data subject would not reasonably anticipate, the data controller may have to obtain the data subject's consent to the new use.[212]

3.3 Minimality

A second core principle of data protection laws is that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are gathered and further processed. This principle is summed up here in

---

(Cont.)
the performance of teleservices. Cf Principle 18 of the Australian Privacy Charter (adopted December 1994; set out in (1995) 2 *PLPR*, 44–45): 'People should not have to pay in order to exercise their rights of privacy … nor be denied goods or services or offered them on a less preferential basis for wishing to do so. The provision of reasonable facilities for the exercise of privacy rights is part of the normal operating costs of organisations'. The Charter is the private initiative of a group of concerned citizens and interest groups; it has not been conferred any official status by a government body.

208 See, eg, Art 2(h) of the EC Directive.

209 The link between fairness and transparency is made explicit in, eg, recital 38 of the EC Directive; COM(92) 422 final – SYN 287, 15.10.1992, 15.

210 The connection between fairness and non-deception is emphasised in, eg, s 1(1) of Part II of Schedule 1 to the UK Act.

211 Examples of express provision are s 5(1) of Canada's federal *Privacy Act* of 1982, IPP 2 of the NZ *Privacy Act* and NPP 1.4 in Schedule 3 to Australia's federal *Privacy Act*.

212 See further Chapter 18 (section 18.4.1).

terms of 'minimality', though it could also be summed up using a variety of other terms, such as 'necessity', 'non-excessiveness', 'proportionality' or 'frugality'.[213]

The principle is manifest in Art 6(1)(c) of the EC Directive which provides in part that personal data must be 'relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. Article 5(c) of the CoE Convention contains an almost identical requirement except that it relates to the purposes for which data are 'stored'. The above provision of the Directive and, to a lesser extent, that of the Convention are *prima facie* directed at ensuring minimality at the stage of data collection. Both instruments also contain provisions directed *prima facie* at ensuring minimality subsequent to that stage. These provisions require personal data to be erased or anonymised once they are no longer required for the purposes for which they have been kept.[214] The minimality principle is also manifest in one of the EC Directive's basic regulatory premises – embodied in Arts 7 and 8 – which is that the processing of personal data is prohibited unless it is necessary for the achievement of certain specified goals.[215]

The minimality principle does not shine so clearly or broadly in all data protection instruments as it does in the Directive. For instance, neither the OECD Guidelines nor UN Guidelines contain an express requirement of minimality at the stage of data collection, though such a requirement can arguably be read into the more general criterion of fairness as set out in section 3.2 above. The OECD Guidelines also omit a specific provision on the destruction or anonymisation of personal data after a certain period. Again, though, erasure or anonymisation may be required pursuant to other provisions, such as those setting out the principle of 'purpose specification' (see below).[216] Many (but not all)[217] national laws make specific provision for the erasure etc of personal data once the data are no longer required.

Rules encouraging transactional anonymity are also direct manifestations of the minimality principle. Currently, very few data protection laws contain rules expressly mandating or encouraging transactional anonymity.[218] It is arguable, though, that such requirements may be read into the more commonly found provisions (described

---

213 The term 'proportionality' is employed by the CoE in several of its data protection instruments: see, eg, para 4.7 of *Recommendation R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes* (adopted 30.9.1997). Cf s 3a of Germany's *Federal Data Protection Act* which employs the notions of 'data avoidance' ('Datenvermeidung') and 'data frugality' ('Datensparsamkeit').

214 See Art 6(1)(e) of the EC Directive and Art 5(e) of the CoE Convention. The former provision is set out in Chapter 18 (section 18.4.3).

215 See further Chapter 18 (section 18.4.3).

216 A point noted in para 54 of the Guidelines' Explanatory Memorandum.

217 The US federal *Privacy Act* being an example. However, a requirement of erasure/anonymisation can arguably be read into other provisions of the Act: see s 552a(e)(1) and (5).

218 The most far-reaching requirements for transactional anonymity are laid down in ss 3a of Germany's *Federal Data Protection Act* and 4(6) of Germany's *Teleservices Data Protection Act* of 1997. See further Chapter 18 (section 18.4.3).

above) in which the minimality principle is manifest, particularly when these provisions are considered as a totality.[219]

3.4 Purpose Specification

Another core principle of data protection laws is that personal data shall be collected for specified, lawful and/or legitimate purposes and not subsequently processed in ways that are incompatible with those purposes. This norm is often termed the principle of 'purpose specification'.[220]

The principle is really a cluster of three principles:

1) the purposes for which data are collected shall be specified/defined;
2) these purposes shall be lawful/legitimate;
3) the purposes for which the data are further processed shall not be incompatible with the purposes for which the data are first collected.

Terminologically, the notion of 'purpose specification' denotes the first-listed principle more aptly than the latter two principles. Nevertheless, the notion of purpose specification is used in this book to cover all three principles.

The principle is prominent in all of the main international data protection instruments.[221] It is also prominent in most (but not all)[222] of the national laws. Some laws stipulate that the purposes for which data are processed shall be 'lawful'.[223] Other laws, such as the Directive and Convention, stipulate that such purposes shall be 'legitimate'.

Fairly solid grounds exist for arguing that the notion of 'legitimate' denotes a criterion of social acceptability, such that personal data should only be processed for purposes that do not run counter to predominant social mores.[224] At the same time, extensive latitude pertains as to how such mores are to be defined. The bulk of data

---

219 See further Chapter 18 (section 18.4.3).

220 See, eg, para 9 of the OECD Guidelines and Principle 3 of the UN Guidelines. Another term often used to describe the principle (or elements of it) is 'finality': see, eg, G Greenleaf, 'The European privacy Directive – completed' (1995) 2 *PLPR*, 81, 84; Article 29 Data Protection Working Party, 'Privacy on the Internet: An Integrated EU Approach to On-line Data Protection', Working Document adopted 21.11.2000, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf>, 69 & 79.

221 See Art 5(b) of the CoE Convention, Art 6(1)(b) of the EC Directive, Principle 3 of the UN Guidelines and para 9 of the OECD Guidelines.

222 Norway's *Personal Data Registers Act* (now repealed) being an example. However, the principle was enshrined in chapters 2–3 (see espec s 3-1) of the main regulations to the PDRA (*Forskrifter i medhold av lov om personregistre mm 21 desember 1979*) and in administrative practice pursuant to the Act. See further Chapter 18 (sections 18.4.2 and 18.4.7). Cf the relatively oblique manifestation of the principle in the federal *Privacy Act* of respectively Australia and the USA.

223 See, eg, DPP 2 in Part I of Schedule 1 to the UK Act of 1998. This is also the case with the OECD Guidelines.

224 See further Chapter 18 (section 18.4.2).

protection instruments comprehend legitimacy *prima facie* in terms of procedural norms hinging on a criterion of lawfulness (eg, that the purposes for which personal data are processed should be compatible with the ordinary, lawful ambit of the particular data controller's activities).[225] Very few expressly operate with a broader criterion of social justification.[226] Nevertheless, the discretionary powers given by some laws to national data protection authorities have enabled the latter to apply a relatively wide-ranging test of social justification, particularly in connection with the licensing of certain data-processing operations.[227] Although this ability is in the process of being cut back in line with reductions in the scope of licensing schemes, it will not disappear completely.[228]

3.5 Information Quality

A fourth core principle of data protection laws is that personal data should be valid with respect to what they are intended to describe, and relevant and complete with respect to the purposes for which they are intended to be processed. All data protection laws contain rules directly embodying the principle, but they vary considerably in their wording, scope and stringency.

Regarding the first limb of the principle (concerning the validity of data), data protection laws use a variety of terms to describe the stipulated data quality. Article 5(d) of the CoE Convention and Art 6(1)(d) of the EC Directive state that personal data shall be 'accurate and, where necessary, kept up to date'.[229] The equivalent provisions of some other data protection instruments refer only to a criterion of accuracy/correctness ('Richtigkeit'),[230] while still others supplement the latter with other criteria, such as completeness.[231]

---

225 See, eg, IPP 1(a) of Australia's federal *Privacy Act*; s 4 of Canada's federal *Privacy Act*; s 11(1)(b) of Norway's PDA.

226 A lonely example is s 4(2) of the Netherlands' *Registration of Persons Act* of 1988 (*Wet van 28 december 1988 houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonregistraties* – repealed by the *Personal Data Protection Act* of 2000) which stated: 'The purpose of a personal data file may not be in conflict with the law, *the maintenance of public order or morality*' (emphasis added). Cf s 5(3) of Canada's *Personal Information Protection and Electronic Documents Act*: 'An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'.

227 For examples, see further Chapter 18 (section 18.4.7).

228 See further Chapter 4 (section 4.2). Section 33 of Norway's PDA, for instance, maintains the possibility for the Data Inspectorate to undertake a relatively open-ended assessment of licensing applications, albeit with respect to a narrower range of data-processing operations than was the case under the 1978 legislation. See further Chapters 4 (section 4.2) and 18 (section 18.4.7).

229 Identical or near-identical requirements are set down in the provisions of several national laws, including Art 9(1)(c) of the Italian Act and DPP 4 in Part 1 of Schedule 1 to the UK Act.

230 See, eg, Art 5 of the Swiss Act.

231 See, eg, para 8 of the OECD Guidelines.

With regard to the principle's second limb, the EC Directive formulates this as a requirement that personal data are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed' (Art 6(1)(c)).[232] Some data protection instruments refer to the criteria of relevance, accuracy and completeness but not non-excessiveness.[233]

Finally, variation exists in terms of the stringency with which data protection instruments require checks on the validity of personal data. The standard set by the EC Directive, for example, is in terms of 'every reasonable step must be taken' (Art 6(1)(d)). By contrast, the UN Guidelines emphasise a duty to carry out 'regular checks' (principle 2).[234]

3.6 Data Subject Participation and Control

A core principle of data protection laws is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations. This principle embraces what the OECD Guidelines term the 'Individual Participation Principle' (para 13), though rules giving effect to it embrace more than what is articulated in that particular paragraph.

Data protection instruments rarely contain one special rule expressing this principle in the manner formulated above. Rather, the principle manifests itself more obliquely through a combination of several categories of rules. First, there are rules which aim at making people aware of data-processing activities generally. The most important of these rules are those requiring data controllers to provide basic details of their processing of personal data to data protection authorities, coupled with a requirement that the latter store this information in a publicly accessible register.[235]

Secondly, and arguably of greater importance, are a category of rules which are aimed at making persons aware of basic details of the processing of data on themselves. This category of rules can be divided into three main sub-categories:

1) rules requiring data controllers to collect data directly from data subjects in certain circumstances;
2) rules prohibiting the processing of personal data without the consent of the data subjects; and
3) rules requiring data controllers to orient data subjects directly about certain information on their data-processing operations.

---

232 Similarly formulated requirements are found in several national laws: see, eg, Art 9(1)(d) of the Italian Act, Art 5(2) of the Hungarian Act and, in effect, s 552a(e)(1), (5) & (6) of the US federal *Privacy Act*.

233 See, eg, para 8 of the OECD Guidelines and ss 4–8 of Canada's federal *Privacy Act*.

234 See further Chapter 18 (section 18.4.4).

235 Examples are provided in Chapter 4 (sections 4.2–4.3).

Rules falling under the first sub-category are found only in a minority of data protection instruments,[236] though such rules could and should be read into the more common and general requirement that personal data be processed 'fairly'.[237] Regarding the second sub-category of rules, examples of these are provided further below.

As for rules belonging to the third sub-category, influential examples of these are Arts 10–11 of the EC Directive which, in summary, require data controllers to directly supply data subjects with basic information about the parameters of their data-processing operations, independently of the data subjects' use of access rights.[238] None of the other main international data protection instruments lay down such requirements directly.[239] National data protection laws have often applied such requirements only when data are collected directly from the data subject.[240] Some other national laws have required this sort of notification only in relation to particular kinds of data processing, such as disclosure of customer data,[241] though notification in such cases has been independent of whether or not the data controller has collected the data directly from the data subject. The current notification requirements pursuant to national laws of at least EU and EEA Member States have been largely harmonised and expanded in accordance with the EC Directive. At the same time, some of the newly enacted national laws within Europe stipulate duties of information which go beyond the *prima facie* requirements of Arts 10–11 of the Directive. These duties arise in connection with certain uses of personal profiles and video surveillance.[242]

Thirdly, there are rules which grant persons the right to gain access to data kept on them by other persons and organisations. For the sake of brevity, this right is described hereinafter as simply 'the right of access' or 'access right(s)'. Most, if not

---

236 See examples, *supra* n 211.

237 See further Chapter 18 (section 18.4.1).

238 The provisions are described in more detail in Chapter 18 (section 18.4.5).

239 The UN Guidelines' 'principle of purpose specification' (principle 3) stipulates that the purpose of a computerised personal data file should 'receive a certain amount of publicity or be brought to the attention of the person concerned'. Cf the more generally formulated 'Openness Principle' in para 12 of the OECD Guidelines: 'There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller'. Articles 10–11 of the Directive are supplemented by Art 21 which requires Member States to 'take measures to ensure that processing operations are publicized' (Art 21(1)) and to ensure that there is a register of processing operations open to public inspection (Art 21(2)).

240 See, eg, s 552a(e)(3) of the US Act, IPP 2 of the Australian Act and Art 18(1) of the Swiss Act (only in relation to 'systematic' collection by federal government bodies).

241 See, eg, s 4b(2) of Denmark's *Private Registers Act* (repealed).

242 In relation to uses of personal profiles, see s 21 of Norway's PDA and s 23 of the Icelandic Act. In relation to video surveillance, see s 40 of Norway's PDA, s 24 of the Icelandic Act and s 6b(2) of the German Act. Section 21 of Norway's PDA is analysed in Chapter 18 (section 18.3.4).

all, data protection instruments make provision for such a right. An influential formulation of the right is given in Art 12 of the EC Directive.[243] This provides persons with a right of access not just to data relating directly to them but also to information about the way in which the data are used, including the purposes of the processing, the recipients and sources of the data, and 'the logic involved in any automated processing of data concerning [the data subject] … at least in the case of the automated decisions referred to in Article 15(1)'.[244] The right in Art 12 is similar to, but also more extensive than, the equivalent rights found in the other main international data protection instruments.[245] None of the latter, with the exception of the UN Guidelines, specifically mention the right to be informed of the recipients of data. None of them specifically mention the right to be informed of the logic behind automated data processing. Most national laws have also omitted specification of the latter rights though this situation no longer pertains in Europe due to adoption of the Directive.

As an aside, very few data protection laws specifically restrict so-called 'enforced access' whereby persons are pushed into utilising their access rights in order to provide a body on which they are dependent (eg, employer, insurance company) with personal information normally unavailable to it.[246] A lonely instance of such a restriction is the 1998 UK *Data Protection Act* (s 56). A similar restriction was also included in the 1992 amended proposal for the EC Directive (Art 13(2)). However, the Directive as it presently stands, fails to remedy the practice of enforced access clearly and directly.[247]

The third major category of rules are those which allow persons to object to others' processing of data on themselves and to demand that these data be rectified or erased insofar as the data are invalid, irrelevant, illegally held, etc. The ability to object is linked primarily to rules prohibiting various types of data processing without the consent of the data subjects. Such rules are especially prominent in the EC Directive, relative to older data protection instruments.[248] Of the latter, some

---

243 See further Chapter 18 (section 18.4.5).

244 Article 15(1) is analysed in detail in Chapter 18 (section 18.3.1).

245 See Art 8 of the CoE Convention, paras 12–13 of the OECD Guidelines and principle 4 of the UN Guidelines.

246 Reference to the practice is made in, ia, the *Fifth Report of the [UK] Data Protection Registrar, June 1989* (HMSO, 1989), Part B, paras 240 & 290; T McBride, 'Coerced release of criminal history information' (1998) 5 *PLPR*, 119; Blume, *Databeskyttelsesret*, *supra* n 93, 175–177.

247 Article 12(a) stipulates that access rights are to be exercised 'without constraint', but it is uncertain if this phrase should be read only in the sense of 'without hindrance' or also in the sense of 'freely'/'without duress'. The French text uses the phrase 'sans contrainte' which arguably connotes both senses, whereas the German text uses the phrase 'frei und ungehindert'. The phrase used in the Danish text ('frit og uhindret') is similar to the German. Cf the Swedish text which only mentions 'utan hinder' ('without hindrance').

248 See espec Art 7(a) of the Directive which stipulates consent as one (albeit alternative) precondition for processing generally.

make no express mention of a consent requirement,[249] while others often stipulate consent in fairly narrow contexts – eg, as a precondition for disclosure of data to third parties.[250] It is important to note that consent is rarely laid down as the sole precondition for the particular type of processing in question; consent tends to be one of several alternative prerequisites. This is also the case with the EC Directive. The alternative prerequisites are often formulated broadly, thereby reducing significantly the extent to which data controllers are hostage to the consent requirement in practice. With regard to Art 7 of the EC Directive, for example, most instances of processing will be able to be justified under the criteria in paras (b)–(f) of the provision.[251]

A specific right to object is also laid down in some data protection laws. The EC Directive contains important instances of such a right, namely in Art 14(a) (which provides a right to object to data processing generally), Art 14(b) (which sets out a right to object to direct marketing) and, most innovatively, Art 15(1) (stipulating a right to object to decisions based on fully automated assessments of one's personal character).[252] These rights to object are not found in other main international data protection instruments.[253] Neither have they existed in the bulk of national laws though this situation no longer pertains in Europe due to adoption of the Directive. As noted in Chapter 1 (section 1.1), the right in Art 15 could well be treated as founding a new data protection principle: ie, that fully automated assessments of a person's character should not form the basis of decisions that significantly impinge upon the person's interests.

With respect to rectification rights, most data protection instruments have provisions which give persons the right to demand that incorrect, misleading or obsolescent data relating to them be rectified or deleted by those in control of the data, and/or require that data controllers rectify or delete such data.[254]

---

249 This is the case with the CoE Convention.

250 See, eg, para 10 of the OECD Guidelines and Art 19(1) of the Swiss Act.

251 These criteria are, in summary, as follows: (b) the processing is necessary for concluding a contract with the data subject; (c) the data controller is legally required to carry out the processing; (d) the processing is necessary for protecting the 'vital interests' of the data subject; (e) the processing is necessary for performing a task executed in the 'public interest' or in exercise of official authority; or (f) the processing is carried out in pursuance of 'legitimate interests' that override the conflicting interests of the data subject. See further discussion of the criteria in Chapter 18 (section 18.4.3).

252 These provisions are described in detail in Chapter 18 (sections 18.3.1 & 18.4.5).

253 Cf principles 5.5, 5.6, 6.10 and 6.11 of the ILO Code of Practice on Protection of Workers' Personal Data (ILO, *supra* n 74) which seek to limit the use of automated decision-making procedures for assessing worker conduct. These principles are described in more detail in Chapter 18 (section 18.3.1).

254 See, eg, Art 12(b) of the EC Directive, Principle 4 of the UN Guidelines, s 14 of the UK Act, Art 13(1)(c) of the Italian Act and IPP 7 of the NZ Act.

3.7 Disclosure Limitation

A sixth core principle of data protection laws is that data controllers' disclosure of personal data to third parties shall be restricted, such that disclosure may occur only upon certain conditions. In practice, disclosure limitation means as a bare minimum that personal data 'should not be disclosed ... except: (a) with the consent of the data subject; or (b) by the authority of law'.[255]

This principle, like that of individual participation and control, is not always expressed in data protection instruments in the manner formulated above. Moreover, neither the CoE Convention nor the EC Directive specifically address the issue of disclosure limitation but treat it as part of the broader issue of the conditions for processing data.[256] Thus, neither of these instruments apparently recognise disclosure limitation as a separate principle but incorporate it within other principles, particularly those of fair and lawful processing and of purpose specification. The OECD Guidelines incorporate the principle of disclosure limitation within a broader principle termed the 'Use Limitation Principle' (para 10), while the UN Guidelines specifically address the issue of disclosure under the principle of purpose specification.

Nevertheless, disclosure limitation is singled out here as a principle in its own right because it tends to play a distinct and significant role in shaping data protection laws. Concomitantly, numerous national statutes expressly delineate it as a separate principle or set of rules.[257]

3.8 Information Security

The principle of information security holds that data controllers should take steps to ensure that personal data are not destroyed accidentally and not subject to unauthorised access, alteration, destruction or disclosure. A representative provision to this effect is Art 7 of the CoE Convention which stipulates:

> 'Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.'

The relevant provisions of the EC Directive are a little more detailed. Article 17(1) requires data controllers to implement security measures for ensuring that personal

---

255 Paragraph 10 of the OECD Guidelines.

256 See espec Arts 5(a), 5(b) & 6 of the Convention, and Arts 6(1)(a), 6(1)(b), 7 & 8 of the Directive.

257 See, eg, s 8 of Canada's federal *Privacy Act*, IPP 11 in both the NZ and Australian Acts.

data are protected from accidental and unlawful destruction, alteration or disclosure. The measures taken are to be commensurate with the risks involved in the data processing 'having regard to the state of the art and the cost of their implementation'. A controller must also ensure – by way of contract or other legal act (Art 17(3)) – that data processors engaged by him/her/it provide 'sufficient guarantees in respect of the technical security measures and organizational security measures governing the processing to be carried out' (Art 17(2)).[258] Further, the measures taken pursuant to Art 17(1) and (3) shall be documented (Art 17(4)).

The principle of information security has occasionally manifested itself in relatively peculiar provisions. Section 41(4) of Denmark's *Personal Data Act* is especially noteworthy. This states that for personal data which are processed for the public administration and which are of particular interest to foreign powers, measures shall be taken to ensure that they can be disposed of and destroyed in the event of war or similar conditions.[259]

3.9 Sensitivity

The principle of sensitivity holds that the processing of certain types of data which are regarded as especially sensitive for data subjects should be subject to more stringent controls than other personal data. The principle is primarily manifest in rules that place special limits on the processing of predefined categories of data. The most influential list of these data categories is provided in Art 8(1) of the EC Directive: it embraces data on a person's 'racial or ethnic origin', 'political opinions', 'religious or philosophical beliefs', 'trade-union membership', 'health' and 'sexual life'. Further, Art 8(5) makes special provision for data on criminal records and the like. Similar lists are found in numerous other data protection instruments at both international and national level, though these vary somewhat in scope. For instance, the list in Art 6 of the CoE Convention omits data on trade-union membership, while the list in the UN Guidelines includes data on membership of associations in general (not just trade unions). The lists in some national laws also include, or have previously included, data revealing a person to be in receipt of social welfare benefits.[260] References to this sort of data, however, have to be dropped from the lists

258 The latter requirements are supplemented in Art 16 which provides: 'Any person acting under the authority of the controller or ... processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law'.

259 A similar rule was found in s 12(3) of the Danish *Public Authorities' Registers Act* of 1978 (repealed) and s 29 of the Icelandic *Protection of Personal Records Act* of 1989 (repealed).

260 See s 6(6) of Finland's *Personal Data Registers Act* of 1987 (repealed), s 4(2) of Sweden's *Data Act* of 1973 (repealed) and Art 3(c)(3) of the Swiss Act.

in the data protection laws of EU and EEA Member States as the list of data categories in Art 8(1) of the Directive is intended to be exhaustive.[261]

Singling out relatively fixed sub-sets of personal data for special protection breaks with the otherwise common assumption in data protection discourse that the sensitivity of data is essentially context-dependant. Accordingly, attempts to single out particular categories of data for special protection independent of the context in which the data are processed, has not been without controversy.[262] Further, not all data protection instruments contain extra safeguards for designated categories of data. This is the case with the OECD Guidelines and the data protection laws of some Pacific Rim countries. The previous data protection regimes of some European countries – notably Austria, Germany and the UK – also provided relatively little protection for such data.

The absence of extra safeguards in the OECD Guidelines appears to be due partly to failure by the Expert Group responsible for drafting the Guidelines to achieve consensus on which categories of data deserve special protection, and partly to a belief that the sensitivity of personal data is not an *a priori* given but dependant on the context in which the data are used.[263] The previous or current absence of extra protections for designated categories of especially sensitive data in some national data protection laws would appear to be due to much the same considerations, along with uncertainty over what the possible extra protection should involve.[264]

---

261 See further the discussion of this point in Chapter 18 (section 18.4.3).

262 For a forceful, highly persuasive critique of such attempts, see S Simitis, ''Sensitive Daten' – Zur Geschichte und Wirkung einer Fiktion', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Verlag Stämpfli & Cie, 1990), 469–493. Cf comments in Chapter 7 (section 7.2.1).

263 See the Guidelines' Explanatory Memorandum, paras 43 & 51; P Seipel, 'Transborder Flows of Personal Data: Reflections on the OECD Guidelines' (1981) 4 *TDR*, no 1, 32, 36.

264 See, eg, Law Reform Commission of Hong Kong, *Report on Reform of the Law Relating to the Protection of Personal Data* (Hong Kong Government Printer, 1994), 99ff; ALRC, *supra* n 158, vol 2, paras 1218ff.

4. Monitoring, Supervisory and Enforcement Regimes

4.1 Data Protection Authorities

The overwhelming majority of countries with data protection laws have established special authorities (data protection authorities) to oversee specifically the implementation of these laws. Notable exceptions are the USA and Japan. Repeated attempts to set up a data protection authority at the federal level in the USA have stranded largely on account of Americans' deep-seated antipathy to regulation by governmental agencies.[265]

In carrying out their tasks, data protection authorities are required to be functionally independent of the governments and/or legislatures which establish them.[266] This criterion of independence boils down to the capacity for a data protection authority to arrive at its own decision in a concrete case without being given case-specific instructions by another body as to what line it should take. Yet insofar as such a decision is legally binding (especially with respect to another government agency), it will usually be subject to political and legal review. Moreover, decision making by an authority will be steered at a more general level by laws and regulations laid down by other bodies.[267]

The oversight function of data protection authorities typically encompasses the handling and resolution of complaints by citizens pertaining to the processing of personal data. It can also involve the auditing of the legality of data-processing operations independent of complaints. Additionally, the authorities are often expected to orient and advise governments, parliaments, private organisations and the general public about data protection matters. Concomitantly, an authority is usually under a duty to maintain a publicly accessible register (hereinafter termed 'oversight register') containing basic details of various data-processing operations covered by

265 See generally Gellman, *supra* n 90, 199–238; Michael, *supra* n 92, 83–84.

266 See, eg, Art 28(1) of the EC Directive.

267 Of course, a range of other administrative, economic and political mechanisms will also tend to undermine their functional independence. An instructive, detailed analysis of the workings of these mechanisms with respect to the national data protection authorities of Sweden, France, the Federal Republic of Germany and Canada is given by David Flaherty in *Protecting Privacy in Surveillance Societies* (Chapel Hill/London: University of North Carolina Press, 1989).

the country's data protection law[268] and to deliver an annual report of its activities to the national government and/or parliament.[269]

The powers of data protection authorities are often broad and largely discretionary.[270] In most cases, the authorities are empowered to issue legally binding (though appealable) orders. In some jurisdictions, however, the authorities either do not have such competence at all,[271] or they have not had it in relation to certain sectors.[272]

Turning to the international data protection instruments, the most detailed treatment of the competence and functions of data protection authorities is found in the Directive. Article 28(1) requires each EU Member State to establish one or more data protection authorities (termed 'supervisory authorities') which are to 'act with complete independence in exercising the functions entrusted to them'. The reference to 'complete independence' means that great care must be taken in ensuring that the authorities' inevitable *administrative* dependence on other bodies (eg, through budget and personnel allocations) does not undermine the functional independence they are otherwise supposed to have. It also means that administrative and legal frameworks which leave open even a small possibility of a data protection authority being instructed by another administrative body on how to exercise its functions, most probably do not satisfy the criterion of Art 28(1).[273]

According to Art 28(2), the data protection authorities must be consulted when administrative measures or regulations concerning data protection are drawn up (Art 28(2)). They shall also be empowered to monitor, investigate and intervene in data-processing operations, hear complaints and take court action in the event of breach of national data protection law (Art 28(3) & (4)). At the same time, they shall be required under Art 21(2) to maintain a publicly accessible register containing

---

268 See, eg, Art 21 of the EC Directive (dealt with below).

269 See, eg, ss 38–40 of the Canadian federal *Privacy Act* and Art 31(1)(n) of the Italian Act. Cf Art 28(5) of the EC Directive.

270 For examples, see Chapter 18 (section 18.4.7).

271 The case with, eg, Germany's Federal Data Protection Commissioner (*Bundesdatenschutz-beauftragter*): see the *Federal Data Protection Act*, espec ss 24–26.

272 The case with, eg, Denmark where the national data protection authority previously had only advisory capacity in relation to the public sector: see ss 27–28 of the *Public Authorities' Registers Act* (repealed). A special case is Finland where primary responsibility for oversight and enforcement of national data protection legislation has been divided between two bodies: the Data Protection Ombudsman ('dataombudsmannen') and the Data Protection Board ('datasekretessnämden'). Under the *Personal Data Registers Act* of 1987 (repealed), the ombudsman had mainly advisory competence though extensive investigatory powers; by contrast, the board had power to issue legally binding orders, including competence to set aside provisions in the Act on a case-by-case basis. The latter competence has been abolished under chapt 9 of the new *Personal Data Act*, whilst the competence of the ombudsman to give legally binding orders has been strengthened.

273 An example of such a framework is the previous system in Norway whereby the Ministry of Justice, upon which the Data Inspectorate is administratively dependant, acted as primary instance for the determination of appeals from the Inspectorate's decisions: see further Chapter 1 (section 1.4.3).

information about the data-processing activities of which they are notified pursuant to, indirectly, Arts 18–19 (dealt with in the next section).

The Directive is silent on whether or not data protection authorities shall be able to impose fines and order compensation for damages though such competence would clearly be compatible with the Directive. The Directive also does not specifically address whether or not these authorities *must* be given competence to issue legally binding orders. Article 28(3), read in conjunction with recitals 9–11,[274] tends to suggest that such competence is required but the wording is not entirely conclusive:[275] authorities are to be given 'effective powers of intervention, such as, for example, that of delivering opinions ..., ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing ...'. It could be argued that the various types of powers listed here are examples only of *options* that Member States may choose between, not necessary constituents of the concept 'effective powers of intervention'; if they were intended to be regarded as necessary constituents, the term 'including' would have been used instead of 'such as, for example'.[276] Moreover, the wording of the provision indicates that the notion of 'intervention' is to be read broadly, such that it covers mere delivery of opinion. As for the criterion 'effective', nothing in the Directive (or its *travaux préparatoires*) conclusively indicates that this can *only* be satisfied through imposition of legally binding orders.[277]

The considerable detail with which the Directive treats the competence and obligations of national data protection authorities contrasts starkly with the other international data protection instruments. The OECD Guidelines have little to say about the need for, and competence of, national data protection authorities. Indeed, they do not require such authorities to be established. A similar situation has pertained up until recently with the CoE Convention. However, an additional

---

274 Set out *supra* n 135.

275 The *travaux préparatoires* are also not entirely conclusive on this point. See, eg, COM(92) 422 final – SYN 287, 15.10.1992, 38 ('To enable the supervisory authority to carry out its duties it must also have effective powers of intervention, such as those enumerated by the Parliament in its opinion, and repeated in the amended proposal: power to order suppression, erasure of data, a ban on the processing operation, etc. Parliament referred to these measures as 'sanctions', but it does not appear necessary that the Directive should define their legal nature').

276 See also the statement of the Council's reasons regarding adoption of the common position for the Directive ('The supervisory authorities' powers of intervention are described in indicative fashion only, so as to allow Member States the requisite leeway in this area'): OJ No C 93, 13.4.1995, 24.

277 Indeed, there is evidence to suggest that the recommendations of an ombudsman can sometimes be as equally effective as such orders. On this point, see Flaherty's comprehensive study (referred to *supra* n 267) which concludes, ia, that the German Federal Data Protection Commissioner, despite having only advisory powers, has had a more pervasive and profound impact on the (federal) public sector in Germany than Sweden's Data Inspection Board has had on the Swedish public sector: *ibid*, 26. It is noteworthy that the amendments to the German *Federal Data Protection Act* which were intended to transpose the Directive, retain the ombudsman-type competence of the Federal Data Protection Commissioner: see further ss 24–26 of the Act.

Protocol to the Convention was adopted on 23.5.2001 by the CoE Committee of Ministers, replicating (in Art 1) the basic thrust of Art 28 of the Directive.[278] As for the UN Guidelines, these specifically address the need to establish national data protection authorities that are 'impartial', 'independent' and 'technically competent' (para 8).

The Directive contains several provisions which will stimulate an internationalisation, at least within the EU, of supervisory and monitoring regimes in the field of data protection. An important provision in this regard is Art 28(6) which provides that Member States' respective data protection authorities:

- may exercise their powers in relation to a particular instance of data processing even when the national law applicable to the processing is that of another Member State;
- may be requested by another Member State's authority to exercise their powers; and
- are to 'cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information'.

The above provisions should entail relatively high levels of co-operation between national data protection authorities. They should also entail increased knowledge and expertise within each of these authorities of other Member States' data protection laws.

Further, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter termed 'Data Protection Working Party') has been established pursuant to Art 29. This body is mainly composed of representatives from each Member State's data protection authority. It acts independently of the Commission and other EU organs but has advisory competence only. Under Art 30, it is to aid the Commission by providing advice on: issues relating to the uniform application of national measures adopted pursuant to the Directive; data protection afforded by non-Member States; possible changes to the Directive and other instruments affecting data protection; and codes of conduct drawn up at Community level.

On a more general note, sight should not be lost of the fact that data protection authorities are not alone in monitoring, encouraging and/or enforcing the implementation of data protection laws. A great number of other bodies are involved to varying degrees in one or more of the same tasks, even if their participation is not always formally provided for in data protection instruments.

On the international plane, notable examples of relevant bodies are the expert committees on data protection and information policy formed under the umbrella of

---

278 *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) regarding supervisory authorities and transborder data flows*, ETS No 179, open for signature 8.11.2001. The Protocol will enter into force upon ratification by five of its signatories (Art 3(3)(a)). As of 23.5.2002 only one State (Sweden) has ratified the Protocol.

the CoE and OECD. A variety of other inter- and non-governmental organisations are also emerging to play a role in the setting of data protection standards. These include the World Trade Organisation (WTO), World Intellectual Property Organisation (WIPO) and World Wide Web Consortium (W3C).[279] Within the EU, especially relevant bodies are the above-mentioned Data Protection Working Party, the Commission,[280] and the Committee of Member State representatives which is to assist the Commission under Art 31 of the EC Directive.[281]

At a national level, obvious examples of relevant bodies are those charged with hearing appeals from the decisions of data protection authorities. Other examples are parliamentary committees, ombudsmen and national auditing offices. In some countries, such as NZ and Germany,[282] data controllers themselves are legally required to appoint internal officers whose tasks are to monitor their respective organisations' compliance with data protection legislation and to function as contacts between the organisations and the data protection authorities.

Further, some countries' laws make specific provision for industries, professions, etc to draw up sectoral codes of conduct/practice on data protection in co-operation with data protection authorities.[283] An increasing number of schemes for the development of such codes is likely, given that the EC Directive requires Member States and the Commission to 'encourage' the drafting of sectoral codes of conduct, at national and/or Community level, in pursuance of the measures contemplated by the Directive (Art 27).[284]

---

279 For a useful overview of these and other international 'players' in the field, see JR Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford L Rev*, 1315, 1355ff. As Reidenberg makes clear, many of these bodies will approach data protection issues from a market-oriented rather than human rights perspective.

280 Note particularly the Commission's considerable powers under the Directive with respect to implementation of the Directive's provisions on transborder data flow (see Arts 25(4)–25(6), 26(3)–26(4)). Principal in this respect is the Commission's power to determine whether a country outside the EU (and EEA) offers an 'adequate' level of data protection for the purposes of Art 25. See further section 4.4.

281 Unlike the Data Protection Working Party, the Committee (hereinafter termed 'Article 31 Committee') has the power to make decisions binding on the Commission. Measures proposed by the Commission are to be approved by the Committee majority. If the latter disagrees with a Commission proposal, the Council – acting by a qualified majority – shall determine the proposal's fate (Art 31(2)).

282 See s 23 of the NZ Act and ss 4f–4g of the German Act.

283 See s 13 of the Irish Act, Parts VI–VII of the NZ Act, s 51(3)–(4) of the UK Act, Part IIIAA of the Australian Act and Art 25 of the Netherlands' Act.

284 Cf para 19(b) of the OECD Guidelines urging Member States to 'encourage and support self-regulation, whether in the form of codes of conduct or otherwise'. Neither the Guidelines nor Directive, however, provide any indication of the exact legal status to be given such codes.

4.2 Notification and Licensing Schemes

Most data protection laws lay down special rules to enhance the ability of data protection authorities to monitor the practices of data controllers. There are two main categories of such rules. The basic differences between these categories lie in the degree to which the data protection authority monitors data-processing activities *before* the latter begin, and the degree to which such monitoring involves formal authorisation of these activities.

One category requires data controllers simply to notify data protection authorities of certain planned processing of personal information. Upon notification, processing is usually allowed to begin. Most data protection laws, including the EC Directive (see below),[285] operate with this sort of requirement, though the ambit of their respective notification schemes has varied.[286]

Occasionally, the notification requirement is, or has been, formalised as a system for registration.[287] Under this sort of system, data controllers must as a general rule apply to be registered with the data protection authority, registration being a necessary precondition for their processing of personal data. When applying for registration, a controller is to supply the authority with basic details of its intended processing operations. Once application for registration is lodged, the controller is legally able to begin processing.

The Directive requires, subject to several derogations, that data controllers or their representatives notify the authority concerned of basic information about 'any wholly or partly automatic processing operation' they intend to undertake (Art 18(1)). With some exceptions, the types of information to be notified must include 'at least':

a) the identity of the data controller and his/her/its representatives;
b) the purposes of the data processing;
c) the categories of data subject and data held on the latter;
d) the categories of recipients of the data;
e) proposed data transfers to third countries; and
f) a general description of adopted security measures for the processing (Art 19(1)).

The second category of control/oversight scheme requires that data controllers must apply for and receive specific authorisation (in the form of a license) from the relevant data protection authority prior to establishing a personal data register or engaging in a particular data-processing activity. Only a minority of countries

---

285 The other three main international data protection instruments, however, refrain from specifically laying down requirements for notification or for other control schemes.

286 See further the overview by the Data Protection Working Party in its Working Document of 3.12.1997 on 'Notification', <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp8en.htm>.

287 The case under, eg, Arts 28–30 of the Hungarian Act and ss 4–9 of the UK Act of 1984 (repealed).

operate, or have operated, with comprehensive authorisation/licensing regimes.[288] It has been more common for countries to reserve a licensing requirement for certain designated sectors of business activity, such as credit reporting,[289] or for overseas transfers of personal data,[290] or for the matching of such data.[291]

The EC Directive allows for a system of 'prior checking' by national data protection authorities with respect to processing operations that 'are likely to present specific risks to the rights and freedoms of data subjects' (Art 20(1)). Elaborating on what might constitute such processing operations, recital 53 refers to operations that are likely to pose specific risks 'by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies'. It would appear from Art 28(3) of the Directive, together with recitals 9, 10 and 54, that data protection authorities may stop planned data-processing operations pursuant to this system of 'prior checking'.[292] Recital 54 makes clear, though, that such a system is to apply only to a minor proportion of data-processing operations: 'with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited'. In other words, data protection regimes in which licensing is the rule rather than exception do not conform with the Directive.

At the same time, the fact that the Directive permits (though does not mandate) some licensing in addition to notification schemes, plus describes the preconditions for such licensing in a rather vague, open-ended way, provides (yet) another possibility for significant divergence in the regulatory regimes of EU/EEA Member States. We find already instances of such divergence. For example, Sweden's *Personal Data Act* dispenses with any licensing requirement, providing instead for mere notification (s 36).[293] By contrast, Norway's *Personal Data Act* retains a licensing requirement for the processing of sensitive data (s 33),[294] though with some

---

288 Such regimes have been set up pursuant to Norway's *Personal Data Registers Act* (repealed), Sweden's *Data Act* of 1973 (repealed), the French Act (in relation to the public sector) and Luxembourg's *Act of 31.3.1979 Regulating the Use of Nominative Data in Computer Processing* (*Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques*). Most of these regimes also allow(ed) for derogation from their licensing requirements. With respect to the old Norwegian licensing scheme, see further Chapter 18 (section 18.4.7).

289 See, eg, s 15 of the Icelandic Act of 1989 (repealed).

290 See section 4.3 below.

291 See, eg, ss 4(4) and 4(5) of Denmark's *Private Registers Act* (repealed).

292 Article 28(3) provides that authorities generally are to have 'effective powers of intervention', including the ability to impose 'a temporary or definitive ban on processing'. Recital 54 specifies that an authority may 'give an opinion or an authorization' following a prior check.

293 The notification requirement does not apply if the data controller has appointed an internal data protection officer (s 37), though allowance is made for government regulations to override this exemption in cases involving 'particular risks for improper intrusion on personal integrity' (s 41).

294 These are basically the data types described in Art 8 of the Directive (see s 2(8) of the PDA).

exemptions.[295] The Data Inspectorate is also empowered to determine, on a case-by-case basis, that other data-processing operations require licensing when they 'obviously infringe weighty data protection interests' ('åpenbart vil krenke tungtveiende personverninteresser') (s 33(2)).

Licensing, registration and notification procedures exist not simply for the purposes of direct control on the part of data protection authorities; they also function partly as learning/sensory mechanisms in the face of legislators' uncertainty about the appropriate regulatory response to data-processing activities. The schemes force data controllers to come in contact with data protection authorities, thereby allowing the latter (and, indirectly, data subjects and the public generally) to learn about controllers' practices and needs, and allowing the authorities to educate controllers about data protection rules.[296]

4.3 Sanctions and Remedies

All data protection Acts stipulate a variety of sanctions and remedies for breach of their provisions. Provision is usually made for a combination of penalties (fines and/or imprisonment), compensatory damages and, where applicable, revocation of licenses and deregistration. Sometimes, strict/objective liability for harm is stipulated.[297] Sometimes too allowance is made for the imposition of ongoing enforcement damages during the time in which a data controller fails to comply with the orders of a data protection authority.[298] In many cases, compensation may be awarded for non-economic/immaterial injury (emotional distress) as well as economic loss.[299] In a very few cases, allowance is made for class actions to be brought.[300]

The topic of sanctions and remedies is dealt with in only very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EC Directive is more specific. It requires that data subjects be given the right to a 'judicial remedy' for 'any breach' of their rights pursuant to the applicable national data protection law

---

295 Licensing is not required if the data subject has voluntarily supplied the data or the processing is carried out by a government agency pursuant to statutory authorisation (s 33(1)) or the processing consists of video surveillance for the purposes of crime control (s 37(2)).

296 On this 'learning' aspect of data protection governance, see further CD Raab, 'Data Protection in Britain: Governance and Learning' (1993) 6 *Governance*, 43, 53ff; CD Raab, 'Implementing data protection in Britain' (1996) 62 *Int Rev of Administrative Sciences*, 493, 507–508; Burkert, *supra* n 19, 180ff.

297 See, eg, s 49(2) of the Norwegian Act in relation to harm caused by credit reporting agencies.

298 See, eg, s 47 of the Norwegian Act and s 41 of the Icelandic Act.

299 See, eg, s 48 of the Swedish Act, s 47(1) of the Finnish Act and s 52(1A) of the Australian Act.

300 See ss 36(2), 38, 38A–38C & 39 of the Australian Act and s 37(2) of Hong Kong's *Personal Data (Privacy) Ordinance 1995*. See further Chapter 15 (section 15.5).

(Art 22). It also stipulates that decisions by a data protection authority which give rise to complaints 'may be appealed against through the courts' (Art 28(3)).[301]

Article 22 does not require Member States to permit individuals to go directly to the courts for breach of data protection rights (effectively bypassing the national data protection authorities) but leaves it open for Member States to allow direct access to the courts.[302] Less clear is whether the reference to 'rights' also embraces those provisions in the Directive that are formulated as duties or obligations on data controllers. Given that breach of a duty or obligation is likely to result in infringement of a data subject's general right to privacy (a right that is indirectly, if not directly, guaranteed by the Directive),[303] and given that the Directive aims at ensuring a 'high' level of data protection,[304] an affirmative answer to the question seems most correct.

Ambiguity inheres also in Art 28(3): does it require Member States to permit court appeals on both questions of law and questions of fact, or are States able to restrict appeals to questions of law only? As the term 'complaints' is not qualified in any way, the provision appears to encourage if not require a broad right of appeal. Yet EU/EC legislators would probably be exceeding their legal competence if the provision were to require changes to present domestic rules limiting judicial review of administrative decisions to questions of law.

Turning to the issue of compensation, the Directive stipulates that in the event of suffering damage from a breach of national provisions adopted pursuant to it, data subjects must be able to receive compensation from the data controller responsible for the damage (Art 23(1)). However, Art 23(2) allows for the complete or partial exemption of data controllers from liability if they are able to prove that they are 'not responsible for the event giving rise to the damage'. The provisions in Arts 22 and 23 are backed up by Art 24, which requires Member States to adopt 'suitable measures' (notably sanctions) for ensuring 'full implementation' of the Directive's provisions.

The Directive omits to specify clearly whether or not the notion of damage in Art 23 covers both economic and non-economic (eg, emotional) loss. Weighing in favour of a broad interpretration of the damage concept in Art 23 are recitals 9 and

---

301 Article 28(3) also addresses the issue of standing with respect to data protection authorities: each such authority is to be given 'the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities'.

302 Cf Article 22 of the 1992 Amended Proposal for the Directive ((COM(92) 422 final – SYN 287, 15.10.1992) which makes no mention of administrative remedies prior to court referral: 'Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed by this Directive'. Had this provision been adopted, data subjects would have found it easier to go straight to the courts with their complaints, bypassing national data protection authorities and any other administrative complaints-resolution bodies.

303 See especially Art 1(1).

304 See especially recital 10 in the Directive's preamble, set out *supra* n 135.

10.[305] Further, the Commission's intention with respect to the equivalent provisions in its 1990 Directive proposal was that '[t]he concept of damage covers both physical and non-physical damage'.[306] Nothing indicates that this intention changed in the subsequent drafting process leading to adoption of the Directive,[307] and nothing indicates that this intention has not been shared by either the European Parliament or Council.[308] Given the ambiguity of the Directive's provisions on this point, the ECJ could well place some weight on this intention if called upon to determine the issue.

In many jurisdictions, the enforcement of data protection laws seems rarely to involve meting out penalties in the form of fines or imprisonment. Data protection authorities appear generally reluctant to punitively strike out at illegal activity with a 'big stick'. A variety of other means of remedying recalcitrance – most notably dialogue and, if necessary, public disclosure via the mass media – seem to be preferred instead.[309] In other words, data protection laws often function to a relatively large extent as 'soft law'; ie, law which 'works by persuasion, is enforced by shame and punished by blame'.[310]

4.4 Transborder Data Flows

All European data protection laws contain rules providing for restrictions to be put on the flow of personal data to countries without sufficient levels of data protection. The chief aim of these rules is to hinder data controllers from avoiding the requirements of data protection laws by shifting their data-processing operations to countries with

---

305 Set out *supra* n 135. Cf recital 55 which states that 'any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller'. However, one cannot place much weight on the presence of 'any' in the English text of the recital since other texts, such as the French, German, Danish and Swedish, omit the adjective altogether.

306 COM(90) 314 final – SYN 287, 13.9.1990, 40. Again, both terms are somewhat diffuse, but the reference to 'non-physical damage' (the German text uses the term 'immateriell Schaden'; the French text 'le préjudice moral') seems sufficiently broad to embrace emotional distress.

307 See, eg, COM(92) 422 final – SYN 287, 15.10.1992, 33 ('Article 23(1), like Article 21(1) in the initial proposal, places a liability on the controller to compensate *any* damage caused to any person ...': emphasis added). The German text is similar ('Schadenersatz für jeden Schaden einer Person zu leisten'), though not the French text ('une obligation de réparer le préjudice causé à toute personne').

308 The Data Protection Working Party claims that the notion of damages in the Directive 'includes not only physical and financial loss, but also any psychological or moral harm caused (known as 'distress' under UK or US law)': see Data Protection Working Party, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', Working Document adopted 24.7.1998, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf>, 13.

309 My impressions here are based on perusal of the annual reports issued by the data protection authorities of Australia, Denmark, Norway, Switzerland and the UK, together with Flaherty's description (see *supra* n 267) of enforcement practices in Sweden, France, Canada and the Federal Republic of Germany.

310 E Blankenburg, 'The Invention of Privacy', in P Ippel, G de Heij & B Crouwers (eds), *Privacy disputed* (The Hague: SDU/Registratiekamer, 1995), 31, 39.

more lenient requirements (so-called 'data havens').[311] This concern has rarely been shared to the same degree by legislators of data protection laws in non-European countries; accordingly, many of these laws have not contained rules specifically allowing for restrictions on transborder flows of personal data. Such rules, though, are increasingly being incorporated in non-European legislation, largely under the influence of the EC Directive (see below).

Up until recently, the basic principle applied by the rules on transborder data flow has tended to be that the transfer of personal data to another country is permitted if the latter provides a level of data protection which is equivalent to the protection provided by the law of the country from which the data are intended to be transferred.[312] As elaborated upon further below, this equivalency criterion is increasingly being supplemented and, in some contexts, replaced by an adequacy criterion. In order to ensure effective application of such criteria, countries often require (with some exceptions) that intended cross-border transfers of personal data be checked and sometimes licensed by their respective national data protection authorities.[313]

All of the four main international instruments on data protection contain rules specifically addressing the matter of transborder data flows. The relevant rules in the CoE Convention are set out in Art 12 and the Additional Protocol to the Convention adopted in May 2001 (though not yet in force).[314] Article 12 primarily concerns the flow of personal data between States Parties to the Convention. It stipulates that a Party 'shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party' (Art 12(2)). However, it permits (though does not require) derogation from this prohibition insofar as the data concerned are specifically protected pursuant to the State Party's legislation and the regulations of the other Party fail to provide 'equivalent protection' for these data (Art 12(3)(a)). Derogation is also allowed in order to prevent the transfer of data to a non-Contracting State, via another State Party, in circumvention of the first State Party's legislation (Art 12(3)(b)). As for the flow of personal data from a Party to non-Party State, this is to be governed by Art 2 of the Additional Protocol to the Convention. The rules in Art 2 replicate the broad thrust of Arts 25–26 of the EC Directive (see below).

---

311 See generally Ellger, *supra* n 75, 87ff, and references cited therein. Assertions have been made that these rules are partly intended to protect economic interests as well. These assertions are discussed further in Chapter 6 (section 6.3.2). For a somewhat dated overview of cases in which transborder flows of personal data have been restricted pursuant to data protection laws, see OECD, *Privacy and Data Protection: Issues and Challenges* (Paris: OECD, 1994), 55–59.

312 See the overview of rules in PM Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 *Iowa L Rev*, 471, 474–477. See also Chapter 11 (section 11.3.3).

313 See, eg, ss 19 & 24 of the French Act; Art 6 of the Swiss Act and Art 13 of the Austrian Act. More generally, see Arts 25–26 of the EC Directive described further below.

314 *Supra* n 278.

Broadly similar, but less complicated, principles on transborder data flows are set down in paras 17–18 of the OECD Guidelines and in Principle 9 of the UN Guidelines. The latter differ in some respects from the other instruments in their terminology – employing the (undefined) criteria of 'comparable' and 'reciprocal' protection – though they probably seek to apply essentially the same standards as the criteria of 'equivalency' and 'adequacy'. At the same time, while the Convention and OECD Guidelines have been primarily concerned with regulating flow of personal data between the Member States of the CoE and OECD respectively, the UN Guidelines seek to regulate data flows between a broader range of countries.

Of the provisions dealt with in this section, the rules in the EC Directive have the greatest impact on transborder data flows. Regarding flows of personal data between EU/EEA Member States, the basic rule of the Directive is that such flows cannot be restricted for reasons concerned with protection of the 'fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' (Art 1(1)). This prohibition is premised on the assumption – expressed in recitals 8 and 9 of the Directive and necessitated by Art 12(3)(a) of the CoE Convention – that implementation of the Directive will result in equivalent levels of data protection across the EU/EEA.[315] A fundamental issue here, not least from the perspective of the individual EU/EEA citizen, is whether pan-EU/EEA equivalency in data protection levels will in fact eventuate.

As for transfer of personal data to countries outside the EU/EEA ('third countries'), this is regulated in Arts 25–26. Both provisions are long, complex and raise a variety of legal issues.[316] For present purposes, it is only necessary to present the main rules here.

To begin with, Art 25(1) stipulates that transfer 'may take place only if ... the third country in question ensures an adequate level of protection'. The adequacy of protection 'shall be assessed in the light of all the circumstances surrounding a data transfer or set of data transfer operations …' (Art 25(2)). Assessment of adequacy will in many cases lie firstly with the data exporters and secondly with national data protection authorites in the EU/EEA. However, the EC Commission has been given the power to make determinations of adequacy which are binding on EU (and EEA) Member States (Art 25(6)).[317] The Commission has decided so far that Switzerland,

---

315 See further Chapter 2 (section 2.2).

316 For discussion of these issues generally, see Data Protection Working Party, *supra* n 308; EC Commission, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data* (Office for Official Publications of the EC, 1998); Schwartz, *supra* n 312, 483ff. For discussion of these issues with regard to the operation of systems for digital rights management, see LA Bygrave & K Koelman, 'Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems', in PB Hugenholtz (ed), *Copyright and Electronic Commerce* (The Hague/London/Boston: Kluwer Law International, 2000), 59, 89–93.

317 The Commission does not make such decisions on its own but with input from: (i) the Data Protection Working Party (which may deliver a non-binding opinion on the proposed decision (Art 30(1)(a) &

Hungary and, to a lesser extent, Canada satisfy the adequacy test.[318] The US 'safe harbor' scheme (described further below) has also been found to offer adequate protection. Doubts about the adequacy of the Australian legislation have been expressed by the Data Protection Working Party,[319] but the Commission has yet to make a final decision on the matter.

The impact of the adequacy rule is significantly mitigated by a set of derogations in Art 26. These derogations permit transfer of personal data to a third country lacking adequate protection if, in summary, the proposed transfer:

1) occurs with the consent of the data subject; or
2) is necessary for performing a contract between the data subject and the controller, or a contract concluded in the data subject's interest between the controller and a third party; or
3) is required on important public interest grounds, or for defending 'legal claims'; or
4) is necessary for protecting the data subject's 'vital interests'; or
5) is made from a register of publicly available information (Art 26(1)).

A further derogation is permitted if the proposed transfer is accompanied by 'adequate safeguards' instigated by the controller for protecting the privacy and other fundamental rights of the data subject (Art 26(2)). The latter provision also states that 'such safeguards may … result from appropriate contractual clauses'. In the same way as under Art 25, the EC Commission has the power to make binding determinations of what constitute 'adequate safeguards' for the purposes of Art 26(2) (see Art 26(4)). It has recently exercised this power by stipulating standard contractual clauses that may be used to govern the transfer of data to third countries that do not offer an adequate level of data protection.[320]

(Cont.)
(b)); (ii) the Article 31 Committee (whose approval of the proposed decision is necessary and which may refer the matter to the Council for final determination (Art 31(2)); and (iii) the European Parliament (which is able to check whether the Commission has properly used its powers). The procedure follows the ground rules contained in *Council Decision 1999/468/EC of 28.6.1999 laying down the procedures for the exercise of implementing powers conferred on the Commission* (OJ L 184, 17.7.1999, 23).

318 *Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary* (OJ L 215, 25.8.2000, 4); *Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland* (OJ L 215, 25.8.2000, 1); *Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act* (OJ L 2, 4.1.2002, 13).

319 See 'Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000', adopted 26.1.2001, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40en. htm>.

320 See *Decision 2001/497/EC of 15.6.2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC* (OJ L 181, 4.7.2001, 19); *Decision 2002/16/EC of*

Articles 25–26 have occasioned considerable controversy in some 'third countries'. Concern has been especially vociferous in the USA, which fears that strict application of the provisions will detrimentally affect US business interests.[321] Considerable discussion has emerged there over the provisions' legality under international trade law, most notably the 1994 *General Agreement on Trade in Services* (GATS) which restricts Signatory States from imposing restrictions on transborder data flow in a manner involving arbitrary or unjustified discrimination against other such States.[322] So far, though, there appears to be little hold in claims that the Directive, either on its face or in the way it is being applied, breaches GATS. This is particularly so because GATS allows the imposition of restrictions on transborder data flow which are necessary to secure compliance with rules relating to the 'protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts' (Art XIV(c)(ii)). While such restrictions must also conform with the agreement's basic prohibition against arbitrary or unjustified discrimination between countries and against disguised restrictions on trade in services, little if any solid evidence exists so far to indicate that Arts 25 and 26 of the Directive are being applied in breach of that prohibition.[323]

Some of the tension between the USA and EU has cooled with the common adoption of a 'safe harbor' scheme whereby US bodies are able to qualify as offering adequate protection for personal data flowing from the EU/EEA, by voluntarily adhering to a set of basic data protection principles.[324] Doubt attaches, though, to the long-term viability of the scheme, its legality and to whether it is an appropriate model for regulating data flows to other third countries.[325]

(Cont.)
27.12.2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (OJ L 6, 10.1.2002, 52).

321 See generally PP Swire & RE Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998).

322 See *Agreement Establishing the World Trade Organization* of 15.4.1994, Annex 1B, espec Arts II(1), VI(1), XIV(c)(ii) and XVII. Prominent instances of the US discussion are Swire & Litan, *supra* n 321, and G Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale J of Int L*, 1, 46ff.

323 See further Shaffer, *supra* n 322, 49ff.

324 See *Commission decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce* (OJ L 215, 25.8.2000, 7).

325 As of 23.5.2002, less than 200 organisations have signed up to the scheme: see <http://web.ita.doc.gov/safeharbor/shlist.nsf/>. Evidence exists that many of these organisations so far are failing to abide by all of the scheme rules: see EC Commission Staff Working Paper on the application of the scheme (Brussels, 13.2.2002, SEC (2002) 196), <http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf>. For a trenchant critique of the scheme's utility and legality, see JR Reidenberg, 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 *Houston L Rev*, 717, 740ff.

5. Concluding Observations for Part I

In light of the material in the preceding chapters of Part I, we can see that the rules found in data protection laws belong to two main categories. First, there are rules concerned directly with regulating the processing of personal data. Secondly, there are rules concerned primarily with monitoring and enforcing the first set of rules. The two categories are not entirely separate; some rules fit under both categories.

Both sets of rules are largely procedural in focus: they either relate to the manner in which personal data are processed or to the manner in which rules are implemented. The predominance of procedural concern appears symptomatic of legislators' uncertainty about the nature of the interests to be protected, together with a desire for regulatory flexibility in the face of technological complexity and change.[326] At the same time, there are elements of data protection laws in which the procedural focus is diminished. A prime example of such an element are those provisions designating certain categories of personal data as requiring special protection.

Looking more closely at the first category of rules mentioned above, we see that these in turn can be divided into two main sub-categories. First, there are rules which regulate the manner and purposes of data processing. These apply a variety of criteria (eg, 'fair', 'lawful', 'legitimate', 'objectively justifiable', 'necessary') to steer the processing of personal data along certain avenues. The criteria are based on commonly accepted social values. At the same time, they are sufficiently nebulous to allow for a considerable degree of flexibility in application. In data protection laws, they govern primarily the relationship between, on the one hand, the purposes for which personal data are processed and, on the other hand, the nature of the data controller's ordinary/natural field of activity; they necessitate, in short, that there be a certain connection between the former and latter.

The criteria of fairness and, secondarily, legitimacy also necessitate rules to ensure that the processing of personal data occurs with the participation of the data subjects. The central types of rules in this respect are those requiring that data processing is authorised, publicised and rectifiable. Rules on authorisation include requirements that data processing occurs only on the basis of consent either directly from the data subjects themselves or from bodies that ostensibly act on their behalf (ie, the legislature and agencies – primarily data protection authorities – set up by the

326 See further, eg, H Burkert, 'The Law of Information Technology – Basic Concepts' (1988) *DuD*, 383, 384–385.

legislature). Rules on publicity include requirements that data subjects are notified directly or indirectly of basic details of data-processing operations. Rules on rectifiability stipulate that data subjects or bodies ostensibly acting on their behalf (primarily data protection authorities) are able to intervene in data-processing operations so as to ensure and/or check that the quality of the data involved is adequate for the purposes of the processing.

The second sub-category of rules are not purely procedural in character but relate to the quality of personal data. The criteria they apply (eg, 'accurate', 'relevant', 'adequate') are linked first to the phenomena which the data are supposed to describe or represent and secondly to the purpose(s) for which the data are supposed to be processed. Again, these criteria demand that a certain connection between the two elements exists in both relationships; ie, the data must give a correct picture of the phenomena they are supposed to describe, and they must be relevant and adequate in relation to the purposes for which they are to be processed. As such, these criteria can be seen as instances of a more general utility criterion that can serve the interests of both data controller and data subject.[327]

As for the second main category of rules (ie, those concerned with monitoring and enforcement), these too can be broken up into two main sub-categories. The first sub-category consists of rules that facilitate monitoring and enforcement functions. This includes the above-mentioned rules on authorisation and publicity of data-processing operations. The second sub-category consists of rules that directly concern monitoring and enforcement functions. It embraces rules on assessment of license applications, establishment and maintenance of oversight registers, rights of access and rectification, and sanctions for illegalities. This sub-category of rules can be divided in turn into further groupings, according to which body (data subject, data protection authority, court, etc) is primarily responsible for exercising the rule concerned.

Present monitoring and enforcement regimes set up by data protection laws are a mixture of reactive and anticipatory forms of control. They focus on dealing with problems that arise after data-processing operations have been initiated, as well as problems that might occur beforehand. Primary instances of reactive control forms are the provisions for *ex post facto* sanctions for breach of data protection laws. Anticipatory controls are manifest in licensing regimes and the research, advisory and (indirectly) monitoring tasks given to data protection authorities. In practice, the distinction between reactive and anticipatory control forms tends to blur, making it difficult to arrive at valid, cross-jurisdictional generalisations about their respective weighting in data protection regimes. Nevertheless, that only a minority of these regimes operate with extensive licensing requirements prior to the registration and further processing of personal data suggests that the regimes are on the whole formally weighted towards use of relatively reactive control mechanisms. This

327 See further Chapter 7 (sections 7.2.5 and 7.3).

tendency could be counteracted, though, by data protection authorities giving priority to their research and advisory tasks.[328]

The monitoring and enforcement regimes set up by data protection laws are also a mixture of paternalistic and participatory control forms. By 'paternalistic' control is meant control exercised by governmental agencies (in this context, primarily data protection authorities) on behalf and supposedly in the best interests of citizens (data subjects). By 'participatory' control is meant control exercised by citizens themselves. A prime example of paternalistic control forms are licensing requirements. A prime example of participatory control forms are rules requiring data subject consent to processing of data. Under many European data protection regimes, paternalistic forms of control have traditionally predominated over participatory forms, though implementation of the EC Directive changes this weighting somewhat in favour of the latter (see further below).

The policy thrust of many data protection instruments is far from unidirectional. This is especially the case with the EC Directive. It is also the case with the other three main international data protection instruments though to a lesser degree. For example, a basic tension exists in all of them between a concern to strengthen data protection and a concern to ensure also the free flow of personal data across national borders. A similar sort of tension is manifest in the fact that most of the core principles in data protection laws are subject to exceptions.

At the same time, this tension can also be viewed as reflecting a concern for fairness, if fairness is taken as requiring that account be taken of the interests of all parties involved in, or affected by, a given data-processing operation.[329] Concomitantly, data protection laws attempt to secure a balance between, on the one hand, the privacy, integrity and autonomy interests of data subjects and, on the other hand, the economic, social and political interests of data controllers in being able to process personal data. This does not necessarily mean, though, the existence of an equal weighting of the two sets of interests in the respective drafters' motivational concerns. For instance, the drafters of the OECD Guidelines and the EC Directive appear to have been primarily interested in ensuring minimal interference of transborder data flows, with data protection being seen essentially as a means of realising this interest. As shown in Chapter 7 (section 7.3), this sort of motivational dynamic is not unique to these two international instruments: other data protection laws have been enacted largely in order to create acceptance for data-processing activities.

---

328 However, empirical evidence indicates that the pursuit of such tasks, and even the proper implementation of licensing schemes, are often hampered by a paucity of resources: see, eg, the evidence gathered by Flaherty, *supra* n 267, 54–55, 114–115, 138, 158, 199, 391–392.

329 See further Chapter 8.

While data protection laws expound broadly similar core principles,[330] we see numerous differences between them in terms of the monitoring and supervisory regimes they establish. The basic differences here relate to the powers of data protection authorities (eg, some function essentially as ombudsmen, others are able to issue legally binding orders) and, accordingly, the nature of the legal preconditions for processing personal data (eg, some require mere notification of processing, others require licensing). There are also significant differences in the ambit of data protection laws: some cover data processing in both the private and public sectors, others cover processing by certain government agencies only; some regulate both manual and automated processing methods, others regulate only the latter; some place restrictions on the flow of personal data to foreign countries, others do not; some provide express protection for data on collective entities, others protect data on individuals only; some lay down extra limits on the processing of designated categories of especially sensitive data, others do not. To some extent, these differences constitute a cleavage line between European and non-European data protection regimes, with the former offering generally more comprehensive and stringent safeguards than the latter, but the line is far from clean.[331]

Under the influence of the EC Directive, though, we can expect a reduction in these differences, at least within the EU/EEA. Nevertheless, it is extremely doubtful that we will see, at least in the short-term, complete or even near-complete uniformity achieved in the data protection regimes of these States. The Directive gives too much reign to the principle of subsidiarity to be able to achieve such uniformity.

Moving from the oldest of the data protection instruments to the youngest, we can discern certain regulatory trends. In data protection discourse, it is popular to categorise these trends in terms of 'generations'; ie, one differentiates between, ia,

---

330 No attempt is made here to canvass in detail possible reasons for this policy convergence, as an excellent study of the matter has already been carried out by Colin Bennett: see Bennett, *supra* n 5, espec chapt 4. Bennett canvasses five hypotheses: convergence has been due to (1) similarity of perceived technological threats, which has forced policy makers to adopt similar solutions; (2) the desire on the part of policy makers to draw lessons from, and emulate, policies adopted earlier in other countries; (3) agreement amongst a small, cross-national network of experts as to appropriate data protection policy; (4) harmonisation efforts of international organisations, particularly the CoE and the OECD; and (5) 'penetration' (ie, a process in which countries are forced to adopt certain policies because of the actions of other countries). Bennett finds that none of these hypotheses *on its own* adequately explains the policy convergence but that they have considerable explanatory power in combination with each other: *ibid*, 150.

331 Again, it is beyond the scope of this book to present in detail possible explanations for these differences. I point again to the study by Bennett (*ibid*, espec chapt 6) for an excellent analysis of this issue. As with his examination of the reasons for policy convergence in terms of core data protection principles, Bennett finds that no one theory or hypothesis suffices to explain national divergence in how these principles have been implemented: *ibid*, 219.

'first-', 'second-' and 'third-generation' data protection laws.[332] However, the analytical utility of employing such fixed chronological categories is diminished by the fact that the trends concerned are often more gradual than the categories indicate. Concomitantly, use of the categories can easily result in ambiguous or misleading generalisations in which distinctions are overstated.[333] Accordingly, these categories are not employed in the following analysis.

The regulatory trends are most easily discernible when comparing the international data protection instruments. First, we see a trend towards more detailed, discriminating provisions and requirements; in short, we see increasing regulatory density. Secondly, we detect an increasing concern to lay down procedural mechanisms for enforcing compliance with data protection principles. Compare, for instance, the simple provisions in the CoE Convention and OECD Guidelines on 'fair' processing of personal data with the more elaborate provisions in Arts 10, 11 and 15 of the EC Directive.

We can also discern some shift in regulatory focus, or, perhaps more accurately, *consolidation* of such shift. An important example here is the EC Directive's focus on the processing of personal data rather than the establishment and use of personal data files (a focus already present in the OECD Guidelines). Another important example is the Directive's focus on manually processed data in addition to automated data processing (again, a focus already present in the OECD Guidelines). Yet another noteworthy example is the Directive's explicit encouragement of the creation of sectoral codes of practice (again, something already anticipated by the OECD Guidelines and, more indirectly, the CoE's various data protection recommendations). This encouragement, though, is offset by a lack of consensus and certainty over exactly what sort of legal function such codes are to have *vis-à-vis* data protection laws within the EU.

Further, there is a discernible trend away from comprehensive licensing regimes to requirements for mere notification/registration of data-processing operations. This is a development in which anticipatory control by data protection authorities gives way to (though is not necessarily extinguished by) more reactive control on the part of such authorities. This development is offset by enhancement (at least on paper) of

---

332 See, eg, V Mayer-Schönberger, 'Generational Development of Data Protection in Europe', in PE Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT Press, 1997), 219–241; Rodotà, *supra* n 19, 267; and Bing, *supra* n 19, 252, 254 & 259.

333 See, eg, Mayer-Schönberger's claim that so-called second-generation laws in Europe (described as those laws introduced in the late 1970s and early 1980s) broke with their first-generation counterparts by, ia, providing for greater opportunities for participatory control: Mayer-Schönberger, *ibid*, 227. While many of the data protection Acts concerned – especially the French Act of 1978 – do place more emphasis on participatory control than was the case, say, with Sweden's *Data Act* of 1973, the differences on this point are often marginal. Rules expressly providing for data subject consent fail to play a central regulatory role in, eg, the relevant Acts of Norway, Luxembourg and the UK. Moreover, such rules are entirely absent from the face of the CoE Convention.

the opportunities for participatory control: data subjects' access rights are supplemented by more extensive notification duties for data controllers, and there is greater readiness to make the consent of data subjects a prerequisite for certain kinds of data processing. Certainly, this gives individuals more room to determine for themselves the manner and extent to which data on them are processed, though it does not necessarily mean that individuals will act to limit such processing or that such processing will decrease.[334] Moreover, data controllers will often be able to avoid the consent rule because of the existence of broadly drawn, alternative requirements for the data processing in question.

334 Indeed, it is plausibly argued that individuals will tend to consent to data processing on account of 'privacy myopia' – ie, their inability to properly value the worth of their data in market terms. See further AM Froomkin, 'The Death of Privacy?' (2000) 52 *Stanford L Rev*, 1461, 1501ff.

PART II:
ORIGINS, RATIONALE AND CHARACTER OF DATA PROTECTION LAWS

6. Catalysts for Emergence of Data Protection Laws

6.1 Introduction

This chapter and the next take up the question of why data protection laws exist. In attempting to provide answers to this question, an examination is made in this chapter of the catalysts for the emergence of data protection laws. The following chapter examines the various interests these laws embody and the various values they aim to safeguard or promote. There is some overlap between the discussion in the two chapters, as the catalysts point to many of the relevant interests and values.

The catalysts for the emergence (and continued existence) of data protection laws fall into three broad categories: (i) technological and organisational developments, and the factors that drive them; (ii) public fears about these developments; and (iii) legal factors. In the following, each of these categories is trreated in the order they are listed above.

6.2 Technological and Organisational Developments

6.2.1 DEVELOPMENTS GENERALLY

The emergence of data protection laws, along with their continued existence, cannot properly be explained without taking account of developments in information technology (hereinafter also termed 'IT') particularly from the onset of the computer age in the 1950s. These developments have brought vastly expanded possibilities for amassing, linking and accessing personal data. The discourse of the 1960s and 1970s out of which data protection laws emerged, shows a preoccupation with these possibilities.[335] Hence, it is with some justification that data protection laws have

335 In the USA, see particularly AF Westin, *Privacy and Freedom* (New York: Atheneum, 1967), chapts 7 & 12; AR Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor: University of Michigan Press, 1971), chapts I–III. Both works have also been influential outside the USA. In the UK, see, eg, M Warner & M Stone, *The Databank Society: Organizations, Computers, and Social Freedom* (London: Allen & Unwin, 1970); P Sieghart, *Privacy and Computers* (London: Latimer, 1976), espec chapts 2 & 3. In Norway, see, eg, E Samuelsen, *Statlige databanker og personlighetsvern* (Oslo: Universitetsforlaget, 1972), 11–12 & chapt 4; *Offentlige persondatasystem*

been characterised as regulatory reactions to technological developments.[336] This notwithstanding, the core concern in data protection laws for safeguarding personal privacy and related values, has roots reaching much further back in time than the onset of the computer age.

One aspect of the technological developments alluded to above has been the strengthening of the technical capabilities of IT in terms of the operational inter-connectivity, speed, bandwidth and intelligence of computers. A related aspect has been the increasing miniaturisation and ubiquity of IT products. Both these aspects have been of some concern in the discourse out of which data protection laws have sprung. Yet of more immediate concern have been certain patterns (partly facilitated by the above-mentioned technical strides) in processing of data, particularly personal data.

During the early discourse on data protection issues, some of these patterns were little more than theoretical possibilities; in later years, all of them have become more or less manifest in concrete processes. To some extent, they overlap with each other.

Two developments figure centrally: (i) growth in the amount of personal data held by various types of organisations; and (ii) integration of these data holdings into centralised databanks. An early manifestation of these developments were proposals during the 1960s to establish centralised population registers.[337] Another early manifestation were plans by several European governments to carry out national population censuses around 1970.[338] Further manifestations can be seen in efforts to introduce common criteria (eg, multi-purpose Personal Identification Numbers (PINs)) for referencing stored data.[339] All of these schemes provided a great deal of fuel for the public debates that helped set in motion the first round of investigative and legislative processes for enactment of data protection laws.[340] Public concern

---

(Cont.)

og personvern, NOU 1975:10, espec 10ff; *Persondata og personvern*, NOU 1974:22, espec 6–7, 28ff. In Sweden, see particularly *Data och integritet*, SOU 1972:47, espec 30–32 & chapts 3–7. In Switzerland, see espec *Botschaft zum Bundesgesetz über den Datenschutz vom 23.3.1988*, 4–5. For a general overview of this discourse and the issues motivating it, see Bennett, *supra* n 5, espec chapt 2.

336 See, eg, S Simitis, 'Auf dem Weg zu einem neuen Datenschutzrecht' (1984) *Informatica e diritto*, no 3, 97, 105; Swire & Litan, *supra* n 321, 50; Burkert, *supra* n 19, 170.

337 The most high-profile instance was the proposal to set up a National Data Center in the USA which would consolidate in one database all information on US citizens held by federal government agencies, ostensibly for the purpose of improving social planning: see further Miller, *supra* n 335, 54–67.

338 See generally Bennett, *supra* n 5, 51–53.

339 See, eg, the Scandinavian countries' comprehensive, public sector schemes for referencing personal data by way of unique identification codes.

340 See generally Bennett, *supra* n 5, 46–53. It is worth noting, though, that little public debate about privacy and data protection issues accompanied the introduction of national PIN schemes in the Scandinavian countries, mainly because the schemes were put in place prior to widespread use of computers: see KS Selmer, 'Hvem er du? Om systemer for registrering og identifikasjon av personer' (1992) *LoR*, 311, 323 & 332; P Blume, 'The Personal Identity Number in Danish Law' (1989–90) 3 *CLSR*, no 5, 10. Such schemes have generated, nevertheless, a large amount of debate on privacy and

over such schemes centred primarily on their potential to significantly roll back the privacy and autonomy of citizens and undermine in turn the foundations for democratic, pluralist society.[341]

A variety of other, related developments have provided additional fuel for the discourse out of which data protection laws have emerged. One such development is the increasingly extensive and routine sharing of personal data across traditional organisational boundaries. Part and parcel of this development is the growing interest of organisations in basing their decisions on data that already exist in structured format in databases maintained by themselves or other organisations.[342] The development entails that data are frequently put to purposes other than those for which the data were originally collated. In short, the re-use of data tends to lead to their re-purposing. This tendency is frequently manifest when, for example, data collected by government agencies for administrative purposes are exploited commercially,[343] or when data are processed in connection with profiling operations.[344]

Public concern over the development has centred partly on the potential of data sharing/re-use across organisational boundaries to render individual citizens unduly transparent, thereby weakening their power-base *vis-à-vis* (large) organisations. Concern has also centred on the fact that the re-use of data can diminish the role played by the data subjects in decision-making processes affecting them. Of further concern have been certain potential consequences flowing directly from data re-purposing. One such consequence is that data are used contrary to the expectations of the data subject. Another potential consequence is that data are misconstrued and, accordingly, misapplied – ie, used for purposes for which they are not suited.[345]

Instances of such misapplication are part of a broader problem relating to inadequacies in the quality of data held by organisations. An accumulating body of evidence suggests that significant amounts of these data are insufficiently precise, correct, complete and/or relevant in relation to the purposes for which they are

---

(Cont.)

data protection issues in subsequent years – not least in countries outside Scandinavia. See, eg, CoE, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (CoE, 1991), espec 20ff; Flaherty, *supra* n 267, espec 15–16, 77–78, 166.

341 See further section 6.3.1 for elaboration of public fears.

342 For further discussion, see, eg, J Bing, 'The informatics of public administration: introducing a new academic discipline' (1992) *Informatica e diritto*, no 1–2, 23, 28ff.

343 For further discussion, see, eg, H Burkert, 'The Commercial Use of Government Controlled Information and its Information Law Environment in the EEC', in WFK Altes, EJ Dommering, PB Hugenholtz & JJC Kabel (eds), *Information Law Towards the 21st Century* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1992), 223–246; P Blume, 'Kommercialisering af offentlig information', in *Ret & Privatisering* (Copenhagen: GadJura, 1995), 65–84.

344 See further Chapter 17.

345 See further, eg, H Burkert: 'Data-Protection Legislation and the Modernization of Public Administration' (1996) 62 *Int Rev of Administrative Sciences*, 557, espec 564–565.

processed.[346] As elaborated upon in section 7.2.3, this problem has featured increasingly as a relatively separate and prominent item of concern in the discourse out of which data protection laws have emerged.

Yet another catalyst for the emergence of data protection law is the increasing automatisation of organisational decision-making processes. Computers are beginning to execute assessments that have customarily been the preserve of human discretion – eg, in the context of determining persons' credit ratings, insurance premiums or social welfare entitlements. This development is closely linked with the above-mentioned growth in data sharing/re-use across organisational boundaries as computerised assessments are increasingly based on pre-collected data found in the databases of third parties. Indeed, with effective communication links between the databases of large numbers of organisations, sophisticated software to trawl these databases, plus appropriate adaptation of the relevant legal rules, computerised decision-making processes have the potential to operate independently of any specific input from the affected data subjects.

Concern over increasing automatisation of decision-making focuses not just on the diminishing influence that data subjects can exercise in such processes. There comes also a fear of automatic acceptance of the validity of the decisions reached. In the words of the EC Commission,

> 'the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities.'[347]

Of related concern is that, at the same time as data subjects' role in organisational decision-making processes is diminishing, the role of their registered data-images is growing. From such an image emerges a 'digital persona' that is increasingly attributed a validity of its own by data controllers.[348] In the context of modern database systems, the digital persona threatens to usurp the constitutive authority of the physical self, despite the necessarily attenuated nature of the former relative to the latter.[349] With (the threat of) usurpation comes (the threat of) alienation.

Also of concern is that the increases in the magnitude and complexity of cross-organisational data flows, and the resultant blurring of organisational lines, is making

---

346 See further section 6.2.3. For closer analysis of the various components of data/information quality, see Chapter 7 (section 7.2.5).

347 COM(92) 422 final – SYN 287, 15.10.1992, 26.

348 For further discussion, see, eg, RA Clarke, 'The Digital Persona and its Application to Data Surveillance' (1994) 10 *The Information Society*, 77–92; M Poster, *The Mode of Information: Poststructuralism and Social Context* (Cambridge: Polity Press, 1990), 97–98.

349 See also J Bing, *Personvern i faresonen* (Oslo: Cappelen, 1991), 12–13, 69; S Bråten, *Dialogens vilkår i datasamfunnet. Essays om modellmonopol og meningshorisont i organisasjons- og informasjonssammenheng* (Oslo: Universitetsforlaget, 1983), 60.

it more difficult for data subjects to trace the flow of data on themselves. Data subjects' ability to control what happens with their various digital personas is concomitantly threatened. Similarly, their ability to identify who or what is responsible for each of the myriad transactions involving their data, plus the full parameters of these transactions, tends to be reduced.[350] Such difficulties are rightly seen as potentially altering the foundations for, and terms of, the 'social contracts' that are implicit in the relations between data subjects and the organisations with which they deal.

It would be wrong to see all of the above developments and attendant concerns as the sole catalysts for the emergence of data protection laws. Just as important are the forces driving the developments.

One such force is modern organisations' enormous appetite for information. This is not to say that the informational appetite of individual persons fails to play any role; organisations are, of course, partly constituted by the desires and needs of individual persons.[351] Nevertheless, the appetite for information on the part of persons acting collectively as formal organisations is most significant for present analytical purposes.

Several scholars claim it was mainly this appetite that brought on the widespread public discussion in the 1960s and 1970s about the need for privacy and data protection.[352] Concomitantly, it is claimed that the role played by technology – first and foremost in the form of mainframe computers – was essentially to exacerbate tensions in the populace caused by organisations' appetite for information.[353]

While these claims have surface plausibility, we should be wary of explanations that attempt to single out *one* fundamental cause for the controversies out of which data protection laws emerged. We should also keep in mind that in terms of cause and effect, the interaction between organisational phenomena and technological developments is two-way.[354] Thus, organisations' informational appetite not only stimulates but is whetted by technological developments.

---

350 This difficulty has been summed up in terms of the 'anonymisation' of transactions. By this is meant essentially the dissolution and merger of transactional contours, together with the resultant problems in identifying them. See J Benno, 'Transaktionens anonymisering och dess påverkan på rättsliga problemställningar', in R Punsvik (ed), *Elektronisk handel – rettslige aspekter* (Oslo: Tano Aschehoug, 1998), 50–75; J Benno, 'The 'anonymisation' of the transaction and its impact on legal problems', The IT Law Observatory Report 6/98, Swedish IT Commission, Stockholm, 1998.

351 See further Part III (espec Chapter 12).

352 See particularly J Rule, D McAdam, L Stearns & D Uglow, 'Preserving Individual Autonomy in an Information-Oriented Society', in LJ Hoffman (ed), *Computers and Privacy in the Next Decade* (New York: Academic Press, 1980), 65; AF Westin, 'Civil Liberties and Computerized Data Systems', in M Greenberger (ed), *Computers, Communications, and the Public Interest* (Baltimore/London: Johns Hopkins Press, 1971), 151, 156.

353 See, eg, Westin, *ibid*, 165; J Rule, D McAdam, L Stearns & D Uglow, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), 11–12.

354 For further discussion of this interaction, see section 6.2.2 below.

Further, the enormity of this appetite, which at times appears to border on the insatiable, is itself a result of a complex array of other, non-technological factors. At a very general level, it expresses the extreme importance of reflexivity and rationality in modern society.[355] More specifically, organisations' information appetite, along with their concomitant interest in developing and utilising IT, reflects a concern to improve their efficiency of performance. Other concerns have also been relevant, such as a desire on the part of government agencies to de-politicise a crisis by attributing its root cause to lack of necessary information.[356] Alternatively, an organisation's use of advanced IT can be aimed at giving an *impression* of efficiency, thus enhancing the organisation's status or attractiveness *vis-à-vis*, say, potential resource providers.[357] In this regard, it should not be forgotten that IT is more than just a set of tools; it has symbolic/totemic dimensions too (eg, as an icon of progress and modernity).[358] Concomitantly, emotional factors can play a role in modern organisations' enthusiasm to take on board new IT products. For instance, the growing sophistication of IT appeals to humans' innate fascination for the 'technically sweet' in the form of advanced, push-button gadgetry.

Nevertheless, the concern to improve performance efficiency has been primarily important in motivating organisations to intensify their utilisation of information and advanced forms of IT. In the private commercial sector, the main end of increased efficiency is typically economic gain. For public sector organisations, improved efficiency typically serves other goals as well. One such goal is the defence and extension of national sovereignty. Another goal – at least in liberal democratic States – is the enhancement of citizens' welfare. All three goals, along with measures to realise them, have often been inter-linked; the connections between capitalism, military activity and welfare politics are numerous and significant. Many of the conditions for the emergence of large information systems in the civil sector have been laid through the prior bureaucratisation of military processes, while the latter

---

355 On the importance of reflexivity, see espec A Giddens, *The Consequences of Modernity* (Cambridge: Polity Press, 1990), 36ff. By 'reflexivity' is meant a condition in which social practices are examined and altered in the light of new information about those practices. On the importance of rationality, see espec M Weber, *The Theory of Social and Economic Organization*, trans AM Henderson & T Parsons (New York: Free Press, 1964), 337 & 339. Rationality refers here to the subjection of human activities to administration and classification based on formalised, impersonal rules of procedure and an emphasis on optimising performance efficiency.

356 See, eg, KC Laudon, *Computers and Bureaucratic Reform. The Political Functions of Urban Information Systems* (New York: Wiley, 1974), espec 50 (identifying this sort of desire behind the proposal in the late 1960s to establish a National Data Centre in the USA).

357 See, eg, R Kling, 'Automated Welfare Client-Tracking and Service Integration: The Political Economy of Computing' (1978) 21 *Communications of the ACM*, 484–493 (documenting concrete instances of this factor motivating the computerisation strategies of public sector organisations in the USA).

358 S Beckman, 'A world-shaping technology', in M Karlsson & L Sturesson (eds), *The World's Largest Machine: Global Communications and the Human Condition* (Stockholm: Almqvist & Wiksell International, 1995), 260, 271.

have frequently been stimulated by, and generators of, capitalist economic enterprise.[359]

These connections notwithstanding, enhancement of citizens' welfare has been prominent in motivating and justifying expansion of *civil* sector agencies' gathering of data on citizens in liberal democratic States. Establishment of social welfare schemes has gone hand-in-hand with growth in the amount of citizen data collected by civil sector agencies. The more ambitious and/or discriminating these schemes have become, the greater has been the need for fine-grained assessments of citizens based on correspondingly detailed personal data. This need has usually been justified in terms of ensuring that the distribution of services and benefits is just; ie, ensuring that these goods flow only to citizens who need and/or legally qualify for them.[360]

In recent years, more entrepeneurial considerations have also played a role in motivating civil sector agencies' intensified processing of personal data. Under the sway of economic exigencies and the business-inspired ideals of 'New Public Management', many Western governments appear to be primarily concerned with cost-cutting. Their intensified utilisation of citizen data seems increasingly motivated by a fiscal imperative, a desire to reduce waste, fraud and abuse with respect to government services.[361] A good example of this fiscal imperative at work is the dramatic increase over the last 15 years or so in systematic computerised matching of personal data stored in different government agencies' registers. Analysis of this development in the USA and Australia shows these matching schemes as aimed mainly at detecting instances in which persons have received excessive government benefits or failed to pay appropriate taxes.[362]

Underlying these economic concerns is an awareness that much of contemporary economic activity is based on the production and exchange of information. Concomitantly, information is increasingly being regarded as a valuable resource in itself. There exists a rapidly growing market in information services, a market in which information as such, and particularly personal data, can be bought and sold for significant financial sums.[363]

---

359 See generally C Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Polity Press, 1990), chapt 3 and references cited therein.

360 See further the observations by Rule *et al*, *infra* n 353.

361 See generally D Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994), 88ff and references cited therein.

362 See, eg, RA Clarke, 'Dataveillance by Governments: The Technique of Computer Matching' (1994) 7 *Information Technology & People*, no 2, 46, 49ff.

363 See, eg, E Novek, N Sinha & O Gandy, 'The value of your name' (1990) 12 *Media, Culture and Society*, 525–543 (analysing the burgeoning trade in customer lists as commodities in their own right).

6.2.2 DEVELOPMENTS IN MASS SURVEILLANCE AND CONTROL

In the context of the discourse out of which data protection laws have sprung, the developments canvassed above would scarcely have aroused concern but for two inter-related factors. The first is that these developments have contributed to a marked increase in the ability of organisations to monitor systematically the activities of those with whom they deal. In other words, the developments have augmented the *surveillance* capabilities of organisations. The second factor is that with this increase has come an enhancement of organisations' *control* capabilities – ie, their ability to exert influence over those who are the subjects of surveillance. In practice, the two types of capability are intimately linked: surveillance is usually carried out for control purposes, and has a controlling effect.

The scope of surveillance and social control in contemporary society is at an unprecedented high. Indeed, this is one of the key defining features of modernity.[364] It is the reverse side to the extreme reflexivity and rationality identified in section 6.2.1.

Three major factors have contributed to the development of systems of mass surveillance. The first is the growth in social scale.[365] The second is the increasing symbiosis of the various surveillance systems run by different organisations.[366] A third factor is the growth of fine-grained concern by organisations for the affairs of their clients.[367] This concern is not always foisted by organisations on an unwitting public; rather, it is very often engendered by popular pressure to see justice done in various ways.[368]

Factors of more ideological character are relevant too. For example, the rise in the 1980s of 'New Right' ideology contributed to the growth of organisational surveillance in many Western countries. The emphasis of such ideology on buttressing the power of the State to fight criminality and protect national security on the one hand, and to stimulate commercial enterprise on the other, opened up for extensive monitoring of both the political and consumerist behaviour of citizens.[369] More generally, sight should not be lost of the pivotal role played by military factors

---

364 See further, eg, Lyon, *supra* n 361, 3, 4; Giddens, *supra* n 355, 57–58; Rule *et al*, *supra* n 352, 68. Surveillance and control levels, though, have not increased uniformly across the board. While there has been growth of systems of *mass* surveillance and control (ie, systems by which organisations monitor and influence the behaviour of large numbers of people – both as individuals and as collective entities), this has occurred against the background of relative declining intensity, at least in numerous Western countries, of the levels of surveillance and control exercised by many *small-scale* groups, particularly families and neighbourhoods. See further J Rule, *Private Lives and Public Surveillance* (New York: Schocken Books, 1974), 342; N Christie, *Hvor tett et samfunn?* (Oslo: Universitetsforlaget, 1982, 2nd rev ed).

365 J Rule, *Private Lives and Public Surveillance* (New York: Schocken Books, 1974), 301.

366 *Ibid*, 308ff.

367 *Ibid*, 321.

368 Rule *et al*, *supra* n 353, 43, 134.

369 Lyon, *supra* n 361, 54–55.

in establishing the foundations for contemporary systems of mass surveillance and control.[370]

Finally, there are technological factors. These deserve closer analysis here, not least because their exact role in relation to surveillance and control is frequently at issue in data protection discourse.

It is sometimes claimed that technologies are neutral. While this can be true in the abstract, technologies are never introduced into, or used in, a social vacuum. In practice, the context in which technologies are used tends to undermine any *a priori* neutrality they might enjoy. Moreover, technologies often have an inherent logic or bias of their own which strongly influences (though does not necessarily determine) the way in which they are used. New technologies can also roll back various constraints that have prevented occurrence of a particular kind of activity. Thus, they help to shift the parameters of social interaction, creating new opportunities of activity, and magnifying existing opportunities. In doing so, they can also create conflicts as well as accentuate old ones.

These remarks should be borne in mind when considering the impact of technological factors on developments in mass surveillance and control. For these developments are in large part facilitated by new forms of technology. At the same time as the latter create new avenues for human interaction and self-realisation, they often provide new opportunities for registering and disclosing data about ourselves. We see this, for example, with the increasing amounts of data registered in connection with activity on the Internet.[371]

To some extent, the developments in mass surveillance and control are also *driven* by new forms of technology. This is particularly the case in respect of technologies (eg, remote sensing satellites, automated dialling machines) with an inherent bias towards enhancing surveillance and/or rolling back privacy.[372]

Nevertheless, other technological developments can bolster personal privacy and autonomy. There is a range of technological mechanisms – often termed 'privacy-enhancing technologies' or 'PETs' – for directly reducing or eliminating the collection and further processing of personal data.[373] More subtly, telecommunications technology in many of its various applications (teleshopping, telebanking etc) frees persons from having to make face-to-face contact with service providers, thereby also freeing them from a situation by which transactional behaviour is traditionally monitored and moulded. In the domestic sphere, privacy

---

370 See further Dandeker, *supra* n 359, espec chapt 3.

371 As documented in, eg, Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, <http://www.ftc.gov/reports/privacy3/ priv-23a.pdf>, 23ff.

372 For an overview of such technologies, see Froomkin, *supra* n 334, 1468–1501.

373 See generally H Burkert, 'Privacy-Enhancing Technologies: Typology, Critique, Vision', in PE Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT Press, 1997), 125–142. For an overview of PETs in relation to electronic payment transactions, see AM Froomkin, 'Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases' (1996) 15 *U of Pittsburgh J of Law and Commerce*, 395, Part III.

and autonomy have been enhanced to an unprecedented extent by a wide range of appliances and tools, including automobiles, telephones, television sets, washing machines, bathrooms and air conditioning. It is even claimed that privacy today 'is as much a result of modern technology as technology is a threat to the private lives of citizens'.[374]

Thus, if we consider technologies as an undifferentiated mass (ie, as technology rather than as various technologies), we see they have a certain double-sidedness in relation to privacy. Technology both enhances and detracts from privacy. It gives with the one hand and takes with the other. This has been termed a 'paradox of privacy'.[375] It should rather be termed a paradox of technology. This paradox occurs not just in relation to technology as an undifferentiated mass; also numerous individual technologies both enhance and detract from privacy. Telephones are an obvious case in point: they free us from face-to-face contact at the same time as they provide another point of contact through which our privacy can be disturbed. A similar double-sidedness occurs with the impact of technology on personal and organisational *empowerment*. Technologies frequently have the potential to empower persons and organisations at the same time as they have the potential to disempower them. Video cameras are one such technology.

Nevertheless, the degree to which each type of potential is realised tends to follow existing power structures. Concomitantly, new forms of IT tend to be employed in ways that primarily serve the interests of dominant organisational elites.[376] Hence, a great deal of caution should be exercised before embracing claims that new forms of IT are likely to bring about the demise of totalitarianism or hierarchies generally. Certainly, new computer networks will increase the difficulties experienced by totalitarian regimes – indeed, any regimes – in controlling data flow, yet this does not mean such regimes are thereby bound to fall. Furthermore, the networks open up new avenues for surveillance which can render illusory much of the freedom and privacy of using them.

While a great deal of data protection discourse has been preoccupied with *technological* threats to privacy and related values, it nevertheless appears to be infused by growing awareness of the double-sided character of technology as described above. Clear evidence of this awareness is found in the recent burgeoning

---

374 K Raes, 'The Privacy of Technology and the Technology of Privacy: The Rise of Privatism and the Deprivation of Public Culture', in A Sajó & FB Petrik (eds), *High-Technology and Law: A Critical Approach* (Budapest: Institute of Political and Legal Sciences, Hungarian Academy of Sciences, 1989), 78.

375 Rodotà, *supra* n 19, 263.

376 See espec the work carried out at the University of California's Irvine School of research and instruction in information systems. An overview of this work is given in KL Kraemer & JL King, 'Social Analysis of Information Systems: The Irvine School, 1970–1994' (1994) 3 *Informatization and the Public Sector*, 163–182. See also WBHJ van de Donk, ITM Snellen & PW Tops (eds), *Orwell in Athens: A Perspective on Informatization and Democracy* (Amsterdam: IOS Press, 1995).

of proposals to apply IT in the service of enhanced privacy and data protection.[377] At the same time, little evidence exists to indicate that the architects of data protection laws share a deep-seated hostility to computers and other forms of IT. Certainly, they share a suspicion of the potential dangers of such technology. They additionally share a desire to ensure that technological developments are subjected to assessment and, to some extent, regulated. Moreover, many early data protection laws have singled out *computerised* data processing as their sole object of control.[378] Yet data protection laws are far from neo-Luddite in aim or inspiration.[379]

What are the key features of modern systems of mass surveillance and control which have aroused concern in data protection discourse? One feature is their growing pervasiveness. This growth has mainly occurred along two axes. First, there has been an expansion across national boundaries. This is evidenced, for instance, in the development of increasingly sophisticated transnational systems for policing, including the establishment of computerised information systems that are run and accessible by police agencies in multiple countries.[380] Secondly, while systems of mass surveillance and control have traditionally been linked primarily to State institutions, such systems are spreading into the private sector. Commercial transactions and consumption patterns in the latter sector are increasingly subject to systematic monitoring for a variety of purposes – credit assessment, marketing, product evaluation, criminal investigation, enforcement of intellectual property rights, etc – which tend ultimately to serve, directly or indirectly, the ends of social control.[381] Part and parcel of this development is the relatively recent emergence of large numbers of private organisations (eg, credit reporting agencies, marketing firms) for which such monitoring is the sole or primary activity. Further, many surveillance and control functions that have traditionally been the preserve of public

---

377 See, eg, Information and Privacy Commissioner of Ontario & Registratiekamer of the Netherlands, *Privacy-Enhancing Technologies: The Path to Anonymity*, August 1995, <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm> (vol 1); <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anoni-v2.pdf> (vol 2)); E Boe, 'Pseudo-Identities in Health Registers? Information Technology as a Vehicle for Privacy Protection' (1994) 2 *The Int Privacy Bulletin*, no 3, 8–13; *Pseudonyme helseregistre*, NOU 1993:22. See also the literature cited *infra* n 1235.

378 See further Chapter 2 (section 2.4.2).

379 See also Simitis, *supra* n 336, 115–116.

380 The Schengen Information System (SIS) is a pertinent example. For a useful description of the system, see M Baldwin-Edwards & B Hebenton, 'Will SIS be Europe's Big Brother?', in M Andersen & M den Boer (eds), *Policing Across National Boundaries* (London/New York: Pinter Publishers, 1994), 137–157.

381 See generally Lyon, *supra* n 361, chapt 8; OH Gandy Jr, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993), chapt 3. With respect to the control potential of electronic systems for enforcement of intellectual property rights, see, eg, JE Cohen, 'A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace' (1996) 28 *Connecticut L Rev*, 981–1039; Bygrave & Koelman, *supra* n 316; G Greenleaf, ''IP, Phone Home': The Uneasy Relationship between Copyright and Privacy, illustrated in the Laws of Hong Kong and Australia' (2002) 32 *Hong Kong LJ* (forthcoming).

sector regulatory agencies, such as the police, are devolving gradually to private organisations.[382]

Another key feature of concern has to do with surveillance techniques: these are now automated, de-personalised, capital-intensive operations to a far greater extent than in the past. As a result, physical proximity between the human watchers and the watched is decreasing. Today's techniques are often less physically obtrusive than their earlier counterparts, and more capable of transcending light conditions, physical barriers and limitations of time and space. Concomitantly, they allow for the gathering of information that previously could only have been collated by resorting to traditional coercive methods of intrusion. They are aimed increasingly at forestalling undesired action rather than simply tracking down such action once it has been carried out. Thus, instead of just targeting specific individuals, they tend also to place large numbers of persons under suspicion.[383] An obvious case in point is the growing use of advanced optical, audio and sensory surveillance tools (eg, video cameras, microphones, infra-red sensors) as a substitute for, or supplement to, the use of security personnel. Another case in point is the evermore extensive practice of automated profiling for a variety of control purposes.[384]

Automated profiling is just one instance of a range of increasingly used and increasingly refined techniques for monitoring and/or anticipating human behaviour through analysis of data in computerised record systems. The growing importance of such techniques for surveillance and control is a reflection of the fact that computer systems increasingly mediate, facilitate and register human activities. This fact reflects in turn the growing ubiquity, miniaturisation and inter-connectivity of computer systems. The important point, though, is that our transactions leave behind them an ever-richer variety of electronic trails. These trails attach not just to extraordinary transactions but to *routine* patterns of life. Systems for electronic funds transfer, related systems for electronic ordering and purchase of goods, systems for electronic logging and control of access to buildings, roads, etc – all of these generate data on our everyday activities.[385]

Common for all of these systems is their automatic generation and registration of enormous masses of transactional data that can be linked to large numbers of persons, as individuals and/or as groups. These data supplement the often already

---

382 Note, eg, the recent trend in some countries to place private financial institutions under a legal duty to report to the police suspected attempts at 'white-washing' illegally generated monies. For a brief description of this trend in Norway, see JP Berg, 'Finansinstitusjonenes rapporteringsplikt til ØKOKRIM ved mistanke om hvitvasking av penger – et gjennombrudd for 'informant'-samfunnet?' (1996) 23 *Kritisk Juss*, 147–163.

383 For more detailed analysis of these developments in surveillance techniques, see, eg, GT Marx, *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988), chapt 10; Lyon, *supra* n 361, chapt 3.

384 See further Chapter 17 (section 17.2).

385 See generally I Mestad, *Elektroniske spor. Nye perspektiver på personvern*, CompLex 3/86 (Oslo: Universitetsforlaget, 1986), chapt 2; Bing, *supra* n 19, 252ff.

extensive amounts of information we are specifically asked to provide organisations in return for various services, or which organisations otherwise gather on us independently of transactions with them. These transactional data are commonly registered, or capable of being registered, without the data subjects' knowledge. Concomitantly, in the absence of data protection laws, data subjects tend to have little if any control over what is registered once they have come in contact with the system in question. While such transactional data are usually of trivial significance on their own, they can reveal much about the behaviour and personalities of the respective data subjects when linked with other data.

Although the above features of modern systems for mass surveillance and control have figured prominently in data protection discourse, they are not always directly or adequately addressed in data protection *laws*. Certainly, some aspects of these features are reflected in the legislation. For instance, the increasing involvement of the private sector in mass surveillance and control explains the tendency for data protection laws to regulate both public and private sectors. Further, the privacy-invasive potential of apparently trivial transactional data is reflected in the fact that most data protection laws do not require (at least *prima facie*) personal data to have a predefined level of sensitivity in order to qualify for legal protection. Nevertheless, other aspects of modern surveillance and control systems, such as their increasingly transnational character, are only now in the process of being addressed by data protection laws – and not always adequately.[386] Still other aspects have yet to receive prominent attention in data protection discourse generally. One such aspect is the growth in numbers of individual persons (as opposed to organisations) who possess, in their *private* capacity, the technological means to process (in particular, disseminate) massive amounts of personal data with increasing ease and decreasing expense. This problem is especially actualised in the context of the Internet.

6.2.3 PROBLEMS WITH QUALITY OF DATA/INFORMATION

Another major catalyst for the emergence and continued existence of data protection laws is an accumulating body of evidence indicating that the quality of data/information utilised by numerous organisations is deficient; ie, that the data/information are insufficiently precise, correct, complete and/or relevant in relation to the purposes for which they are processed. The exact scale of the problem, though, is difficult to gauge as detailed empirical studies of data/information quality are lacking for many organisational sectors. Nevertheless, some such studies have generated alarming results.[387]

---

386 See further the assessment of regulation of profiling practices in Chapters 18–19.

387 For an extensive set of examples, with particular focus on the USA and Norway, see Bygrave, *supra* n 73, 13ff.

A multitude of factors affect the quality of data/information. Some of these factors are basically technological in character (eg, faults with hardware and software); some are essentially organisational (eg, the extent to which information is actually used by the persons or organisations engaged in its processing); while others are primarily legal (eg, the availability and utilisation of access rights). Still others pertain primarily to human cognition. For present purposes, to canvass all of these factors in detail is unnecessary.[388] For the purposes of the discussion in Part IV, however, it is pertinent to stress that the set of factors relating to human cognition play a relatively large role in determining data/information quality.[389] In other words, poor data/information quality is often a reflection of poor thinking. Exacerbating this tendency has been a paucity of systematic academic and managerial attention to data/information quality.[390]

A clear illustration of poor thinking (or what can also be termed poor 'cognitive quality') leading to misapplication of data is the outcome of a matching program initiated by a Swedish municipality, Kungsbacka, in the early 1980s. The aim of the program was to identify persons in illegal receipt of housing aid, and involved the matching of income data held in various data registers. The matching resulted in a large number of spurious 'hits', primarily because account was not taken of the fact that the matched data registers operated with different concepts of 'income'.[391] The results of this matching program illustrate the obvious but important point that many terms used to categorise data can have different underlying referents – a point that those responsible for the Swedish matching program failed to appreciate.

Problems with poor data/information quality have occurred despite the existence, in many cases, of legal rules aimed at minimising them. A great deal of these rules are found in data protection laws.[392] We are thereby tempted to put a question-mark against the efficacy of such laws in ensuring adequate data/information quality. Are the relevant rules in these laws sufficiently clear as to what is required of data controllers in terms of quality assurance? Are the rules sufficiently stringent? Or do many organisations that are supposed to comply with the rules fail to do so for reasons of ignorance, apathy, indifference and/or an attitude that compliance is too burdensome?[393]

---

388 For more detailed analyses of these factors, see, eg, Bygrave, *supra* n 73, RW Bailey, *Human Error in Computer Systems* (Englewood Cliffs, New Jersey: Prentice-Hall, 1983); & FB Cohen, *Protection and Security on the Information Superhighway* (New York: John Wiley & Sons, 1995), 33–56.

389 See further Bygrave, *supra* n 73, and references cited therein.

390 *Ibid*.

391 See further B Nyberg, *Samkörning av personregister*, IRI-rapport 1984:2 (Stockholm: Institutet för Rättsinformatikk, 1984), 16–21; Bing, *supra* n 19, 251–252; & J Freese, *Den maktfullkomliga oförmågan* (Stockholm: Wahlström & Widstrand, 1987), 94–96.

392 See further Chapter 3 (espec section 3.5) and Chapter 18 (espec section 18.4.4).

393 Aspects of these questions are taken up in Part IV where they have considerable bearing for determining the ability of data protection laws to minimise the potentially detrimental impact of profiling practices on data subjects.

6.3 Fears

6.3.1 FEARS OVER THREATS TO PRIVACY AND TO RELATED VALUES

While the developments outlined in section 6.2 have each contributed in varying degrees to the emergence and/or continued existence of data protection laws, they are not sufficient causes of such legislation. What has helped transform them into issues of legislative concern is a congeries of public fears about some of these developments' potential and actual effects. One set of fears relates to increasing transparency, disorientation and disempowerment of data subjects *vis-à-vis* data controllers. Another set of fears concerns loss of control over technology. A third set pertains to dehumanisation of societal processes.

Anxiety over increasing transparency, disorientation and disempowerment of data subjects revolves mainly around the effects of two developments: (i) growth in the amount of data gathered and shared by organisations; (ii) diminishing participation by data subjects in decision-making processes affecting them. On the one hand, these developments involve increases in the knowledge organisations have about the individuals, groups and other organisations with whom they deal. With a rational basis in Francis Bacon's adage 'knowledge is power', many people fear that this knowledge increase will make it easier for organisations to influence data subjects' behaviour in ways that unfairly undermine their autonomy and integrity. At the same time, they fear the possibility that the data disseminated within and between organisations are invalid, misconstrued or misapplied in some way, thereby leaving the data subject(s) vulnerable to unwarranted interference. On the other hand, the above developments involve increases in the complexity of cross-organisational data flows and in the blurring of organisational lines. Accordingly, it is feared that these developments will tend to make it more difficult for data subjects to trace the flow of data on themselves thus threatening their control over what happens with their various virtual personas. It is likewise feared that persons' ability to identify who or what is responsible for each of the myriad transactions involving their data, plus the full parameters of these transactions, will tend to be reduced.

The sum of these fears is a general anxiety that the above developments, if unchecked, will result in an unprecedented aggregation of power in large organisations, thereby threatening the bases for democratic, pluralistic society. This anxiety is well-expressed in the report of the Australian Law Reform Commission (ALRC) recommending enactment of data protection legislation:

> 'If privacy protection were not strengthened, it would be difficult for Australian society to maintain its traditions of individual liberty and democratic institutions in the face of technological change, which has given to public and private

> authorities the power to do what a combination of physical and socio-legal restraints have traditionally denied to them.'[394]

Similarly, in a famous decision of 1983 (which contributed to the subsequent strengthening of German data protection legislation),[395] the German Federal Constitutional Court (*Bundesverfassungsgericht*) observed that modern forms of data processing threaten the free development of personality by making it increasingly difficult for citizens to determine who knows what about them. The Court went on to note that this difficulty can have a chilling effect on citizen's social engagement, thereby impairing pluralism and democracy.[396]

The second set of fears revolves mainly about the spiralling complexity of IT, information flows and organisational patterns. People fear that the environment resulting from this complexity will elude full human comprehension. They warn of a future in which humans will increasingly come under the sway of runaway technology that cannot be effectively steered.[397]

The third set of fears revolves mainly around the encroachment of automated/machine processes on human interaction. These fears envision the gradual development of an instrumental, mechanistic conception of humans. Concomitantly, they portend a future in which human relations are subjugated by an unfeeling, purely instrumental rationality, of which computer technology is one manifestation. In such a society, it is claimed, human spirit will give way to moral indifference and fatalism.[398]

Of the three sets of fears described above, the first-mentioned has predominated in data protection discourse and played the greatest role in kick-starting enactment of data protection legislation. To some extent, though, all three sets of fears overlap with each other. Moreover, many of the themes of the second and third-mentioned sets are reflected in the debate over use of PINs and the automatisation of decision-making processes.

The above fears have been nourished by certain concrete experiences. Of especial importance in this respect have been the traumas of fascist oppression prior

---

394 ALRC, *supra* n 158, vol 1, 17.

395 See further section 6.4.1.

396 65 BVerfGE, 1, 43.

397 See, eg, MD Kirby, 'Information Security – OECD Initiatives' (1992) 3 *J of Law and Information Science*, no 1, 25, 26, 29–30; also published in (1992) 8 *CLSR*, 102, 103–104.

398 This set of fears, together with the second-mentioned set, are best expressed in the works of Jacques Ellul and Joseph Weizenbaum though neither of these works has figured prominently in the discourse dealing specifically with data protection. See espec J Ellul, *The Technological Society*, trans J Wilkinson (New York: Vintage, 1964) – originally published as *La technique ou l'enjou du siècle* (Paris: Armand Colin, 1954); and J Weizenbaum, *Computer Power and Human Reason. From Judgment to Calculation* (San Francisco: WH Freeman & Company, 1976).

to and during World War Two.[399] Also important, especially in the USA, has been the Watergate scandal of the early 1970s.[400]

Particular concrete manifestations of information technology have nourished these fears as well. The mainframe computer in the form of the IBM 360 series played a significant role in this respect during the 1960s and 1970s. For the average person, what seemed especially threatening about the mainframes was a combination of their physical bulk, their placement outside the public domain and their concomitantly mysterious but (for those times) powerful data-processing potential.[401] In the course of the last 15 years, though, these threatening characteristics have lost much of their impact due to computers' increasing ubiquity, miniaturisation and user-friendliness. In terms of technology, what arguably tends to nourish public fears now is less any one image of a certain type of computer but a more variegated image of a web of interconnected technologies (video surveillance cameras, smart cards, vehicle tracking devices, etc) able to track people's myriad patterns of behaviour.

Not only have concrete experiences and manifestations of IT nourished the above fears, certain dystopian visions have played a significant role too. In data protection discourse, the most salient of these visions stems from George Orwell's novel, *Nineteen Eighty-Four*, published in 1949. Less salient, but of growing significance, is the vision of 'panopticism' expounded initially by Michel Foucault on the basis of Jeremy Bentham's famous prison plan of 1791.[402] Both works, particularly that of Foucault, highlight the way in which social control can rest upon an informational imbalance between the observers and the observed: the latter are rendered potentially transparent *vis-à-vis* the former, but not *vice-versa*. While the extent to which these control dynamics actually permeate contemporary societies is debatable,[403] the vision of panopticism alerts us to the intimate connection between surveillance and control, and to the subtelty with which the latter mechanisms can work. From a data protection perspective, the linking of control to informational

---

399 See, eg, K S Selmer, 'Elektronisk databehandling og rettssamfunnet', in *Forhandlingene ved Det 30. nordiske juristmøtet, Oslo 15.–17. august 1984* (Oslo: Det norske styret for De nordiske juristmøter, 1984), Part II, 41, 44.

400 See, eg, Bennett, *supra* n 5, 72.

401 As Alan Westin allegedly commented in 1972, 'you do not find computers on streetcorners or in free nature, but in big, powerful organizations': cited in Bing, *supra* n 19, 247.

402 See M Foucault, *Discipline and Punish: The Birth of the Prison*, trans A Sheridan (Harmondsworth: Penguin, 1977), 195–228. Bentham's plan was for the building of a prison he termed the Panopticon. The prison would allow for the constant surveillance of prisoners from a central watch tower but prevent (through special lighting devices) prisoners from identifying when and by whom they were watched.

403 For a sensitive discussion of the sociological utility of the notion of panopticism, see Lyon, *supra* n 361, 71ff, 166ff & 202ff. There can also be little doubt that aspects of *Nineteen Eighty-Four* – most notably, its focus on *State* power and on *blatantly* violent control measures – diminish its relevance for discourse on contemporary surveillance and control in relation to the majority of citizens in Western, liberal democracies. The more subtle, pleasurable and insidious forms of control depicted in Aldous Huxley's *Brave New World* (1932) better describe what these citizens are likely to experience.

imbalance between observers and the observed is particularly important. Also important is how panopticism helps to show that the mere registration of personal data – quite apart from the actual use of the data in decisions affecting the data subject(s) – has disciplinary potential. Accordingly, the notion of panopticism figures increasingly in data protection discourse. Numerous scholars are taking up Foucault's analysis and adapting it to take account specifically of modern applications of information technology.[404] Nevertheless, the notion of panopticism seems still not to be as prominent in the general public consciousness as *Nineteen Eighty-Four*. The latter has undoubtedly played a more significant role in igniting debate in Western societies on the need for greater privacy and data protection to counter the growing pervasiveness of systems of mass surveillance.

Some of the fears described above – particularly the first set – are reflected in recent surveys of public attitudes to privacy and data protection issues. Although such surveys can suffer from methodological weaknesses,[405] they do provide evidence of high levels of public concern for privacy and data protection,[406] at least in the abstract.[407] The surveys also provide evidence of a growing feeling amongst people that they are losing their privacy and/or ability to control how data on

404 See, eg, K Robins & F Webster, 'Cybernetic capitalism: Information, technology, everyday life', in V Mosco & J Wasko (eds), *The Political Economy of Information* (Madison: University of Wisconsin Press, 1988), 44–75; Gandy, *supra* n 381; Marx, *supra* n 383, 220ff; Poster, *supra* n 348, 91ff. Surprisingly, Foucault makes no mention of modern computer technology in his discussion of panopticism.

405 See further WH Dutton & RG Meadow, 'A tolerance for surveillance: American public opinion concerning privacy and civil liberties', in KB Levitan (ed), *Government Infostructures* (New York: Greenwood Press, 1987), 147, 167.

406 For Australia, see Federal Privacy Commissioner, *Community Attitudes to Privacy*, Information Paper 3 (Canberra: AGPS, 1995), 7; Federal Privacy Commissioner, *Privacy and the Community, July 2001*, <http://www.privacy.gov.au/publications/rcommunity.html>. For Canada, see Louis Harris & Associates (in association with AF Westin), *Equifax Canada Report on Consumers and Privacy in the Information Age* (Ville d'Anjou: Equifax Canada, 1995), 4; see also Fédération nationale des associations de consommateurs du Québec (FNACQ) & Public Interest Advocacy Centre (PIAC), *Surveying Boundaries: Canadians and Their Personal Information* (FNACQ/PIAC, 1995), 1, 54–55. For Denmark, see, ia, Instituttet for Fremtidsforskning, *Danskernes holdninger til informationsteknologi* (Copenhagen: Post Danmark, 1996), 50 & 96. For Norway, see E Gulløy, *Undersøkelse om personvern: Holdninger og erfaringer 1997*, Notat 97/46 (Oslo: Statistisk sentralbyrå, 1997), 17 & 29. For the UK, see Data Protection Registrar, *Tenth Report of the Data Protection Registrar, June 1994* (London: HMSO, 1994), 79. For the USA, see, eg, Louis Harris & Associates (in association with AF Westin): *Harris-Equifax Mid-Decade Consumer Privacy Survey 1995* (Atlanta: Equifax, 1995), 7.

407 The surveys show that privacy and data protection appear, by and large, to be second-order concerns of the public. Moreover, they show that people tend not to forego receiving some sort of service (eg, credit, insurance) in order to protect their privacy. See, eg, JE Katz & AR Tassone, 'Public Opinion Trends: Privacy and Information Technology' (1990) 54 *Public Opinion Quarterly*, 124, 127, 137–138; Gulløy, *supra* n 406, 17, 20–21, 30, 41–42; Data Protection Registrar, *supra* n 406, 79; Instituttet for Fremtidsforskning, *supra* n 406, 13, 55–60.

themselves are being used.[408] Accompanying this feeling are low levels of public trust that organisations will not misuse personal information.[409]

These levels of distrust, along with the fears they manifest, are arguably part of a more general trend in contemporary society whereby human interaction and self-perception are increasingly pervaded by consciousness of risk.[410] We are experiencing a gradual loss of 'cognitive sovereignty' over the parameters and consequences of our actions.[411] We feel less able to divine what is dangerous and what is safe for ourselves. At the same time, our apprehension of danger is focused increasingly on what we *do not* see, what we *do not* feel, what we *do not* know – 'Not-Yet-Events'.[412]

While sociological discourse on risk society often focuses on threats to the natural environment brought on by industrial processes, the growing pervasiveness of systems of mass surveillance and control, and associated developments in utilisation of personal data, undoubtedly help to constitute the above features of risk consciousnessness. We are faced with information systems of growing complexity and diminishing transparency; data on ourselves – both as individuals and as members of various collective entities – are being handled by many persons and organisations of which we know little or nothing. Exacerbating the anxiety brought on by this loss of cognitive sovereignty are the dystopian visions of Orwell, Foucault and others.

The expansion of risk consciousness makes it apposite to view data protection laws as concerned with shoring up public trust in the way organisations process personal data.[413] This concern manifests itself partly in the basic principles of data protection laws, particularly those principles, such as purpose specification, which are directly aimed at promoting foreseeability in data-processing outcomes and thereby reducing deficits in data subjects' cognitive sovereignty.[414] However, the

---

408 See, eg, Privacy Commissioner, *supra* n 406, 7 & 10; Louis Harris & Associates (Canada), *supra* n 406, 6 & 23; Katz & Tassone, *supra* n 407, 128–129, 138; Louis Harris & Associates, *supra* n 406, 24 & 37.

409 See, eg, I Székely, 'New Rights and Old Concerns: Information Privacy in Public Opinion and in the Press in Hungary' (1994) 3 *Informatization and the Public Sector*, 99, 102–103; Louis Harris & Associates, *supra* n 406, 40; Gandy, *supra* n 381, 140–141. Cf Instituttet for fremtidsforskning, *supra* n 406, 54 & 80 (indicating relatively high levels of trust on the part of Danes).

410 See espec U Beck, *Risikogesellschaft. Auf den Weg in eine andere Moderne* (Frankfurt am Main: Suhrkamp, 1986) – published in English as *Risk Society: Towards a New Modernity* (London: Sage, 1992); N Luhmann, *Soziologie des Risikos* (Berlin/New York: Walter de Gruyter, 1991) – published in English as *Risk: A Sociological Theory* (Berlin/New York: Walter de Gruyter, 1993). By 'risk' is meant the possibility of human action triggering events with detrimental consequences for society.

411 Beck, *ibid*, 53.

412 *Ibid*, 33.

413 See further Chapter 7 (section 7.3). This dimension of data protection laws is emphasised particularly in the work of Herbert Burkert: see espec 'Systemvertrauen: Ein Versuch über einige Zusammenhänge zwischen Karte und Datenschutz' (1991) *á la Card Euro-Journal*, no 1, 52–66.

414 See further Chapters 7 (section 7.2.5) and 18 (section 18.4.2).

effort at generating trust in information systems is manifest not just in the contents of data protection laws but in their very *legality*. As Burkert points out, data protection laws attempt to generate trust in information systems largely by utilising public trust in the efficacy of legal norms.[415]

At the same time, the way in which data protection laws – particularly the first pieces of such legislation – have been drafted shows traces of a deficit in cognitive sovereignty on the part of legislators and other policy makers.[416] The prominence in these laws of procedural controls and relatively diffuse, open-ended rules, together with the creation of data protection authorities, are partly symptomatic of legislative uncertainty about the appropriate regulatory response to the fears outlined above.[417] Somewhat paradoxically, though, certain of these features – namely, the use of relatively diffuse, open-ended rules – are likely to have a debilitating effect on the generation of legal certainty and thereby the generation of public trust.

Despite heightened risk consciousness and large numbers of people expressing concern for privacy and data protection, actual examples of large-scale, popular movements with such concern figuring prominently on their agenda are few.[418] The dry remark of a former member of the US Congress seems appropriate: 'privacy is an issue in which public concern is a mile wide and an inch deep'.[419] Concomitantly, the process leading to enactment of data protection laws has been steered in most cases only indirectly by pressure from the general public. Of greater influence have been the prescriptions of a relatively small, transnational network of concerned experts.[420]

6.3.2 ECONOMIC FEARS

The three sets of fears set out previously in this section are not the only fears that have acted as catalysts for the emergence of data protection laws. A fourth set of fears, touched upon in Part I, has had an impact too. Unlike the other three sets of fears, this fourth set is primarily economic in character and shared mainly by governments and business organisations. Moreover, it does not help to explain the *initial* emergence of data protection laws but the adoption of data protection instruments after the first wave of laws were in place.

---

415 Burkert, *supra* n 413.

416 See also Burkert, *supra* n 326; S Simitis, 'New Trends in National and International Data Protection Law', in J Dumortier (ed), *Recent Developments in Data Privacy Law* (Leuven: Leuven University Press, 1992), 17.

417 They are 'partly' symptomatic because, in some cases, these features of data protection laws are arguably also the result of a desire not to fundamentally upset organisations' existing data-processing practices: see further Chapter 7 (section 7.3).

418 See generally Bennett, *supra* n 5, 146 & 243

419 Glenn English, quoted in Dutton & Meadow, *supra* n 405, 148.

420 See Bennett, *supra* n 5, 127ff.

One aspect of this set of fears revolves around the desire by governments and business groups to stimulate consumer interest in participating in various electronic transactions, particularly those of a commercial nature. It is feared that without data protection legislation in place, there will not be sufficient consumer confidence to engage in these transactions.[421] This fear has mainly manifested itself in the last few years, when full-scale electronic commerce has become technically feasible and economically desirable.

Another aspect revolves about the fact that many data protection laws allow for restrictions to be put on the flow of personal data to countries without sufficient levels of data protection.[422] It is feared that by hindering transnational data flows, the laws could disrupt commercial and/or governmental processes. This possibility has helped prompt national governments to enact data protection laws that are recognised as adequate by countries already in the possession of such laws. The clearest example of this process at work is the passage of the UK *Data Protection Act* of 1984: the desire by the UK government to avoid restrictions on the flow of data into the country was decisive in its decision to enact the legislation.[423] However, fear of disrupted data flows has probably had the greatest impact in stimulating adoption of international data protection instruments, especially the OECD Guidelines and EC Directive. Justice Michael Kirby, Chairman of the expert group responsible for drafting the OECD Guidelines, writes:

> 'It was the fear that local regulation, ostensibly for privacy protection, would, in truth, be enacted for purposes of economic protectionism, that led to the initiative of the OECD to establish the expert group which developed its Privacy Guidelines. The spectre was presented that the economically beneficial flow of data across national boundaries might be impeded unnecessarily and regulated inefficiently producing a cacophony of laws which did little to advance human rights but much to interfere in the free flow of information and ideas.'[424]

Similarly, work on drafting the EC Directive was motivated to a large extent by fear that disharmony between the various data protection regimes of EC/EU Member

---

421 See, eg, Industry Canada & Justice Canada, Task Force on Electronic Commerce, *The Protection of Personal Information – Building Canada's Information Economy and Society* (Ottawa: Industry Canada/Justice Canada, 1998), 6; *Europe and the Global Information Society. Recommendations to the European Council* (Brussels, 26.5.1994 – the 'Bangemann Report'), 33.

422 See Chapter 4 (section 4.4).

423 See IJ Lloyd, 'The Data Protection Act – Little Brother Fights Back?' (1985) 48 *Modern L Rev*, 190, 190–191; Bennett, *supra* n 5, 141–143.

424 MD Kirby, 'Legal Aspects of Transborder Data Flows' (1991) 5 *Int Computer Law Adviser*, no 5, 4, 5–6.

States would hinder realisation of the internal market.[425] However, the possibility – alluded to by Kirby – of national data protection laws being passed for the purposes of economic protectionism seems to have been absent from the concerns of the EC organs when they set about drafting the Directive.

Fears about economic protectionism were aired mainly in North American quarters during the late 1970s and early 1980s. They tended to result in allegations that an underlying motivation for the enactment of many of the national data protection laws in Europe was to protect the nascent, European data-processing industries from foreign (US) competition.[426] Such allegations reflected unease, especially on the part of US trade representatives, over the spate of European data protection laws that were enacted in the mid- to late 1970s. It was feared that these laws were introduced too quickly, without adequate discussion of their economic consequences, and would hinder the international expansion of the data-processing industry, which is dominated by American firms.[427] Criticism focused upon two features of these laws. The first was that the laws contain provisions restricting transborder flows of personal data in certain circumstances. The second feature, which essentially is an expansion of the first, was that some of these laws protect(ed) data on legal persons in addition to data on individuals, consequently widening the scope of the restriction on transborder data flows.

Very little solid evidence has been provided to back up the allegations of economic protectionism. Regarding the legislative history of the Norwegian *Personal Data Registers Act*, for instance, no mention is made in the Act's preparatory documents of the need to protect Norwegian industry from foreign competition.[428] As for the actual consequences of the Act's regulation of transborder data flows, empirical studies have not found evidence of this regulation being practised in a protectionist manner. The same applies with respect to regulation of transborder data flows pursuant to the first data protection laws of Germany, Austria, Sweden, France and the UK.[429]

---

425 See, eg, Commission Communication of 13.9.1990 on the protection of individuals in relation to the processing of personal data in the Community and information security (COM(90) 314 final), 4. See also recitals 3, 5 & 7 in the preamble to the EC Directive.

426 See, eg, KR Pinegar, 'Privacy Protection Acts: Privacy Protectionism or Economic Protectionism?' (1984) 12 *Int Business Lawyer*, 183–188; Office of the US Special Trade Representative, 'Trade Barriers to Telecommunications, Data and Information Services' (1981) 4 *TDR*, no 5, 53; GS Grossman, 'Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations' (1982) 4 *Northwestern J of Int Law and Business*, no 1, 1–36; RP McGuire, 'The Information Age: An Introduction to Transborder Data Flow' (1979–80) 20 *Jurimetrics J*, 1–7.

427 See generally DP Farnsworth, 'Data Privacy: an American's View of European Legislation' (1983) 6 *TDR*, no 5, 285–290.

428 See the discussion on regulating transborder data flows in Ot prp 2 (1977–78), 9–10, 96. See also H Seip, 'Unfair Competition in Computer Services?' (1981) 4 *TDR*, no 8, 33.

429 See Ellger, *supra* n 75, 428–430 (concluding on the basis of an in-depth examination of the data protection regimes of Austria, Sweden, Denmark, Norway, France, the Federal Republic of Germany and the UK that, at least up until 1990, no solid evidence exists that rules for restricting TBDF under

The final proof advanced in support of the protectionism theory is the fact that some of the European data protection laws expressly protect(ed) data on legal persons. It has been claimed that, because of this fact, these laws cannot have been passed simply in order to protect the right of privacy; hence, they have also been passed for the purpose of economic protectionism.[430] This argumentation rests upon two assumptions: (i) that the purpose of 'pure' data protection laws is only to safeguard privacy; and (ii) that privacy as a concept and legal right can only embrace natural/physical persons. As shown in Part III, both assumptions are highly questionable.

While the protectionism theory seems to lack validity in relation to national data protection laws passed in Europe in the 1970s and 1980s, it is perhaps less easily refuted with respect to the EC Directive. Much evidence exists to indicate that the EC Commission, together with the Council of Ministers, first took up the issue of data protection in the 1970s largely out of concern for fostering development of the internal market and European IT-industry.[431] Traces of such a concern appear also in the Commission Communication setting out the first proposal for the data protection Directive.[432] Yet to what extent this concern accurately reflects a desire for economic protectionism is unclear. Equally unclear is the extent to which final adoption of the Directive took place in order to fulfil such a desire. Nevertheless, it is scarcely to be overlooked that implementation of the Directive – particularly Arts 25 and 26 – might well have protectionist benefits for data controllers established within the EU.

(Cont.)

these regimes operated as 'non-tariff trade barriers'). Ellger points out also (*ibid*, 429 & 270) that only an extremely small percentage of cross-border transfers of personal data were stopped. The findings of an earlier, albeit narrower, study by Bing are in line with Ellger's findings: see J Bing, *Data Protection in Practice – International Service Bureaux and Transnational Data Flows*, CompLex 1/85 (Oslo: Universitetsforlaget, 1985). However, the rules in Denmark's *Private Registers Act* on transborder data flows were not concerned solely with protection of individual persons; they were also grounded upon a desire to build up a national computer industry, such that public or private enterprise in Denmark could continue to operate independent of events in other countries: see Blume, *Personregistering*, *supra* n 93, 129 and references cited therein. Nevertheless, the latter concern apparently did not reflect a desire for economic protectionism as such but a desire to ensure that enterprises in the country could continue functioning in the event of a foreign crisis.

430 Pinegar, *supra* n 426, 188; Grossman, *supra* n 426, 12, 20; McGuire, *supra* n 426, 4.

431 See generally WJ Kirsch, 'The Protection of Privacy and Transborder Flows of Personal Data: the Work of the Council of Europe, the Organization for Economic Co-operation and Development and the European Economic Community' (1982) *Legal Issues of European Integration*, no 2, 21, 34–37; H Geiger, 'Europäischer Informationsmarkt und Datenschutz' (1989) 5 *RDV*, 203–210; R Ellger, 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 1)' (1991) 7 *RDV*, 57, 59–61.

432 See COM(90) 314 final, 13.9.1990, 4.

6.4 Legal Factors

A range of legal factors have contributed to the emergence and continued existence of data protection laws. These factors can be divided into two main categories according to the kind of contribution they have made. First, there are factors (hereinafter termed 'positive legal factors') that have served as sources of inspiration for the development of data protection laws by positively providing the latter with a normative basis. Secondly, there are factors (hereinafter termed 'negative legal factors') that have contributed to the emergence of data protection laws by failing to tackle adequately the problems arising as a result of the developments outlined in sections 6.2 and 6.3.

6.4.1 POSITIVE LEGAL FACTORS

Legal sources of inspiration for the development and continued existence of data protection laws are spread over a variety of instruments: international treaties, national Constitutions, other national legislation and judicially created doctrines. Much of the formal normative basis for law on data protection is provided by catalogues of fundamental human rights as set out in certain multilateral instruments, notably the *Universal Declaration of Human Rights* (UDHR) of 1948, the *International Covenant on Civil and Political Rights* (ICCPR) of 1966,[433] and the main regional human rights instruments.[434] The normative significance of these catalogues is expressly recognised in some of the data protection laws themselves, with the CoE Convention and the EC Directive being two prime examples.[435]

A variety of provisions in the catalogues inspire the central principles of data protection laws. Examples here are provisions proclaiming rights to liberty, freedom of thought, freedom from discrimination and freedom from torture. However, provisions proclaiming a right to privacy or private life[436] constitute the most direct inspiration for the principles of data protection laws. The central significance of such provisions is manifested in the CoE Convention and EC Directive both of which single out the 'right to privacy' from other rights of data subjects as being especially

433 Adopted 16.12.1966; in force 23.3.1976.

434 These being the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR) of 1950, the *American Declaration of the Rights and Duties of Man* (ADRDM) of 1948, the *American Convention on Human Rights* (ACHR) of 1969 (in force 18.7.1978), and the *African Charter on Human and People's Rights* (ACHPR) of 1981 (in force 21.10.1986).

435 See Art 1 of the Convention and Art 1 and recital 10 of the Directive.

436 See Art 12 of the UDHR, Art 17 of the ICCPR, Art 8 of the ECHR, Art V of the ADRDM and Art 11 of the ACHR. Cf the ACHPR which omits express protection for privacy or private life. This omission is not repeated in all human rights catalogues generated outside the Western, liberal-democratic sphere. See, eg, the Cairo Declaration on Human Rights in Islam of 5.8.1990 (UN Doc A/45/421/5/21797, 199), Art 18 of which expressly recognises a right to privacy for individuals.

pertinent in the context of data protection.[437] It is also manifested in case law developed pursuant to Art 17 of the ICCPR and Art 8 of the ECHR. Both provisions have been authoritatively interpreted as requiring implementation of and respect for many of the core principles of data protection laws.[438] Indeed, the case law indicates that each provision has the potential to embrace all of these core principles, though it has not, as yet, added to them in any significant way.[439]

A second important source of legal inspiration for the emergence of data protection laws are various provisions in national Constitutions (or Basic Laws). Sometimes the link between data protection laws and Constitutional provisions is expressly recognised in the former.[440] More commonly, though, the link is expressly provided for in the Constitutions. Some of the latter contain an express right to data protection.[441] Other Constitutions expressly require that data protection legislation be enacted.[442] Constitutions often also contain a broad range of other provisions that help form the normative underpinnings of data protection laws. These provisions are expressed in terms of protecting such values as human dignity, personality, privacy and the like.

Though the latter sorts of values are relatively diffusely formulated, their normative relevance – both actual and potential – for the development of data protection laws has been made manifest in judicial decision making, most notably that of the Federal German Constitutional Court. In a famous and influential decision of 15.12.1983, the Court struck down parts of the federal *Census Act* (*Volkzählungsgesetz*) of 1983 for breaching Arts 1(1) and 2(1) of the Federal Republic's *Basic Law*.[443] Article 1(1) provides: 'Human dignity is inviolable. To

---

437 See Art 1 of both instruments. Note too the Preamble to Australia's federal *Privacy Act* (indicating that the Act is, in part, necessary to give effect to the right of privacy in Art 17 of the ICCPR).

438 In relation to Art 17 of the ICCPR, see General Comment 16 issued 23.3.1988 by the Human Rights Committee (UN Doc A/43/40, 181–183; UN Doc CCPR/C/21/Add.6; UN Doc HRI/GEN/1/Rev 1, 21–23), paras 7 & 10. In relation to Art 8 of the ECHR, leading cases decided by the ECtHR include *Klass v Germany* (1978) A 28; *Malone v United Kingdom* (1984) A 82; *Leander v Sweden* (1987) A 116; *Gaskin v United Kingdom* (1989) A 160; *Kruslin v France* (1990) A 176-A; *Niemitz v Germany* (1992) A 251-B; *Amann v Switzerland* (2000) RJD 2000-I. See further Bygrave, *supra* n 102.

439 See further Bygrave, *supra* n 102.

440 See, eg, s 2(a) of the US federal *Privacy Act*.

441 See, eg, Art 59(1) of the Hungarian Constitution of 1949; Art 35 of the Portuguese Constitution of 1976; and Art 19(3) of the Slovak Constitution of 1992. All Constitutional references here and in the following are taken from the comprehensive, regularly up-dated collection of national Constitutions available via <http://www.uni-wuerzburg.de/law/>.

442 See, eg, Art 8 of Chapt II of the Finnish Constitution (as recently amended); Art 10(2) & (3) of the Netherlands' Constitution of 1983; and Art 18(4) of the Spanish Constitution of 1978. Cf the less stringent requirement in Art 3 of Chapt 2 of Sweden's Instrument of Government of 1975 (*Regeringsformen*, SFS 1974:152).

443 65 BVerfGE, 1. For an English translation of the Court's decision, see (1984) 5 *HRLJ*, no 1, 94ff. For detailed commentary, see, eg, S Simitis, 'Die informationelle Selbstbestimmung – Grundbedingung einer verfassungs-konformen Informationsordnung' (1984) *Neue juristische Wochenschrift*, 398–405;

respect and protect it is the duty of all State authority'. Article 2(1) provides: 'Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or against morality'. The Court held that the two provisions give individuals a right to 'informational self-determination' ('informationelle Selbstbestimmung'); ie, a right for the individual 'to determine for himself whether his personal data shall be disclosed and utilised'.[444] The Court went on to hold that, though this right is not absolute,[445] it will be infringed if personal data are not processed in accordance with basic data protection principles.[446] Of the latter, the Court focused especially on the principle of purpose specification.

Another important judicial decision in this context is the ruling of 9.4.1991 by the Hungarian Constitutional Court in which census legislation was struck down for violating Art 59(1)[447] of the national Constitution.[448] In reaching its decision, the Court expounded substantially the same line taken by the German Federal Constitutional Court in the Census Act judgment. It laid particular emphasis on the purpose specification principle,[449] and stipulated, concomitantly, that the creation of a general, uniform PIN for unrestricted use is unconstitutional.[450]

Both of the above decisions have had a significant impact on the development and conceptualisation of data protection law in Germany and Hungary respectively. The *Census Act* decision helped stimulate efforts to revise and strengthen Germany's federal data protection legislation.[451] The impact of the judgment of the Hungarian

---

(Cont.)
EH Riedel, 'New Bearings in German Data Protection: Census Act 1983 Partially Unconstitutional' (1984) 5 *HRLJ*, no 1, 67–75. For analysis of the decision in the light of the Court's subsequent case law, see J Aulehner, '10 Jahre 'Volkzählungs'-Urteil: Rechtsgut und Schutzbereich des Rechts auf informationelle Selbstbestimmung in der Rechtsprechung' (1993) 7 *CR*, 446–455. For analysis of the long-term significance of the decision for German data protection, see S Simitis, 'Das Volkzählungsurteil oder der lange Weg zur Informationsaskese – (BVerfGE 65, 1)' (2000) 83 *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, no 3–4, 359–375. For comparison of the decision with the equivalent case law of the US Supreme Court, see PM Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37 *American J of Comparative Law*, 675–701.

444 65 BVerfGE, 43 ('Das Grundrecht gewährleistet … die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen').

445 *Ibid*, 43–44.

446 *Ibid*, 46ff.

447 See *supra* n 441.

448 See Hungary's Official Gazette (*Magyar Kozlony*), No 30, 13.4.1991, 805. For commentary on the court's decision and its impact on Hungarian society, see I Székely, 'Hungary Outlaws Personal Number' (1991) 14 *TDR*, no 5, 25–27.

449 See part II of the judgment.

450 See part III, point 3 of the judgment.

451 See generally Simitis, *supra* n 56, paras 26ff. Cf Simitis, 'Das Volkzählungsurteil oder der lange Weg zur Informationsaskese – (BVerfGE 65, 1)', *supra* n 443 (detailing the slow and incomplete implementation of the principles laid down in the decision).

Constitutional Court is partly seen in Art 7(2) of Hungary's data protection Act which states that 'unlimited, general and uniform personal identification codes shall not be used'.

Facets of administrative law and law on judicial proceedings provide a third important source of inspiration for the emergence of data protection legislation. Traditional rules on due process embody principles that are precursors to some of the central data protection rules. These principles require in part that government and judicial decision makers: (i) be unbiased or disinterested in the matter which is decided; (ii) base their decisions on relevant evidence; and (iii) give an opportunity to be heard to persons whose interests will be adversely affected by the decisions.[452] Strong links exist between the first two of these principles and those provisions of data protection laws dealing with information quality.[453] Equally strong links exist between the third-listed principle and those provisions in data protection laws dealing with data subject participation and control.[454] Some of the latter provisions – particularly those concerning the access rights of data subjects – also parallel the thrust of legislation on public access to government-held information (hereinafter termed legislation on 'freedom of information' (FOI)).[455]

At a higher level of abstraction, we can discern within data protection laws considerable influence from older doctrines on 'rule of law'. Such doctrines are broadly concerned with regulating power relations between the State and citizens by curbing arbitrariness in the exercise of State power. In furtherance of this concern, they stipulate the importance of subjecting State power to legal controls that promote foreseeability and accountability in government decision-making processes.[456] This is not to say that the concerns of doctrines on rule of law are fully commensurate with the concerns of data protection laws. While the former are traditionally limited to governing the relationship between State organs and citizens, most data protection laws also regulate directly the relationship between private organisations and

---

452 See, eg, M Allars, *Introduction to Australian Administrative Law* (Butterworths, 1990), chapt 6, for an overview of these principles as found in Australian administrative law. For an overview of the equivalent principles as found in Norwegian administrative law, see, eg, Eckhoff & Smith, *supra* n 36, chapts 18, 22–24.

453 For an overview of such provisions, see Chapter 3 (section 3.5).

454 For an overview of such provisions, see Chapter 3 (section 3.6).

455 Cf the emergence in Latin American jurisdictions of relatively rudimentary data protection regimes revolving around the concept of 'habeas data' (roughly meaning 'you should have the data'). The latter concept is an outgrowth of due-process doctrine based on the writ of *habeas corpus*. See further A Guadamuz, 'Habeas Data: The Latin-American Response to Data Protection' (2000) *The Journal of Information Law and Technology*, no 2, <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html>. As Guadamuz notes, 'habeas data' primarily embraces access and rectification rights, though in some of the jurisdictions concerned other rights figure too, such as the right to demand that personal data be kept confidential.

456 See further E Boe, 'Forholdet mellom rule of law og rettssikkerhet', in DR Doublet, K Krüger & A Strandbakken (eds), *Stat, politikk og folkestyre: Festskrift til Per Stavang på 70-årsdagen* (Bergen: Alma Mater, 1998), 43–65; and Allars, *supra* n 452, 14ff.

citizens. Moreover, doctrines on rule of law focus traditionally on specific decision-making processes to which a private individual or organisation is a party, whereas the focus of data protection laws is on the processing of personal information. Such processing need not be directly related to a specific decision-making process, though it often is.[457] Further, doctrines on rule of law tend to encompass a range of issues – eg, the quality of legal norms and the quality of judicial operations – with which data protection laws are not directly concerned.

A fourth major source of inspiration for the emergence of data protection laws are rules in national legislation and case law which lay down rights to privacy and/or personality.[458] Rules dealing with defamation, wrongful discrimination and intellectual property are also pertinent, though to a lesser degree.[459] All of these rules prefigure the basic thrust of data protection laws in that they prohibit various kinds of behaviour, including certain ways of processing personal data, in order to protect the autonomy, integrity, dignity and/or privacy of the data subject(s).

There is little doubt that general doctrines on property rights have also played a role in inspiring data protection laws, though the exact importance and extent of this role are difficult to gauge. Much depends on how one defines property rights. These can be defined at such a level of generality that they are taken as providing the fundamental basis for enormous tracts of the legal system.[460] If we define property rights as conferring ownership of some object or thing, in the sense that the rights holder is given a legally enforceable claim to exclude others from utilising that object/thing, some reflection of such rights can be discerned in those provisions of data protection laws that make the processing of personal data conditional on the consent of the data subject(s). However, these provisions are frequently watered down by exemptions that make it difficult to see the resultant level of data ownership (in the above-defined sense) as much more than symbolic. Moreover, there tend to be few, if any, other direct and obvious manifestations of property rights doctrines in data protection laws or their *travaux préparatoires*. This is not to deny the possibility

---

457 At the same time, though, no real reason exists – apart from the weight of tradition – for maintaining the two limits identified above in the concerns of rule of law doctrines. Such doctrines are logically capable of being applied to private sector practices and to the processing of personal information relatively independent of specific decision-making processes.

458 For Norwegian examples, see *infra* n 553 *et seq* and accompanying text.

459 For a short discussion of the interrelationship of copyright and privacy/data protection law, see LA Bygrave, 'The Technologisation of Copyright: Implications for Privacy and Related Interests' (2002) 24 *EIPR*, 51, 52.

460 As exemplified in the following claims by Samuel Warren and Louis Brandeis in their seminal journal article on the right to privacy in Anglo-American common law: 'The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested': S Warren & L Brandeis, 'The Right to Privacy' (1890–91) 4 *Harvard L Rev*, 193, 211. In other parts of their article, however, Warren and Brandeis seem to view such a broad use of the notion of property rights as out of keeping with usual understanding of the notion: see, eg, *ibid*, 213.

of several of the core principles of the legislation serving to protect, albeit indirectly, the idea(l) of data subjects owning their data (again, in the above-defined sense of ownership).[461]

Some of the early and influential contributors to the discourse out of which data protection laws emerged, have championed property rights doctrines as providing a desirable basis for data protection regimes.[462] A similar line has been advanced by some of the more recent contributors to data protection discourse.[463] Nevertheless, just as many, if not more, contributors to this discourse – especially outside North America – are sceptical to such an approach.[464]

As an aside, this scepticism has much to commend it. A property rights approach could encourage a commodification of data protection rights and ideals which favours certain sectors of the population. Secondly, it is questionable that adoption of property rights approaches will assist arguments for providing increased levels of data protection, as such rights – like most other rights – are seldom applied in an absolute manner. Thirdly, the conceptual propriety and utility of the notion of 'ownership' of personal data/information are doubtful. Fourthly, many of the challenges faced by data protection law and policy cannot be adequately addressed under the property rights rubric. One such challenge, for instance, concerns the ability (or, rather, increasing inability) of data subjects to comprehend the logic of information systems.

It would be wrong to see the existence of each of the legal factors canvassed above as a necessary precondition for the enactment of data protection laws. For instance, some countries, such as the UK and Germany, enacted data protection laws without having comprehensive FOI legislation already in place. To take another

---

461 See further D Elgesem, 'Remarks on the Right of Data Protection', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 83, 90ff (analysing the 'property function' of data protection laws; ie, the way in which the latter help secure a data subject's 'claim to ex ante agreement to the transfer of personal information').

462 See primarily Westin, *supra* n 335, 324–325.

463 See, eg, P Mell, 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness' (1996) 11 *Berkeley Technology LJ*, 1, espec 74ff; RT Nimmer & PA Krauthaus, 'Information as Property: Databases and Commercial Property' (1993) 1 *Int J of Law and Information Technology*, 3, espec 29ff; P Blume, 'New Technologies and Human Rights: Data Protection, Privacy and the Information Society', Paper no 67, Institute of Legal Science, Section B, University of Copenhagen, 1998, 4; KC Laudon, 'Markets and Privacy' (1996) 39 *Communications of the ACM*, no 9, 92–104; J Rule & L Hunter, 'Towards Property Rights in Personal Data', in CJ Bennett & R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999), 168–181.

464 See, eg, Y Poullet, 'Data Protection between Property and Liberties – A Civil Law Approach', in HWK Kaspersen & A Oskamp (eds), *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990), 161–181; Miller, *supra* n 335, 211ff; R Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989), 49; J Litman, 'Information Privacy/Information Property' (2000) 52 *Stanford L Rev*, 1283–1313.

example, some countries, such as Australia and the UK, enacted data protection laws without specifically recognising a right to privacy in their respective legal systems.

Further, the links between each of the above-cited legal factors and data protection laws are not always directly recognised in the *travaux préparatoires* of the latter or in other related commentary. Likewise, awareness of such links has varied from jurisdiction to jurisdiction and from period to period. In Norway, for example, the enactment of the *Personal Data Registers Act* was accompanied by considerable awareness of the close similarity between data protection concerns and administrative law doctrines,[465] whilst the links to human rights as formalised, say, in the ECHR and ICCPR were downplayed.[466] In recent years, however, data protection discourse in Norway has increasingly recognised the normative importance of human rights law for data protection.[467] To take another example, legislators in some European countries, such as France, apparently failed to see the close connections between laws on data protection and laws on FOI, at least when these laws were first enacted.[468] This is in contrast to Canada and Hungary where the two types of laws were enacted in single, co-ordinated legislative packages.

Finally, the development and existence of data protection laws have inspired – and will continue to inspire – changes in other legal fields, including those to which the above-cited legal factors belong. There exists, in other words, an ongoing cross-fertilisation of legal influences. This process is most apparent in the interaction of data protection laws and human rights law. On the one hand, greater readiness to construe treaty provisions on the right to privacy as containing data protection guarantees is partly inspired by the emergence of data protection laws.[469] On the other hand, such readiness serves to stimulate the enactment of data protection laws in countries where such laws do not already exist, or to stimulate the strengthening of existing laws. Such readiness also serves to anchor data protection laws more firmly in traditional human rights doctrines, thereby influencing the way these laws are conceptualised.

In relation to some legal fields, we see only the beginnings of a potential cross-fertilisation process. An example here is the interaction of data protection laws with

---

465 See further Chapter 7 (section 7.2.4) and references cited therein.

466 There is, eg, a paucity of references to human rights in the *travaux préparatoires* to the PDRA. Cf Bing, *supra* n 48, 232 (claiming in 1981 that Norwegian and other European data protection laws are 'more closely related to the law of public administration than to the law of individual liberties').

467 See, eg, P Falck, *Personvern som menneskerett. Den europeiske menneskerettighets-konvensjon artikkel 8 som skranke for innsamling, behandling og bruk av personopplysninger*, Det juridiske fakultets skriftserie nr 56 (University of Bergen, 1995); JP Berg, 'Offentlige skattelister – i strid med EMK?' (1998) *Kritisk Juss*, 203–204; NOU 1997:19, 41–42. Cf Ø Rasmussen, *Kommunikasjonsrett og taushetsplikt i helsevesenet* (Ålesund: AS Borgund, 1998), 50–52 (underplaying this importance).

468 See, eg, H Burkert, 'Access to Information and Data Protection Considerations', in C de Terwangne, H Burkert & Y Poullet (eds), *Towards a Legal Framework for a Diffusion Policy for Data held by the Public Sector* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1995), 23, 49.

469 See further Bygrave, *supra* n 102 with respect to case law pursuant to Art 17 of the ICCPR and Art 8 of the ECHR.

competition law. In at least one jurisdiction (Belgium), the enactment of data protection law is leading to changes in traditional doctrines on 'fair competition', with the latter being infused with elements of the former.[470] However, the full extent and manner of such impact remain to be seen, as do the ways in which competition law might rub off on the practice and/or conceptualisation of data protection laws.

6.4.2 NEGATIVE LEGAL FACTORS

It is trite that data protection laws would not have emerged had legislators believed that pre-existing legal rules could assuage public fears over the developments outlined in section 6.2. Thus, the introduction of data protection laws has been preceded by a range of studies concluding, for the most part, that other rules already in existence lack the precision and/or breadth to tackle these fears sufficiently.[471]

In some cases, pre-existing legal rules have also been found to have the potential to *exacerbate* threats to personal privacy and integrity. This is best exemplified in Sweden, which has a long-standing tradition of open government enshrined in constitutional provisions granting citizens a right of access to government documents.[472] While concern in the late 1960s about this access right focused initially on the prospect of the right being curtailed because of its possible inapplicability to machine-readable data, a subsequent concern arose that computerisation might well lead to a situation in which exercise of the right facilitated the fast and easy dissemination of large amounts of personal data.[473] Accordingly, the enactment of Sweden's *Data Act* of 1973 can be viewed as 'a qualification of the principle of freedom of information, made in recognition of the threat to personal privacy posed by the age of computers'.[474]

Some legal instruments previously judged inadequate from a data protection perspective, have subsequently shown considerable potential to embrace data protection principles. An example is the ECHR. Work by the CoE on drafting its early Resolutions on data protection,[475] followed by its 1981 Convention on the same

---

470 See the Belgian case law referred to *infra* n 613.

471 For Australia, see particularly ALRC, *supra* n 158, vol 1, part III, espec 476–477. For Denmark, see particularly *Delbetænkning om private registre*, Bet 687 (Copenhagen: Statens trykningskontor, 1973), espec 39–40; *Delbetænkning om offentlige registre*, Bet 767 (Statens trykningskontor, 1976), espec 147–148. For Sweden, see particularly *Data och integritet*, SOU 1972:47, espec 61–64. For the USA, see particularly Westin, *supra* n 335, chapts 13–14; Miller, *supra* n 335, chapts V–VI.

472 See Chapter 2, § 2 of the *Freedom of the Press Act* of 1949 (*Tryckfrihets-förordningen*, SFS 1949:105), which is part of the Swedish Constitution. This right of access was first established in the *Freedom of the Press Act* of 1766.

473 See further Bennett, *supra* n 5, 62–65.

474 Flaherty, *supra* n 267, 99.

475 Resolution (73)22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector (adopted 26.09.1973), and Resolution (74)29 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Public Sector (adopted 24.09.1974).

matter, arose out of a perception that the ECHR did not provide sufficient protection for individuals in the face of computerised processing of personal data, particularly in the private sector.[476] However, as noted in section 6.4.1, the ECtHR has since exhibited increasing willingness to read basic data protection principles into Art 8 of the ECHR.[477]

476 See, eg, Hondius, *supra* n 55, 63ff and references cited therein.

477 See further Bygrave, *supra* n 102.

7. Values and Interests Safeguarded by Data Protection Laws

7.1 Introduction

This chapter explores the rationale of data protection laws by elucidating the values and interests that these laws aim, explicitly and/or implicitly, to safeguard. In the following, the term 'data protection interests' is used to denote these concerns of data protection laws. The concerns need not manifest themselves in the provisions of the laws; traces of them might be found instead in the *travaux préparatoires* for the laws or in the way the laws are applied by data protection authorities and other enforcement bodies.

While the term 'data protection interests' is primarily used in this chapter to denote the *current* concerns of data protection laws, it is also capable of embracing interests which closely relate, conceptually and ethically, to these concerns but which are not safeguarded to a significant degree by the present laws. The identification of such interests serves to point out directions in which data protection laws might move in the future. Indeed, an intention of this chapter is not simply to aid in delineating the legally valid ambit of current data protection legislation (ie, the ambit that would be seen as acceptable by the judiciary); it is also to aid in delineating the *potential* 'agenda' of data protection as a body of law.

Data protection interests can be divided into two main categories: (i) the interests held by data subjects; and (ii) the interests held by data controllers. The bulk of the chapter is taken up with analysing the first category. This is due not just to the primary thrust of the basic aims of data protection laws but also the concerns of Part III.

7.2 Interests of Data Subjects

7.2.1 PRIVACY AND INTEGRITY

The notions of privacy and, to a lesser extent, integrity figure centrally in the most popular conceptualisations of the data protection interests of data subjects. According to these conceptualisations, one – if not *the* – major aim of data protection laws is to safeguard the privacy and/or integrity of data subjects. Of the two notions, privacy

tends to enjoy most prominence. As shown below, however, the notions of privacy and integrity are often defined similarly in data protection discourse.

It is difficult to disagree with the proposition that data protection laws are very much concerned with safeguarding the privacy and/or integrity of data subjects. This concern is expressly manifest in the opening provisions of many data protection laws, both old and new, or in the laws' *travaux préparatoires*.[478]

The salience of the privacy concept in this context partly reflects the central importance accorded to privacy as ideal and value in liberal ideology.[479] It is in societies built up to a large extent around liberalism that data protection discourse has flourished. Widespread public discussion of the implications of computerised processing of personal data first took off in the USA, where there already existed a long (though by no means consistent) tradition of public, academic and judicial concern for privacy.[480] The salience of the privacy concept in North American data protection discourse contributed to ensuring a high profile for the concept in the subsequent discussions in other countries on data protection issues. This was particularly the case with other English-speaking countries and in international forums where English dominates. Yet also other countries framed much of their discussions, at least initially, around concepts that roughly equate with, or embrace, the privacy concept. In Western Europe, these concepts tended to be drawn from jurisprudence developed there on legal protection of personality. For example, discussion in Germany initially focused to a considerable extent on the concept of 'Privatsphäre' ('private sphere').[481] In Sweden – as shown further below – it centred around the concept of 'personlig integritet' ('personal integrity').

Despite their high profile in data protection discourse, the concepts of privacy and integrity remain somewhat nebulous. This is notoriously so with privacy. The concept is difficult to define with precision. This difficulty is both engendered and exacerbated by the loose, haphazard manner in which the concept is sometimes used,[482] and by the fact that existing definitions can be so vacuous as to render the concept analytically unserviceable.[483] There is also considerable controversy, if not

---

478 See Chapter 2 (section 2.3).

479 See S Lukes, *Individualism* (Oxford: Blackwell, 1973), 62; Mallmann, *supra* n 13, 17.

480 For an overview of the development of US concern for privacy, see PM Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill/London: University of North Carolina Press, 1995).

481 See, eg, the 1970 proposal by the (West) German Interparliamentary Working Committee (Interparlamentarische Arbeitsgemeinschaft) for a 'Law for the Protection of Privacy from Misuse of Databank Information' (*Gesetz zum Schutz der Privatsphäre gegen Missbrauch von Datenbankinformationen*): described in HP Bull, *Datenschutz oder Die Angst vor dem Computer* (Munich: Piper, 1984), 85.

482 See, eg, ME Katsh, *Law in a Digital World* (New York: Oxford University Press, 1995), 234 (employing privacy as both a condition and as a doctrine with a particular goal).

483 See, eg, SG Davies, *Monitor: Extinguishing Privacy on the Information Superhighway* (Sydney: Pan Macmillan Australia, 1996), 260 (defining privacy as 'the relationship between people and the world around them').

confusion, both within and outside academic circles over the proper ambit of the privacy concept.[484] It does not help either that what is considered private, plus the manner in which privacy norms are enforced, can vary from one period and culture to another.[485] All of the above difficulties apply equally, if not more, in relation to the concept of integrity.[486]

Thus, it should come as no surprise to find that privacy and integrity are never directly defined in those data protection laws that employ the terms. The laws which come closest to defining either of the terms only provide definitions of what amounts to a *breach* of privacy for the purposes of each Act.[487] This failure to define privacy and integrity entails that the meaning of these concepts for the purposes of data protection laws must be sought partly in the substance of the principles laid down in the laws themselves and partly in the way these principles have been applied. At the same time, if use of the terms privacy and integrity in the legislation is not to be regarded as redundant, the failure to define the terms entails that their meaning must also be derived in part from general, societal notions of what privacy and integrity are.

The failure to define privacy and integrity in data protection laws is not necessarily a weakness with these laws: it provides room for flexibility in their implementation. Further, the fact that the concepts of privacy and integrity are somewhat vague does not necessarily detract from their utility in data protection laws and discourse: it enables them to assimilate and express in a relatively comprehensive, economic manner the congeries of fears attached to increasingly intrusive data-processing practices.[488] Indeed, this characteristic helps to explain the protracted prominence of these concepts in data protection discourse. Moreover, in data protection advocacy, it 'may be useful to adopt a large concept in order to offset an equally large rhetorical counter-claim: freedom of inquiry, the right to know, liberty of the press …'.[489]

Nevertheless, failure to define the concepts in data protection laws has a cost insofar as it detracts from the laws' capacity for prescriptive guidance. The exact extent of this cost depends on the way in which the concepts are employed: if they

---

484 For an overview of the lines of debate, see generally JC Inness, *Privacy, Intimacy, and Isolation* (New York/Oxford: Oxford University Press, 1992), chapt 2; JW DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca/London: Cornell University Press, 1997), chapts 2–3.

485 For examples of variation, see B Moore, *Privacy: Studies in Social and Cultural History* (Armonk, New York: ME Sharpe, 1984); JM Roberts & T Gregor, 'Privacy: A Cultural View', in JR Pennock & JW Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), 199–225.

486 See, eg, *En ny datalag*, SOU 1993:10, 150–161 (documenting the difficulties experienced in Swedish data protection discourse with respect to arriving at a precise definition of 'personlig integritet').

487 See, eg, s 13 of Australia's federal *Privacy Act* and s 2 of Israel's *Protection of Privacy Law*, 5741-1981.

488 See also PA Freund, 'Privacy: One Concept or Many', in JR Pennock & JW Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), 182, 193–194.

489 *Ibid*, 193.

merely figure in the objects clause of a law, the cost will tend not to be so great as when the concepts are employed in rules intended to regulate behaviour more directly. Another cost of failure to define the concepts, not just in the context of their use in data protection laws, is that they remain vulnerable to the criticism of being incapable of definition. Such criticism runs over easily into claims that the concepts have no independent, coherent meaning in themselves and should be subsumed by other concepts.[490] This cost is difficult to tolerate for persons (such as myself) who view the concepts of privacy and integrity as denoting distinct values that are not adequately delineated by other notions, and who believe, accordingly, that normative discourse would be impoverished were these concepts to fall into disuse.[491]

The above remarks notwithstanding, the privacy concept is pregnant with definitional variation. Analysis of the literature on privacy reveals four major ways of defining the concept.

One group of definitions views privacy essentially in terms of non-interference. This sort of characterisation of privacy gained prominence largely in the wake of the law review article by Warren and Brandeis who argued that the right to privacy in Anglo-American common law is part and parcel of a right 'to be let alone'.[492] In Sweden, the concept of personal integrity has been defined along similar lines.[493]

A second group of definitions, closely related to the first, conceives of privacy in terms of degree of access to a person. Ruth Gavison's definition of privacy as a condition of 'limited accessibility' is a leading example here. According to Gavison, this condition of limited accessibility consists of three elements: 'secrecy' ('the extent to which we are known to others'); 'solitude' ('the extent to which others have physical access to us'); and 'anonymity' ('the extent to which we are the subject of others' attention').[494]

A third group of definitions conceives of privacy primarily in terms of information control. The most influential of these definitions is by Alan Westin:

---

490 For an example of this sort of claim mounted against the privacy concept, see JJ Thomson, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs*, 295–314.

491 This line is argued most convincingly and elegantly by Ruth Gavison: see Gavison, *supra* n 64.

492 Warren & Brandeis, *supra* n 460, 195, 205. See also the influential definition of the right to privacy adopted at the Nordic Conference of Jurists (organised by the International Commission of Jurists) in Stockholm, May 1967: 'The Right to Privacy is the right to be let alone to live one's own life with the minimum of interference'. Cited in S Strömholm, *Right of Privacy and Rights of the Personality* (Stockholm: Norstedt, 1967), Appendix IV, 237.

493 See, eg, *Data och integritet*, SOU 1972:47, 56 and *Personregister – Datorer – Integritet*, SOU 1978:54, 36.

494 Gavison, *supra* n 64, 428–436. Similar definitions are advanced in, eg, A Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totoma, New Jersey: Rowman & Littlefield, 1988), 15; Bok, *supra* n 63, 10; JH Reiman, 'Driving to the Panopticon' (1995) 11 *Santa Clara Computer and High Technology LJ*, 27, 30; O'Brien, *supra* n 64, 16.

> 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[495]

In Sweden, the concept of personal integrity has also been viewed as embracing (though not necessarily limited to) a similar claim to information control.[496]

Finally, there exists a group of definitions relating privacy exclusively to those aspects of persons' lives that are 'intimate' and/or 'sensitive'. Julie Inness, for instance, defines privacy as 'the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions'.[497] According to such a view of privacy, not every disclosure of any type of information about a person will amount to a loss of privacy. A loss will occur only when 'sensitive' and/or 'intimate' personal information is disclosed.[498]

The above four groups of definitions are by no means exhaustive of the various ways in which privacy is conceived, but they constitute the main lines of definition. Putting aside differences in terms of whether they view privacy as a state/condition, claim or right,[499] there is little direct clash between them. This harmony, however, is preconditioned on the assumption that the first three definitional categories (ie, those defining privacy in terms of non-interference, inaccessibility and information control) only encompass intimate and/or sensitive aspects of persons' lives. As shown further below, many of the scholars etc who champion one of the first three groups of definitions, do not view privacy as delimited in this way.

An extensive and long-running debate has raged over which of the above types of definitions is the most correct. To analyse this debate in detail is unnecessary for the purposes of this book. It suffices to note, first, that the debate carries with it the danger of underplaying the multidimensional character of privacy. Much of it also overlooks the fact that law and policy do not always need to operate with precise, clean-cut definitions of values.[500] Furthermore, the debate is difficult to resolve conclusively because it rests to a considerable extent on intuitive assessments of how the privacy concept is supposed to be commonly understood.

---

495 Westin, *supra* n 335, 7. Other examples of definitions of privacy primarily in terms of information control are found in L Lusky, 'Invasion of Privacy: A Classification of Concepts' (1972) 72 *Columbia L Rev*, 693, 709; Miller, *supra* n 335, 40; EA Shils, 'Privacy: Its Constitution and Vicissitudes' (1966) 31 *Law & Contemporary Problems*, 281, 282.

496 See, eg, *Skydd mot avlyssning*, SOU 1970:47, 58; *Fotografering och integritet*, SOU 1974:85, 56; *ADB och samordning*, SOU 1976:58, 127; *En ny datalag*, SOU 1993:10, 159.

497 Inness, *supra* n 484, 140.

498 See, eg, Inness, *supra* n 484, 58ff; WA Parent, 'A New Definition of Privacy for the Law' (1983) 2 *Law and Philosophy*, 305, 306–307; Wacks, *supra* n 464, 16–18.

499 These differences cut across the boundaries of the four definitional groups.

500 See also DeCew, *supra* n 484, espec chapt 4; AL Allen, 'Genetic Privacy: Emerging Concepts and Values', in MA Rothstein (ed), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (New Haven: Yale University Press, 1997), 31, 35.

The major role played by intuition is especially apparent in relation to the issue of whether or not the disclosure of 'non-intimate' information about oneself involves a loss of privacy. Some scholars contend that privacy is not diminished by disclosure of such information, and appeal to our intuition in support of their contention.[501] Other scholars appeal to our intuition in order to justify the opposite claim.[502] On this issue, my intuition sides with the latter scholars.[503] Another issue in which intuition plays a significant role concerns whether the notion of privacy can apply to corporate entities.[504]

Of the four definitional groups outlined above, the conception of privacy that best accords with my intuition is in terms of limited accessibility along informational, spatial and psychological planes. I believe that this conception comes closest to capturing the core of privacy at the same time as it does relatively large justice to the multidimensionality of the concept.

In data protection discourse, however, the most popular definitions of privacy are in terms of information control.[505] Also non-English words describing the data protection interest(s) of data subjects – for instance, 'personlig integritet' (Swedish) and 'personvern' (Norwegian) – are commonly defined along similar lines.[506] The popularity of such definitions in data protection discourse should come as no surprise. They appear directly applicable to the issues raised by organisations' data-processing practices, at the same time as they harmonise fairly well with, and build upon, central principles on due administrative process. Furthermore, a control-based definition of privacy arguably lends the concept considerable normative force as it allows privacy advocates to tap into the dynamic ethical undercurrent associated with the ideal of self-determination. In my opinion, though, privacy is more aptly characterised as a condition which can result from, or facilitate, exercise of information control, rather than as co-extensive with such control. Concomitantly, conflating privacy with control serves to rob privacy of its conceptual uniqueness, which is already under much press. This might detract in turn from the force of

---

501 See, eg, Wacks, *supra* n 464, 19; Inness, *supra* n 484, 58.

502 See, eg, A Schafer, 'Privacy: A Philosophical Overview', in D Gibson (ed), *Aspects of Privacy: Essays in Honour of John M Sharp* (Toronto: Butterworths, 1980), 1, 11; JW DeCew, 'The Scope of Privacy in Law and Ethics' (1986) 5 *Law and Philosophy*, 145, 168–169.

503 Nevertheless, the nature of the information disclosed will help to determine the *significance* of the privacy loss for the person concerned and thereby the extent to which a remedy for that loss is required.

504 See further Chapter 12 (section 12.2).

505 In addition to the references cited *supra* n 495, see, eg, B Slane, in *Private Word: News from the Office of the Privacy Commissioner*, April 1996, no 4, 6; RD Blekeli, 'Framework for the Analysis of Privacy and Information Systems', in J Bing & KS Selmer (eds), *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980), 21, 24; Committee on Data Processing (the Lindop Committee), *Report of the Committee on Data Protection*, Cmnd 7341 (London: HMSO, 1978), 10, para 2.04; Rodotà, *supra* n 19, 261.

506 On definitions of 'personvern', see *infra* section 7.2.4. On definitions of 'personlig integritet', see *supra* n 496.

privacy advocacy in the long run. Witness, for instance, the considerable criticism of US case law on the constitutional right to privacy for using the privacy concept to address issues that seem essentially to concern autonomy.[507]

The least popular conception of privacy in data protection discourse appears to be that linking privacy exclusively to intimate or sensitive aspects of persons' lives. One probable factor behind this relative unpopularity is that intimacy-oriented definitions of privacy are unable to anticipate and capture the process by which detailed personal profiles are created through combining disparate pieces of ostensibly innocuous information. As information systems in both the public and private sectors become increasingly integrated, such aggregation is likely to occur on an even larger scale during the coming decades.[508] Accordingly, any conception of privacy which does not capture or reflect this process is of relatively little utility for present and future appreciation of data protection issues.

A related cause of unpopularity of intimacy-oriented conceptions of privacy stems arguably from their relatively close connection to so-called 'Sphärentheorie' ('sphere theory').[509] The latter, which appears to have reached its fullest development in German jurisprudence on 'Persönlichkeitsrecht' ('law of personality'), is based upon a view of personal life as divided into a series of spheres ('Sphären') or realms ('Bereich') of activity (including expression and thought), each protected from intrusion according to its intimacy or sensitivity for the individual concerned.[510]

Elements of the theory had some influence on early contributions to data protection discourse. This can be seen, for example, in Jon Bing's attempt to categorise all personal data according to their sensitivity.[511] Yet the theory was quickly dispensed with as the primary operational rationale for data protection law, mainly because it fails to delineate clearly the contours of the various spheres, why

---

507 See, eg, R Wacks, 'The Poverty of Privacy' (1980) 96 *Law Quarterly Rev*, 73, espec 78ff; H Gross, 'Privacy and Autonomy', in JR Pennock & JW Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), 169, 180–181; E Boe, ''The Right to Privacy' i USA' (1994) *LoR*, 577–578.

508 See further Chapters 6 and 17 (sections 6.2.2 and 17.2).

509 This is not to suggest that conceptualisations of privacy in terms of non-intrusiveness, inaccessibility or information control necessarily clash with sphere theory, but the connection between them and this theory are not as obvious since they do not expressly focus on a particular grading of intimacy or sensitivity.

510 For overviews of the theory, its origins and problems, see, ia, A Hasselkuss & C-J Kaminski, 'Persönlichkeitsrecht und Datenschutz', in W Kilian, K Lenk & W Steinmüller (eds), *Datenschutz* (Frankfurt am Main: Athenäum, 1973), 109, 115–126; H-H Maass, *Information und Geheimnis im Zivilrecht* (Stuttgart: Ferdinand Enke, 1970), 22ff. Hubmann, for instance, identifies three main spheres. In order of ascending intimacy and worthiness of protection, these are: the individual sphere ('Individualsphäre'), private sphere ('Privatsphäre) and secret sphere ('Geheimsphäre'). See H Hubmann, *Das Persönlichkeitsrecht* (Cologne/Graz: Böhlau, 1967, 2nd ed), 268–332. Information about activities belonging to the secret sphere is said to enjoy stringent protection against unauthorised disclosure: *ibid*, 325.

511 J Bing, 'Classification of Personal Information with Respect to the Sensitivity Aspect' in *Proceedings of the First International Oslo Symposium on Data Banks and Society* (Oslo: Universitetsforlaget, 1972), 98–141.

these exist and what breaches them.[512] The basic assumptions of the theory have also been criticised for allegedly having little or no foundation in reality: it is claimed, for instance, that the intimacy or sensitivity of data always varies from context to context.[513]

The latter claim might not amount to a telling objection to the validity of sphere theory. The claim rests on an assumption that the degree of intimacy and/or sensitivity of all personal information is ultimately a function of culturally relative norms rather than of, say, a psychological disposition shared by all human beings. This assumption is plausible but difficult to prove. Moreover, within particular, albeit broadly defined, cultures (eg, 'modern Western society'), there are *some* types of information (eg, information concerning persons' affliction by sexually-transmitted diseases) that remain intimate and/or sensitive in most – if not all – contexts (within the particular culture). It might be more correct to argue that what changes from context to context (within the particular culture) is not the degree of intimacy and/or sensitivity of such information but the extent to which one is prepared or required to allow it to be disclosed or used.[514]

In any case, sphere theory has the same major drawback from a data protection perspective as intimacy-oriented definitions of privacy: it fails to capture the creation of detailed personal profiles through the aggregation of ostensibly innocuous information.[515] A more practical problem is that legislative embodiment of the theory, or of concomitant attempts to grade data according to their sensitivity, would require a casuistic form of regulation which is complex and lengthy.[516]

Given the above problems, it is not surprising to find little direct manifestation of sphere theory and intimacy-oriented conceptions of privacy in the provisions of data protection laws. The ambit of the laws is generally not limited to information of a particular, predefined quality about persons.[517] Nevertheless, direct manifestation of sphere theory and intimacy-oriented conceptions of privacy occurs in those laws that place extra restrictions on the processing of certain types of especially sensitive, personal data.[518]

---

512 For early Norwegian criticism of the theory, see, ia, RD Blekeli, 'Individ og informasjonsbehandling – et teoribidrag' (1974) 7 *Skriftserien Jus og EDB*, 1, 11, 18–19; NOU 1975:10, 12, 38; NOU 1974:22, 31; KS Selmer, 'Elektronisk databehandling: Kan trollet temmes?' (1973) *LoR*, 195, 196.

513 See, eg, S Simitis, 'Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung' (1973) 2 *DVR*, 138, 143–145; W Steinmüller, 'Objektbereich 'Verwaltungsautomation' und Prinzipien des Datenschutzes', in Kilian, Lenk & Steinmüller, *supra* n 510, 51, 67–68.

514 See also Wacks, *supra* n 464, 23, 181.

515 See, eg, Simitis, *supra* n 513, 151–154; Steinmüller, *supra* n 513, 68–69.

516 This is indicated by Bing's attempted sensitivity grading (*supra* n 511), which listed several hundred separate data items.

517 See further Chapter 2 (section 2.4.1). Hence, Inness, who champions an intimacy-oriented definition of privacy, claims it is misconceived to characterise data protection laws as concerned with privacy. In her view, such laws are better characterised as protecting 'secrecy': Inness, *supra* n 484, 60–61.

518 See further Chapter 3 (section 3.9).

Even if intimacy-oriented conceptions of privacy are reflected only weakly in the provisions of data protection laws, we cannot conclude that such laws are only marginally concerned with safeguarding privacy. As shown further below, each of the other three main conceptions of privacy (ie, in terms of non-interference, limited accessibility and information control) are clearly embodied in most of the laws' core principles.

7.2.2 VALUES AND INTERESTS ASSOCIATED WITH PRIVACY

While data protection laws can help to safeguard data subjects' privacy, it is not the case that this is their only rationale, even from the perspective of data subjects. The safeguarding of privacy itself serves a large range of other values and interests, each of which must accordingly form part of the rationale for data protection laws.

An immense literature exists on the values and interests served by privacy.[519] There is also an immense number of ways in which these values and interests are described. Further, considerable debate occurs in this literature over the exact role privacy plays in securing these values and interests: is privacy, for instance, a necessary prerequisite for realising the value or interest concerned or is it simply a factor that enhances the likelihood of realisation? For present purposes, it suffices merely to point to central values and interests that recur in this literature, without canvassing the complicated issue of the *exact* role played by privacy in securing each value/interest. Further, it is unnecessary to differentiate here between the various definitions of privacy advanced in the literature: the analysis below is pitched at such a level of generality that it can apply to accounts of privacy in terms of either limited accessibility, non-interference, information control or protection of intimate matters.

One value promoted by privacy (and, thereby, data protection laws) is *individuality*. Privacy helps to set the boundaries by which we constitute and regard ourselves as individual persons.[520] Further, it helps to prevent the flattening out of human personalities such that they become one-dimensional[521] and/or merge with the mass.[522]

Closely related to individuality is *autonomy*. A person's privacy acts as a barrier to manipulation or control by others.[523] Concomitantly, it facilitates a person's ability

519 For an overview, see Allen, *supra* n 494, chapt 2.

520 See, eg, JH Reiman, 'Privacy, Intimacy, and Personhood' (1976) 6 *Philosophy & Public Affairs*, 26–44; I Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Monterey: Brooks/Cole Publishing Company, 1975), 48–50.

521 See, eg, H Arendt, *The Human Condition* (Chicago: The University of Chicago Press, 1958), 71.

522 See, eg, EJ Bloustein: 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University L Rev*, 962, 1003.

523 See, eg, Westin, *supra* n 335, 33.

to freely choose social roles.[524] Such independence, of course, also promotes individuality as described above.

Another pertinent value – also closely related to the first two – is *dignity*. A person's privacy serves to screen out behaviour by others which can affront his/her sense of intrinsic worth.[525] In so doing, it also serves to maintain the person's *integrity*. At the same time, rules and other conventions for protecting privacy (including, of course, data protection laws) may be viewed as ultimately grounded in respect for dignity.[526]

A fifth value served by privacy is *emotional release*. Privacy provides a refuge from the psychological stresses of having to comply with the social expectations inherent in public role-playing.[527] Concomitantly, it goes some way to providing an antidote for psychological overheating in the form, say, of schizophrenic behaviour.[528]

Closely connected to emotional release is *self-evaluation*. Privacy provides a person the necessary space and peace 'to integrate his experiences into a meaningful pattern and to exert his individuality on events'.[529]

A seventh value promoted by privacy is *inter-personal relationships* of love, friendship and/or trust. Privacy fosters such relationships by allowing persons to discriminate between other persons in terms of what information they are willing to share.[530]

All of the above values can be summed up as being more or less concerned with 'achieving individual goals of self-realization'.[531] At the same time, privacy and the above values do not simply have relevance for the well-being of individual persons; they have a broader societal significance too. Their protection serves to constitute a society infused with civility, stability, pluralism and democracy.

With regard to *civility*, norms for the protection of privacy (and of the other values listed above) both promote and embrace a concern for mutual respect between individual persons. Without such mutual respect there is little chance of building a secure sense of community.[532] Similarly, these norms help to maintain societal *stability* by dissipating the tensions inherent in social relations.[533]

---

524 See, eg, Mallmann, *supra* n 13, 36ff and references cited therein.

525 See, eg, DN Weisstub & CC Gotlieb, *The Nature of Privacy: A Study for the Privacy and Computers Task Force* (Ottowa: Departments of Communications and Justice, 1972), 46; Bloustein, *supra* n 522.

526 See, eg,Weisstub & Gotlieb, *ibid*, 50; Bloustein, *supra* n 522, 1003ff.

527 See, eg, Westin, *supra* n 335, 34–36.

528 See, eg, RK Merton, *Social Theory and Social Structure* (New York/London: The Free Press, 1968), 429.

529 Westin, *supra* n 335, 36.

530 See, eg, C Fried, 'Privacy (A Moral Analysis)' (1968) 77 *Yale LJ*, 475, 484–485; RS Gerstein, 'Intimacy and Privacy' (1978) 89 *Ethics*, 76–81; J Rachels, 'Why Privacy is Important' (1975) 4 *Philosophy & Public Affairs*, 295, 329.

531 Westin, *supra* n 335, 39.

532 See further RC Post, 'The Social Foundations of Privacy: Community and Self in the Common Law' (1989) 77 *California L Rev*, 957–1010; D Feldman, 'Privacy-related Rights and their Social Value',

With regard to *pluralism*, safeguards for privacy (and for the other values listed above) help to secure diversity of opinion and lifestyle.[534] Such safeguards also help to prevent the accumulation of political, social and/or economic power within the hands of a small group of persons.[535] Concomitantly, such safeguards also serve to secure the necessary conditions for active citizen participation in public life; in other words, they serve to secure *democracy*.[536]

The insight that privacy safeguards have broad societal benefits is not something that we can take for granted. Much of the discourse on privacy and privacy rights – particularly in the USA – has tended to focus only on the benefits these have for individuals *qua* individuals.[537] Moreover, privacy and privacy rights have often been seen as essentially in conflict with the needs of 'society'.[538] The counterpart of this is a considerable literature seeking to highlight various ways in which privacy rights detract from the common good.[539] These tendencies have the unfortunate consequence that they lead to skewed appreciation of the societal benefits of privacy rights, thus hampering advocacy for strong(er) data protection laws.

(Cont.)
in P Birks (ed), *Privacy and Loyalty* (Oxford: Clarendon Press, 1997), 15, 22ff; and, more generally, J Rawls, *Political Liberalism* (New York: Columbia University Press, 1993), 319.

533 See further B Schwartz, 'The Social Psychology of Privacy' (1968) 73 *American J of Sociology*, 741–752, espec 742.

534 Refer, eg, to the conformity-inducing potential of panopticism as described in Chapter 6 (section 6.3.1). See also Simitis, *supra* n 19, 733–734.

535 See, eg, K Lenk, 'Information Technology and Society', in G Friedrichs & A Schaff (eds), *Microelectronics and Society: For Better or For Worse* (Oxford: Pergamon Press, 1982), 273, 284. The notion of 'pluralism' denotes here diversity of opinion and lifestyle on the one hand, and broad distribution of power on the other. See further section 7.2.5 below.

536 As is made clear in the *Census Act* decision of the German Federal Constitutional Court: *supra* n 396 and accompanying text. See also, eg, R Gavison, 'Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs. Freedom of Speech' (1992) 43 *South Carolina L Rev*, 437, 461–462; Regan, *supra* n 480, chapt 8; BR Ruiz, *Privacy in Telecommunications: A European and an American Approach* (The Hague/London/Boston: Kluwer Law International, 1997), espec 10ff. See further section 7.2.5 below.

537 See generally the overview in Regan, *supra* n 480, chapts 2 & 8.

538 *Id*.

539 Common criticisms of privacy rights are that they entrench social hierarchies, promote insularity and intolerance, and permit deception and hypocrisy to flourish. Prominent examples of works in which various of these criticisms are advanced include those of Koen Raes (see *supra* n 374; 'De skjulte dimensioner i rätten til privatliv' (1989) 12 *Retfærd*, no 45, 4–17), Richard A Posner (see espec 'The Right to Privacy' (1978) 12 *Georgia L Rev*, 393–422; 'Privacy, Secrecy and Reputation' (1979) 28 *Buffalo L Rev*, 1–55), and Anders R Olsson (see *IT och det fria ordet – myten om Storebror* (Stockholm: Juridik & Samhälle, 1996)). While some of these criticisms have a limited validity, they are frequently advanced in an overly blunt, simplistic manner. Concomitantly, they often fail to take adequately into account the fact that privacy rights co-exist with, and are balanced and modified by, a range of other rules, and that it is the function of privacy rights in the overall scheme of a legal system which is crucial for assessment of their effects.

Fortunately, data protection discourse shows increasing recognition of the value of privacy and data protection norms not simply for individual persons but also for the maintenance of pluralist, democratic society. In the terminology of Michelman, Habermas and others, data protection discourse is gradually supplementing a 'liberal' perspective on data protection rights with a 'republican' perspective. Under the former perspective, rights are viewed as securing negative liberties (ie, freedom *from*), while the republican perspective sees rights as securing positive freedoms (ie, freedom *to*). Concomitantly, the liberal perspective stresses the importance of rights as safeguarding the individual against intrusions from the public sphere (polity), while the republican perspective stresses the importance of rights as enabling individuals' participation in the public sphere (polity).[540]

Prominent advocates of the latter perspective within data protection discourse are Spiros Simitis in Germany and Paul Schwartz in the USA. For Simitis, data protection laws do not signal a concern to maintain a closed, private sphere for the individual citizen but formulate rather the preconditions for creating a society based on citizen participation.[541] Schwartz argues that data protection laws should be seen as furthering both 'deliberative autonomy' (ie, 'the underlying capacity of individuals to form and act on their notions of the good when deciding how to live their lives') and 'deliberative democracy' (ie, 'the decisional process by which individuals make choices about the merits of political institutions and social policies').[542] Under the latter parole, he states that data protection laws 'must structure the use of personal data so that individuals will be free from state or community intimidation that would destroy their involvement in the democratic life of the community'.[543]

7.2.3 INFORMATIONAL VALUES AND INTERESTS

Some contributors to data protection discourse draw attention to the express concern in data protection laws with setting standards for the quality of personal information. Mallmann, for instance, views this concern as one of the two basic 'Zielfunktionen' ('goal functions') of data protection.[544] He divides this concern into three elements: ensuring that information is (i) correct, (ii) complete and (iii) not used out of context. Similarly, Burkert observes that data protection laws attempt to maintain 'borderlines

---

540 See, eg, J Habermas, *Faktizität und Geltung. Beiträge zur Diskurstheori des Rechts und des demokratischen Rechtsstaates* (Frankfurt am Main: Suhrkamp, 1992), 325ff and references cited therein; F Michelman, 'Law's Republic' (1988) 97 *Yale LJ*, 1493, 1503ff and references cited therein.

541 See, eg, S Simitis, *supra* n 336, 111.

542 PM Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 *Iowa L Rev*, 553, 560–561. See also, eg, Schwartz, *supra* n 428.

543 *Ibid*, 561.

544 Mallmann, *supra* n 13, 70–79. The other of these 'Zielfunktionen' is protection of privacy: *ibid*, 16–69.

of meaning' in the face of the technological possibility for cross-contextual processing of data.[545]

At an even higher level of abstraction, data protection laws have been viewed as measures to counter so-called 'Daten-schmutz' ('information pollution').[546] Hans-Peter Gassmann, for example, draws parallels between data protection laws and environmental protection laws, not just in the history of their development but also in their respective concerns. He suggests that data protection laws are aimed partly at sanitising the informational environment.[547]

Concern for adequate information quality appears to figure evermore prominently in data protection discourse. Indeed, Norway's new *Personal Data Act* contains an objects clause (s 1(2)) specifically referring to the need for 'adequate quality of personal data' ('tilstrekkelig kvalitet på personopplysninger') in addition to the needs for personal integrity and privacy. The growing prominence of concern for adequate information quality is due partly to aspects of the trend towards electronic interpenetration – most notably the increasingly cross-contextual character of data processing, as described in Chapter 6 (sections 6.2.1 and 6.2.2). It is due also to the accumulating body of empirical evidence (referenced in Chapter 6 (section 6.2.3)) indicating that the quality of information processed by various organisations is often poor.

While adequate information quality obviously can serve to secure the privacy and related interests of data subjects, it breaks down into a multiplicity of interests that have little *direct* connection to the values described in sections 7.2.1 and 7.2.2.[548]

7.2.4 NORWEGIAN INTEREST MODELS

This section describes Norwegian attempts to conceptualise the data protection interests of data subjects. These attempts are noteworthy for two reasons. First, they are amongst the most comprehensive and systematic of their kind. Secondly, they are concerned to a great extent with finding stable points of reference in the actual *development* and *practice* of data protection legislation.

---

545 H Burkert, 'Data Protection and Access to Data', in P Seipel (ed), *From Data Protection to Knowledge Machines* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990), 49, 62. See also Burkert, *supra* n 345, 565.

546 JN Druey, ''Daten-Schmutz' – Rechtliche Ansatzpunkte zum Problem der Über-Information', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Verlag Stämpfli & Cie, 1990), 379–396.

547 H-P Gassmann, 'Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa', in R Dierstein, H Fiedler & A Schulz, *Datenschutz und Datensicherung* (Cologne: JP Bachem Verlag, 1976), 11, 13–15.

548 See further section 7.2.5. Indeed, as demonstrated in that section, efforts to realise the values constituting adequate information quality can clash with realisation of data subjects' privacy, integrity and autonomy.

The central term used in Norwegian discourse on privacy and data protection is 'personvern'. Translated directly into English, 'personvern' means 'protection of the person'. The term was coined in the early 1970s to denote primarily the interest a person has in being able to control the processing of information on him-/herself, particularly when the processing is done by computer.[549] This definition is expressly acknowledged as being close to the definition of privacy given by Westin, Miller and others.[550] The definition was adopted early on by the Data Inspectorate,[551] and has dominated Norwegian discourse on data protection generally. However, alternative definitions have been advanced some of which are more in line with the literal connotation of 'personvern'.[552]

The notion of 'personvern' has close thematic and etymological ties to older notions of 'personlighetsvern' ('protection of the personality') and 'personlighetens rettsvern' ('legal protection of the personality'). The latter notions describe a body of law which protects the individual in various contexts from breaches of his or her physical and mental integrity.[553] Much of this body of law is set down in statutory rules, especially those of the *Penal Code*.[554] At the same time, there exists a general protection of personality which is independent of statute law (but which helps constitute the latter) and which can be developed and applied by the courts. While case law applying this protection of personality is far from extensive, it confirms that a major dimension of such protection is the safeguarding of privacy and related interests in connection with the processing of personal information.[555]

Despite the close ties between 'personlighetsvern'/'personlighetens rettsvern' and 'personvern', it is claimed that the focus of the former notions differs from that of the latter. 'Personvern' is said to focus upon the phenomenon of mass administration based on systematic, computerised processing of personal data on large numbers of persons. In contrast, the orientation of the concepts of 'personlighetsvern' and 'personlighetens rettsvern', along with their accompanying legal doctrines, is said to be towards protecting individuals' integrity in *ad hoc*

---

549 See espec RD Blekeli, 'Hva er personvern?', in RD Blekeli & KS Selmer (eds), *Data og personvern* (Oslo: Universitetsforlaget, 1977), 21.

550 Blekeli, *supra* n 505, 24.

551 See, eg, St meld 14 (1983–84), *Datatilsynets årsmelding 1982*, 15.

552 See, eg, KS Selmer, 'Datatilsynets rolle i et komplisert samfunn', in E Djønne (ed), *Datatilsynet: 10 år som personvernets vokter*, CompLex 4/90 (Oslo: TANO, 1990), 59, 66 (describing 'personvern' as primarily a safeguard for the individual to ensure that information processing in public and private administration is not carried out secretly or does not otherwise expose the individual to dangers, drawbacks or discomfort).

553 For a summary description of this body of law, see A Bratholm & B Stuevold Lassen, 'Personlighetens rettsvern', in K Lilleholt (ed), *Knophs oversikt over Norges rett* (Oslo: Universitetsforlaget, 1998, 11th ed), 102–113.

554 *Almindelig borgerlig straffelov 22 mai 1902 nr 10*. For a brief overview, see LA Bygrave & AH Aarø, 'Norway', in M Henry (ed), *International Privacy, Publicity and Personality Laws* (London: Butterworths, 2000), 333, 334ff.

555 For a brief overview, see *ibid*, 340–341.

situations (eg, exposure of individuals' private affairs in the mass media) that do not necessarily involve computerised data processing.[556] However, this distinction is rapidly blurring due to an increasing tendency to employ 'personvern' to address matters previously viewed as typically concerning 'personlighetsvern' or 'personlighetens rettsvern'.[557] Indeed, 'personvern' is now often used synonymously with protection of personal integrity.[558]

The following analysis, though, focuses on the traditional conceptualisation of 'personvern', particularly as developed by Ragnar Dag Blekeli and Knut Selmer. This conceptualisation has dominated Norwegian data protection discourse and been most fruitful in terms of operationalising 'personvern'.

A basic premise of this conceptualisation is that 'personvern' is not linked to a particular object or sphere, such as the individual's personality; rather, it is concerned with the relationship between data subject and data controller.[559] Concomitantly, the idea that 'personvern' is primarily concerned with protecting a personal sphere or space ('sphere theory' or 'sfæreteorien') is rejected.[560]

In general, 'personvern' has tended to be explicated in the context of decision-making processes. In this context, 'personvern' is said to embrace a set of related interests which a person has in relation to the making of decisions by others on the basis of information about him-/herself. The notion of interest seems to be synonymous with a concern to realise certain valued states of affairs.[561] As for the notion of decision ('beslutning'), this is sometimes viewed as capable of embracing both formal decisions made by organisations and informal reactions from persons with whom one has everyday contact.[562] Nevertheless, the thrust of analysis focuses on relatively formal decision-making processes, in line with the thrust of doctrines on 'rule of law' ('rettssikkerhet'). Indeed, the latter doctrines appear to have had a

556 See, eg, Schartum, 'Mot et helhetlig perspektiv på publikumsinteresser i offentlig forvaltning? – Rettssikkerhet, personvern og service' (1993) 16 *Retfærd*, no 63, 43, 46; Bing, *supra* n 349, 33.

557 See, eg, Den nasjonale forskningsetiske komité for medisin, *Registrering, bruk og gjenbruk av genetiske data* (Oslo: Norges forskningsråd, 1993), 12; NOU 1993:22, 42; St meld 33 (1994–95), 5; Rt 1994, 51, 56; Rt 1991, 616, 623.

558 See references, *supra* n 557.

559 Blekeli, *supra* n 549, 15; J Bing, 'Personvern og EDB: En internasjonal oversikt', in *Den personliga integriteten: Föredrag vid den XX:e nordiska studentjuristtämman i Lund* (Juridiska Föreningen i Lund, 1979), 49, 50.

560 See, eg, Blekeli, *supra* n 512, 18–19; NOU 1975:10, 12; Selmer, *supra* n 512, 196. This does not mean that conceptualisations of 'personvern' along the lines of 'sphere theory' have been laid completely dead but they are rare. For one such conceptualisation, see G Apenes, 'Personvern kontra bedriftssikring – sikring av materielle verdier eller vern av personers integritet', lecture held at a conference entitled 'Sikkerhetsdagene', Trondheim, 1.11.1993 (claiming that 'personvern' involves respect for individuals' right to a personal sphere about their persons within which they reign supreme).

561 See, eg, Blekeli, *supra* n 505, 23.

562 See, eg, Blekeli, *supra* n 549, 21.

pervasive influence on development of the traditional conceptualisation of 'personvern'. This becomes clear when we examine the interests described below.

Three core interests have been linked to 'personvern'. In summary form, these interests are usually formulated in terms of 'confidentiality' ('diskresjon'), 'insight' ('innsyn') and 'completeness' ('fullstendighet'). The interest in confidentiality is described in terms of a person's desire to restrict the flow of data about him-/herself to other persons or organisations. This interest pertains both to the situation in which the data flows directly from the data subject to another person/organisation and to the situation in which the data flow onwards from that person/organisation to third parties. The interest in insight – also sometimes expressed as an interest in awareness ('opplysthet') – is said to concern a person's desire to know who processes data about him-/herself, what data are processed and the purpose(s) for the processing. As for completeness, this denotes an interest in ensuring that personal information is complete, correct, relevant and not misleading in relation to the purpose(s) for which it is processed.[563]

The link between 'personvern' and decision-making processes is drawn most clearly in the work of Blekeli. For Blekeli, 'personvern' and 'privacy' involve securing for a person a 'relevant information basis' for the taking of decisions that make use of information about that person.[564] He describes the interests in confidentiality, completeness and insight largely in terms of this concern for relevance. He emphasises that upholding the interest in confidentiality helps to prevent personal information being applied to specific decision types for which the information is irrelevant. Completeness is described as an interest that 'no information element that [the data subject] ... considers to be relevant to the decision basis should be omitted and that the relevant elements should be correct, up to date and sufficiently precise'. Similarly, the interest in insight is viewed in terms of the ability of the data subject to control the relevance of 'decision bases'.[565]

The last interest, that of insight, is often linked to data subjects' interest in 'participation' ('deltagelse') and 'influence' ('medvirkning' and/or 'innflytelse') in relation to decision-making processes based on data about them. In some analyses, the latter interest appears to be regarded as part-and-parcel of the interest in insight;[566] in others, the interest in participation and influence is viewed as the core basis of 'personvern'.[567]

---

563 Fuller descriptions of these three interests, along with the other interests commonly linked to the notion of 'personvern' (see below), can be found in KS Selmer, 'Innledning', in E Djønne, T Grønn & T Hafli, *Personregisterloven med kommentarer* (Oslo: TANO, 1987), 9, 13–15; Bing, *supra* n 349, 42–63; DW Schartum, *Rettssikkerhet og systemutvikling i offentlig forvaltning* (Oslo: Universitetsforlaget, 1993), 51–71; and NOU 1997:19, 24–26.

564 Blekeli, *supra* n 505, 26–27.

565 *Ibid.*

566 See, eg, KS Selmer, 'Det stramme samfunn', in RD Blekeli & KS Selmer (eds), *Data og personvern* (Universitetsforlaget, 1977), 27, 32.

567 See,eg, Bing, *supra* n 559, 61.

The above interests have figured prominently in Norwegian theory on 'personvern' right from the time when the latter concept began to be used. They have been subsequently supplemented by four other interest types. One of these is the interest in 'protection from unreasonable disturbance of private life' ('vern mot utidig innblanding i privatlivet').[568] This interest concerns the desire to preserve the peace of one's private life from being disturbed by the intrusive activities of others.

The other three interests, compared with those described above, are said to relate not so directly to persons as individuals but to have a more collective, societal relevance.[569] They are commonly described in terms of 'citizen-friendly administration' ('borgervennlig forvaltning'), 'protection against misuse of power and excessive control' ('vern mot maktmisbruk og overdreven kontroll') and 'robust society' ('robust samfunn').

The interest in citizen-friendly administration denotes a desire that citizens be served cordially, efficiently and correctly by the organisations with which they deal. This implies that communication between organisations and citizens be open and informative, and that organisations preserve their 'human face'.[570] In terms of organisational decision making, the interest is also said to involve ensuring that decisions are properly reasoned, reached without undue delay and in accordance with applicable law.[571]

The interest in protection against misuse of power and excessive control is said to embrace the so-called 'legality principle' ('legalitetsprinsipp') in Norwegian law.[572] It is also said to embrace the desire to avoid a surveillance level in society which renders citizens so transparent that they are stripped of any real ability to play different roles in different contexts.[573] Moreover, the interest denotes a concern that the development and organisation of a country's information systems take due account of the possibility of the systems being utilised for totalitarian ends in the event, say, of foreign occupation.[574]

As for the interest in robust society, this relates to the issue of 'vulnerability'; ie, the growing dependence of modern society on information technology to execute administrative, political and economic tasks, and the resultant social crisis that could occur were this technology to malfunction. A robust society is said to be a society in

---

568 Selmer, *supra* n 563, 14.

569 See, eg, Bing, *supra* n 349, 42.

570 See, eg, Selmer, *supra* n 563, 14–15.

571 See, eg, Selmer, *supra* n 566, 35. Selmer is alone in reading the latter requirement of legality into the interest in citizen-friendly administration. In some subsequent descriptions of the interest, he omits the requirement.

572 See, eg, Selmer, *supra* n 563, 15. Put somewhat simplistically, the legality principle requires that clear legal authority exists for State measures infringing upon citizens' autonomy, privacy and/or integrity. For an instructive overview of various formulations of the principle, see I Hjort Kraby, 'Hva er lov? – særlig om legalitetsprinsippet og faktiske handlinger' (1996) *Jussens Venner*, 145–160.

573 Selmer *id*.

574 See, eg, Selmer, *supra* n 399, 44 & 48.

which such vulnerability is minimised; in other words, it is a society in which information and information systems are protected from damage caused by accident or intentional interference.[575]

The interest catalogue set out above is not the only interest catalogue to have been advanced in relation to 'personvern' as concept and concern.[576] Yet it has been the most influential in setting the agenda for Norwegian data protection law. It has also functioned with a fair amount of success as the main heuristic aid in explaining the nebulous notion of 'personvern' to newcomers to the field of data protection. A measure of this success is its increasing use by jurists in other Nordic countries.[577]

The development of the interest catalogue is largely an attempt to make 'personvern' operational. More specifically, it is an attempt to generate tangible points of reference to guide the drafting and implementation of data protection law. As such, the interest catalogue plays an important role in explaining the rationale for, and practice of, the old *Personal Data Registers Act* and the new *Personal Data Act*.[578] Additionally, the catalogue has acquired a legal basis in the sense that all of the above interests are more or less embodied in the provisions of each Act, their *travaux préparatoires* or the practice of the Data Inspectorate.[579] Indeed, the catalogue sets out the scope for what the Inspectorate may base its decisions upon when exercising its discretionary powers, though the Inspectorate is not thereby prevented from expanding upon the catalogue through its uncontested exercise of these powers.[580] In this regard, it is apposite to regard the catalogue as functioning as a set of guiding standards ('retningslinjer') in Sundby and Eckhoff's sense of the

---

575 See, eg, Bing, *supra* n 349, 59–60.

576 Other notable interest catalogues are found in Samuelsen, *supra* n 335, 23–27; *Forskningsetikk og personopplysninger* (Oslo: Norges almennvitenskapelige forskningsråd, 1979), 13–14; NOU 1993:22, 43–44; LA Bygrave & JP Berg, 'Reflections on the Rationale for Data Protection Laws', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 3, espec 16–26. Common for these alternative catalogues, compared with the traditional catalogue, is that they give more prominence to the interest in integrity and concomitantly focus more explicitly on the psychological effects of certain data-processing activities on data subjects. Nevertheless, a great deal of overlap exists between all of them.

577 See, eg, A von Koskull, 'Personvärn och personalrekrytering, eller transformation och skygglappar' (1996) *Tidsskrift utgiven av Juridiska Föreningen i Finland*, no 6, 391–433; Blume, *Databeskyttelsesret*, *supra* n 93, 26ff.

578 KS Selmer, 'Datatilsynets kontroll med forvaltningen', in A Bratholm, T Opsahl & M Aarbakke (eds), *Samfunn, Rett, Rettferdighet: Festskrift til Torstein Eckhoffs 70-årsdag* (Oslo: TANO, 1986), 586, 593. As already intimated, the interest catalogue is also used by the Data Inspectorate to explain what it means by 'personvern' and to explain the basis for its decision making: see, eg, St meld 15 (1996–97), *Datatilsynets årsmelding for 1995*, 8.

579 See, eg, Selmer, *supra* n 578, 593–598 (detailing the way in which central elements of the interest catalogue manifest themselves in the PDRA's provisions and *travaux préparatoires*).

580 See, eg, KS Selmer, 'Borgenes vakthund – Forvaltningens vokter', in G Hansen, E Erichsen, H Sørebø, T Hafli & E Djønne (eds), *Mennesket i sentrum: Festskrift til Helge Seips 70-årsdag* (Oslo: TANO, 1989), 145, 153. Of course, the legitimacy of this expansion is conditional upon the Inspectorate not going beyond the limits of its competence as fixed by Parliament.

term.[581] In other words, the catalogue indicates which factors should be taken into account when weighing up the pros and cons of a particular phenomenon that falls to be regulated pursuant to Norwegian data protection law, without necessarily determining the outcome of the balancing process.

The explication of 'personvern' in terms of the above catalogue of interests has not been without criticism. This criticism has manifested itself largely in the 1990s. The substance of the criticism is that the interest catalogue is not sufficiently comprehensive, in part because of its focus on administrative decision-making processes,[582] and in part because of its failure to indicate the relative weight of the interests concerned *vis-à-vis* each other and opposing interests.[583] Some of the labels used to identify the interests concerned have also been criticised.[584]

While much of this criticism is valid, the catalogue of interests set out above has not been intended to constitute an exhaustive definition of the 'personvern' concept.[585] Its exponents recognised early on that the catalogue could be developed further. Decision-making processes have simply constituted a point of departure for development of the catalogue, not necessarily the end-point for this development. The initial focus on such processes is justified to some extent by the fact that data protection needs are most acute in these contexts. Further, many of the interests – particularly the interests in completeness and insight – have little *practical* meaning except in relation to the actual uses to which personal data are put.[586] One can also protest that it is too much to ask that the interest catalogue indicate the relative weight of the interests concerned, as such weighting is largely context-dependant. Given the multiplicity of contexts for the processing of personal data, to present in the abstract an accurate description of the interests' relative weight is scarcely possible without making the presentation excessively complex and casuistic.

This said, the interest catalogue still needs to be refined and expanded if it is to provide a fully accurate conceptualisation of the rationale for data protection laws from the perspective of data subjects. In light of this need, an alternative interest catalogue is elaborated below. This catalogue builds upon and overlaps considerably with the traditional catalogue. The differences between the two reflect variations in emphasis rather than a clash of paradigms.

---

581 See the references cited *supra* n 35.

582 See, eg, NOU 1993:22, 43 & 236; St meld 33 (1994–95), *Personvern og telekommunikasjon*, 5. See also KJ Ims, *Informasjonsetikk i praksis. Datasikkerhet og personvern* (TANO, 1992), 75 (commenting that fear of information use is just as important in relation to 'personvern' as the actual use of information).

583 See, eg, Bygrave & Berg, *supra* n 576, 38; Rasmussen, *supra* n 467, 56.

584 See, eg, J Hansen, *SAFE P: Sikring av foretak, edb-anlegg og personverninteresser etter personregisterloven*, CompLex 12/88 (Oslo: TANO, 1988), 20 (commenting that the term 'completeness' ('fullstendighet') is too narrow in ambit to adequately describe the interest(s) in information quality which data protection should embrace).

585 See, eg, Blekeli, *supra* n 549, 29–30.

586 Schartum, *supra* n 563, 60.

7.2.5 A RE-ELABORATION OF DATA PROTECTION INTERESTS

Introductory remarks

Like the traditional catalogue, the set of interests presented in this section is intended both to delineate the concerns of data protection generally and the concerns of data protection as a legislative phenomenon, primarily in relation to data subjects. Concomitantly, this set of interests is not intended solely to depict the agenda of data protection laws as they currently stand but also to depict some of the potential agenda of future data protection laws. Ultimately, of course, this set of interests depicts the concerns of human beings – a point elaborated upon further below.

Again, like the traditional catalogue, this set of interests is not intended to determine the outcome of the myriad conflicts thrown up by the existence and implementation of data protection laws; it simply aids in identifying and clarifying the interests at stake. In other words, it helps to structure interest-balancing processes pursuant to these laws, but does not directly determine the outcome of such processes.

Along with the traditional catalogue, this set of interests also plays a pedagogical/heuristic role in explaining the ambit of data protection concerns to newcomers to the field. Closely linked to this pedagogical role is the catalogue's legal-political function: the catalogue can be used as a standpoint from which to compare how various data protection laws safeguard the interests concerned, and it can buttress attempts to extend the scope and stringency of these laws.

Very few of the interests set out below are *uniquely* the concerns of law and policy on data protection. Indeed, some of the interests are promoted to a far greater extent through other types of instruments than data protection laws. It could be argued, accordingly, that terming such interests 'data protection interests' is misconceived. However, this argument misconceives what is meant here by 'data protection interests': the latter term is not intended to be proprietary in the sense that those interests embraced by it are to be regarded as exclusively the concerns of law and policy on data protection. An interest can be categorised as a 'data protection interest' and still be capable of categorisation under another field of law and policy.

The catalogue is divided into two groups of interests. The first of these groups (hereinafter termed group 1) contains interests that relate to the quality of personal data, information and information systems. The second group (group 2) comprises interests concerned with the condition of persons as data subjects and with the quality of society generally.

For the most part, the interest catalogue pertains to data that are personal (ie, capable of being linked to specific persons). However, some interests pertain also to situations in which non-personal data are processed. In those situations involving personal data, it is assumed (as in the catalogues above and data protection laws generally) that the data do not necessarily relate to especially intimate or sensitive aspects of the data subjects' lives.

Although the interest catalogue is presented here primarily from the perspective of individual persons in the role of data subjects, it should be kept in mind that the catalogue is also capable of applying to collective entities in the same role. This capability is explored further in Part III.

In the following, a brief description of each interest is first provided. Thereafter the manifestation(s) of the interest in data protection laws is briefly described.

Group 1 interests

These interests concern the quality of personal information and information systems. They fall, to some extent, under the rubric of 'completeness' in the traditional interest catalogue. The term 'completeness', however, is too narrow to capture the full breadth of either the interest(s) to which it is supposed to refer or the interests described immediately below. There are three main sets of group 1 interests: one set relates directly to the content of personal data; another relates to the uses to which personal data are put; the third set concerns the quality of the information systems that process the data. Each of these interest sets is, in practice, related to, and affected by, the other two sets.

With regard to the set of interests directly concerning data content, the overarching interest here is the interest in *validity* of personal data. Validity is a measure of the extent to which personal data correspond with the attributes of persons which the data are supposed to represent. For the sake of brevity and convenience, these attributes are termed Real World Objects (RWO). When persons are said to have an interest in the validity of data, they are said to be desirous of the data corresponding with the appropriate RWO as closely as possible. The interest in validity is composed of several sub-interests:

1) the *precision* of data (ie, the level of detail at which the data describe or define the RWO);
2) the *comprehensiveness* of data (ie, the extent to which all data that are necessary to represent the RWO are present); and
3) the *correctness* of data (ie, the degree to which the correspondence between the data and the RWO is error-free).

An important aspect of the second dimension (comprehensiveness) is the *identifiability* of the data (ie, the extent to which the data are able to be connected to the RWO that they are supposed to represent). An important aspect of the third dimension (correctness) is the *currency*, *actuality* or *up-to-dateness* of the data (ie, the age of the data measured in terms of the time difference between when the data are used for a given purpose and when the data first were collected and stored).

The second main set of group 1 interests relates to the uses to which personal data are put. The overarching interest here is the interest in *utility* of personal information. Utility is a measure of the correspondence between information and the purpose(s) for which the information is processed (ie, collected, registered, stored, used and/or disseminated). The interest in utility is composed of two main sub-

interests: the *relevance* and *completeness* of information. The notion of completeness is easy to define; it simply refers to the extent to which all relevant information is present in relation to a particular application. The notion of relevance, however, is difficult to describe in the abstract and without resorting to circular definitions that refer to concepts (such as pertinence, suitability or conformity) that are equally hard to define. It is often, though not always, possible to measure the *hypothetical* degree to which a given set of information is relevant to a given application, in terms of the extent to which the outcome of the application would differ according to whether or not the information is taken into account. Nevertheless, this does not explain how relevance is determined.

There are two classes of factors determining relevance: (i) those that could be loosely called 'logical', and (ii) those that could be loosely termed 'legal/moral'. Of the former, the primary factor concerns the tightness of the logical/semantic link between the information and the use (potential or actual) of the information. Another logical factor is the weight carried by the information because of its perceived credibility and reliability – though this factor can also be partly a function of legal/moral factors. The latter class of factors is constituted by rules (legal and/or moral) that allow only certain types of information to be taken into account for certain purposes. Often the two classes of factors will be in harmony with each other, but this will not always be the case. Thus, the two classes of factors can give rise to two kinds of relevance – logical and legal/moral – which are not co-extensive.

The third set of group 1 interests relate first and foremost to the quality of information systems. The overarching interests in this respect can be summed up in terms of the *manageability*, *robustness*, *accessibility*, *reliability* and *comprehensibility* of information systems.

The manageability of an information system (IS) refers to the degree to which the IS – and interactions between the IS and other systems – can be steered, administered and maintained in a desired manner. It also refers to the extent to which the IS operates on the basis of a clear allocation of responsibilities for defining, registering, storing, rectifying and disseminating the data handled by it.

The robustness of an IS refers to the degree to which the system is (in)vulnerable to extraneous interference. This interest is roughly similar to what is denoted in the traditional catalogue by the interest in a 'robust society'.

The interest in accessibility of an IS relates to the extent to which an IS allows data to be located and retrieved. The interest covers both the practical/physical ease with which data can be located and retrieved, and the time it takes to locate and retrieve the data.

The reliability of an IS relates to the extent to which the system functions in accordance with the expectations of those who use it and those who are affected by it. This interest also embraces the degree to which the system takes account of the levels of random error and bias ('systematic' error) with which it operates.

The comprehensibility of an IS relates to the degree to which the system hinders or promotes understanding of the way in which it functions. By 'understanding' is meant not just the understanding of the persons or organisations which are responsible for operating the system, but also the understanding of persons or organisations which are affected by the system (eg, as data subjects). Furthermore, the interest in comprehensibility embraces the capacity of the IS to promote or hinder understanding of the data it handles, including how easily the system permits discovery of faults with these data.

These five IS interests should not be understood as rigid categories nor as being entirely separate of each other. For example, considerable overlap occurs between the robustness and reliability of an IS, and between its manageability and comprehensibility.

There also exist a range of miscellaneous interests which are embraced by various of the five IS interests but which are not made adequately explicit in the above presentation. One such interest concerns the *integrity* of data (ie, the extent to which the data remain free from unauthorised alteration or destruction whilst being processed). This interest falls mainly under the interests in IS robustness and reliability.

Another such interest concerns the *interpretability* of data (ie, the extent to which the data can be usefully understood). An essential component of interpretability is, of course, the *presentation* and *form* of the data (ie, the way in which data appear). The interest in interpretability falls mainly under the interest in IS comprehensibility.

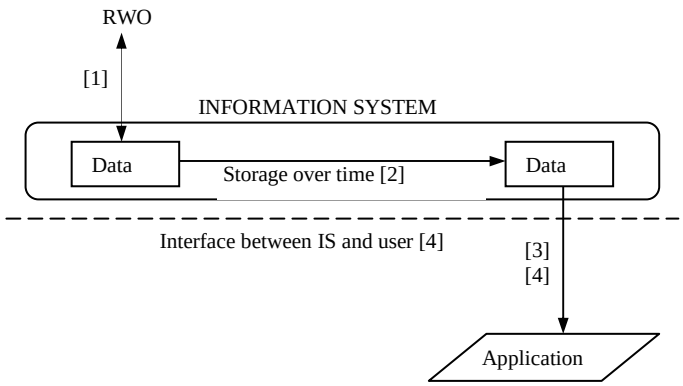
A third such interest relates to the *predictability* of the means and outcome of data-processing operations from the perspective of the data subject. This interest can be read into the interest in IS reliability. However, its realisation also depends on realisation of most of the other group 1 interests, along with some of the interests in group 2 – particularly the interest in insight.

Yet another interest relates to *registration quality* (ie, the way in which data are registered in a given IS). Essential components of registration quality are:

1) *registration completeness* (ie, the extent to which each RWO that is supposed to be registered in a given IS, actually is registered in that system);
2) conversely, *registration correctness* (ie, the degree to which entities that are *not* supposed to be registered in the IS are not in fact registered, and the degree of mistaken double or multiple registration of an RWO in a given IS).

The interest in registration quality embraces the interest in data interpretability at the same time as it falls under the interests in IS comprehensibility, reliability and manageability.

To sum up, all of the above quality elements can be placed diagramatically as follows:



Key
[1] Validity (of data)
- precision
- comprehensiveness (including identifiability)
- correctness (including currency/up-to-dateness)

[2] Integrity (of data); robustness and reliability (of IS)
[3] Utility (of information)
- relevance
- completeness

[4] Manageability (of IS)
- registration quality

[4] Robustness (of IS)
[4] Accessibility (of IS)
[4] Reliability (of IS)
- predictability
- registration quality

[4] Comprehensibility (of IS)
- interpretability
- registration quality

Realisation of each of the sets of group 1 interests defined above is always affected by the understanding, motivations and worldview of the data controller/processor/user. All information is created and processed on the basis of certain perceptions. Such perceptions help determine how a particular problem or task is understood, and, accordingly, which information is deemed relevant and necessary for tackling it. Concomitantly, poor understanding of a problem/task (ie, poor cognitive quality) will tend to result in poor interpretation, organisation and/or application of the information that is processed to address the problem/task. Thus, we can read into each of the three sets of interests described above an interest in *adequate cognitive quality*; ie, a concern to ensure that data controllers/processors/users properly comprehend (i) the nature of the problems/tasks for which they

process information, and (ii) the quality (relevance, validity, etc) of the information they process to address those problems/tasks.

Legal manifestation of group 1 interests

The clearest embodiment of the interest in validity is in provisions such as Art 5(d) of the CoE Convention and Art 6(1)(d) of the EC Directive which state that personal data 'shall be accurate and, where necessary, kept up to date'. Broadly similar provisions are found in all data protection laws. However, the laws tend to: (i) eschew use of the term 'validity' for a variety of other terms; (ii) make explicit mention of some of the sub-interests of validity (eg, up-to-dateness) but not all of the sub-interests; and (iii) differ according to the stringency with which they require checks on data validity.[587] Legal manifestation of the interest in validity occurs also in provisions giving data subjects rectification rights with respect to incorrect, misleading or obsolescent data. By implication, the interest in validity is also manifest in provisions creating access rights for data subjects or notification duties for data controllers. The latter duties not only serve the interest in validity by alerting data subjects to the existence of data-processing practices which they (the data subjects) might want to monitor; in situations where the data are supplied by the data subjects (eg, in response to a questionnaire), notification duties can also help foster a climate of trust which can increase the probability of the data subjects supplying valid data. Such a climate of trust can also be fostered by data controllers publicising the fact that they handle data in conformity with basic data protection principles.

The clearest legal manifestation of the interest in utility is in provisions, such as Art 6(1)(c) of the EC Directive, stating that personal data 'shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. The interest is also embodied, though a little less directly, in provisions setting out the principles of purpose specification and minimality. Legal manifestation of the interest in completeness occurs also, albeit indirectly, in provisions like Art 15(1) of the EC Directive which regulate the use of fully automated decision-making processes.[588]

There is little direct legal manifestation of the five interests relating expressly to the quality of information systems. This is because data protection laws tend expressly to address various stages in the processing of personal data rather than the operation of the information systems for such processing, Nevertheless, the interest in IS manageability lies implicit in *all* of the provisions setting out data subjects' rights and data controllers' corresponding duties. The interest is also expressly manifest in provisions like Art 17(2) and 17(3) of the EC Directive which expressly require a data controller to ensure by way of contract or some other legal act that data processors engaged by the controller provide 'sufficient guarantees' of technical and organisational security with respect to the processing. The interests in IS robustness

587 These three points are discussed in more detail in Chapter 18 (section 18.4.4).

588 See further Chapter 18 (section 18.3.1).

and reliability, together with the concomitant interest in data integrity, lie implicit in provisions concerned with data security and data validity. The interests in IS accessibility and comprehensibility, along with the concomitant interests in data interpretability and registration quality, can be read into provisions on access rights for data subjects and notification duties for data controllers. Concern for registration quality also lies implicit in the provisions on data validity. As for the interest in predictability, this can be discerned in provisions embodying the purpose specification principle as well as in provisions on data subjects' access rights and data controllers' notification duties.

Finally, there is little direct legal manifestation of the interest in adequate cognitive quality. However, the interest lies implicit in many of the provisions that help to secure the interest in utility. Through use of criteria such as 'relevance' and 'compatibility', these provisions require data controllers to reflect over the nature of the data being processed, the nature of the purposes for which processing takes place, and the nature of the relationship between the data and the processing purposes.

Group 2 interests

This group of interests are primarily concerned with the condition of persons as data subjects and secondarily with the condition of society generally. Seven basic interests make up this group: *privacy*, *autonomy*, *civility*, *pluralism*, *democracy*, *rule of law* and *balanced control*. The divisions between them should not be seen as hard and fast; they overlap considerably with each other. Moreover, realisation of the one interest will be partly a function of realisation of one or more of the other interests. Further, each of them are ultimately grounded in concern for human dignity.

A person's interest in privacy is his/her interest in being inaccessible to other persons and organisations. This interest is composed of two main sub-interests:

1) *non-transparency* (ie, a person's interest in avoiding being rendered transparent *vis-à-vis* other persons and organisations);
2) *non-interference* (ie, a person's interest in being left alone, physically and/or psychologically).

Part of the interest in non-transparency is the interest in *anonymity* (ie, a person's interest in being able to act without being identified). Part of the interest in non-interference is the interest in *non-information* (ie, a person's interest in not being given information by other persons or organisations).

A person's interest in autonomy encompasses his/her interest in *informational self-determination*; ie, the interest of a person in freely determining how data on him-/herself are processed by others. A 'weaker' version of the interest is an interest in *informational co-determination*; ie, the interest of a person in having some, though not the final, say in how data on him-/herself are processed by others.

The interests in informational self-determination and co-determination include the following sub-interests:

1) *insight* (ie, a person's interest in knowing who processes data about him-/herself, what data are processed, the purpose(s) of the processing, etc);
2) *outflow control* (ie, a person's interest in determining the flow of information from him-/herself to others);
3) *inflow control* (ie, a person's interest in determining the flow of information from others to her-/himself).

Closely related to the interest in insight are the interests in accessibility and comprehensibility of information systems. The latter two interests are described above in the category of group 1 interests.

Closely related to both the interests in outflow and inflow control is the interest in *identificational self-determination* (ie, a person's interest in being able to determine and protect his/her identity in relation to both him-/herself and others).[589]

Part of the interest in inflow control, and closely related to the interest in non-information, is the interest in *attentional self-determination* (ie, a person's interest in being able to give his/her attention to what he/she wants).[590] In contrast to the interest in identificational self-determination, which is mainly actualised when incoming (and outgoing) information relates to the person concerned, the interest in attentional self-determination, along with the interest in non-information, can also be relevant when incoming information relates solely to other persons or is non-personal.

While the above group 2 interests primarily concern various forms of information processing at the level of the individual data subject, the interests described below tend to lie on a different plane; they primarily concern relatively abstract, society-wide goals. The first of these interests, civility, denotes a desire to establish attitudes of mutual respect between persons, at both individual and collective levels, and in both private and public sectors. The interest encompasses the interest in citizen-friendly administration listed in the traditional catalogue, though it is broader as it pertains to more relationships than just those between individual persons and the organisations with which they deal.

The interest in pluralism denotes a concern, firstly, to secure a diversity of opinions and lifestyles, and, secondly, to ensure that social, economic and/or political power is spread across a broad range of groups and organisations so that not one single such group/organisation is able to dominate the others. In other words, the interest denotes a concern to avoid both conformist and totalitarian tendencies. As such, the interest in pluralism has much the same content as the interest in protection against misuse of power and excessive control listed in the traditional catalogue.

---

589 This interest encompasses the interest in protecting self-conception as defined by Samuelsen, *supra* n 335, 23ff. Cf Harris *et al* who term this interest as one of 'self-identification': DJ Harris, M O'Boyle & C Warbrick, *Law of the European Convention on Human Rights* (London/Dublin/Edinburgh: Butterworths, 1995), 307.

590 This interest is the same as what Stanley Benn refers to as 'privacies of attention'; ie, 'the ability to exclude intrusions that force one to direct attention to themselves rather than to matters of one's own choosing'. See SI Benn, 'The Protection and Limitation of Privacy' (1978) 52 *Australian LJ*, 601, 608; SI Benn, *A Theory of Freedom* (Cambridge: Cambridge University Press, 1988), 288.

As for the interest in democracy, this denotes an interest in ensuring that all citizens actively participate in the public government of societal processes. The notion of 'democracy' here encompasses not just participation through formal parliamentary elections but participation through all kinds of actions – both formal and informal – that are public in the sense that they are aimed at attracting the attention of and influencing persons outside the citizen's domestic/family sphere. The interest in democracy does not figure explicitly in the traditional catalogue, though it arguably lies implicit in the interest in protection against misuse of power and excessive control.

The interest in rule of law denotes here a concern to subject certain activities (in the instant case, data processing) to legal controls so as to secure accountability, foreseeability and proportionality in the execution and outcome of those activities. It also denotes a concern not just to ensure that the activities are carried out within the boundaries set by law but that they are actively regulated by legal measures. Moreover, it denotes a concern to ensure that these measures are themselves of a certain quality; ie, that they are sufficiently accessible and precise to allow data controllers and data subjects to foresee their consequences. In the context of the traditional catalogue, the interest in rule of law embraces aspects of the interest in citizen-friendly administration and the interest in protection against misuse of power and excessive control. One group of experts on data protection implicitly recognises the close connection between the interest in rule of law and the interest in pluralism, by noting that data protection involves 'the creation of rules of law for information collection and use, so that the activities of the centers of power in a society are controlled by law'.[591] However, the interest in rule of law is also closely linked to, and overlaps with, the other group 2 interests, particularly the interest in balanced control.

The latter interest is extracted from the work of Dag Wiese Schartum,[592] who argues that control measures (in the sense of measures to monitor the extent to which legal rules are properly applied)[593] ought not to be one-sidedly focused on curbing, say, criminal acts of citizens, but to focus on a range of other concerns as well. Schartum lists five 'dichotomies' in terms of control efforts: (1) effort spent on controlling citizens as opposed to effort spent on providing citizens with guidance; (2) effort spent on carrying out advance (*ex ante*) control as opposed to effort spent on retrospective (*ex post facto*) control; (3) effort spent on control operating in disfavour of citizens (eg, taking away benefits from citizens who are not entitled to

591 See the Final Report of the Bellagio Conference on Current and Future Problems of Data Protection (held in Bellagio, April 1984), set out in DH Flaherty, 'Nineteen Eighty-Four and After' (1984) 1 *Government Information Quarterly*, 431, 434.

592 See DW Schartum, 'Proportional Control?' (1997) 11 *Int Rev of Law Computers & Technology*, 107–116; DW Schartum, 'Den kontrollerende forvaltning' (1997) 20 *Retfærd*, no 77, 51–66.

593 Schartum employs this notion of control primarily in relation to measures for monitoring the legality of the actions of public authorities when the latter determine individual cases.

them) in contrast to effort spent on control operating in favour of citizens (eg, identifying under-use of welfare services); (4) effort spent on control directed towards the operations of the controlling body (internal control) as opposed to control efforts directed at the operations of others (external control); (5) effort spent on controlling computerised operations in contrast to effort spent on controlling non-automated/manual operations. In each of these five cases, Schartum proposes that there should be some 'proportionality' of efforts in the sense that the one effort should not be given priority at the complete expense of the other effort. These five axes of proportionality make up (and form sub-interests of) the interest in balanced control. The notion of control is used here in much the same sense as Schartum uses it. However, it should be emphasised that control covers measures for monitoring not just the case-handling procedures of public authorities but also the equivalent procedures of private organisations. Additionally, it bears emphasising that both sets of measures tend to involve the monitoring, in turn, of the activities of private citizens. The interest in balanced control does not figure explicitly in the traditional interest catalogue though aspects of it arguably lie implicit in the interest in citizen-friendly administration and the interest in protection against excessive control. The interest is closely related to the interest in rule of law; indeed, it can be seen as an outgrowth of the criterion of proportionality embraced by the latter interest.

Legal manifestation of group 2 interests

The interests in non-transparency and non-interference are most directly manifest in provisions setting out the principles of fair and lawful processing, purpose specification, minimality, disclosure limitation and information security. Implementation of these provisions places restrictions on the ability of people and organisations to gain access to information on others. It can also decrease the chance of persons being asked to supply information on themselves and thereby decrease the extent to which they suffer interference or attention from information gatherers. The same can be said for provisions requiring data controllers to take measures to safeguard or improve information quality. Implementation of such provisions lessens the risk of a data controller making a decision concerning a person on the basis of inaccurate and/or irrelevant information. This lessens in turn the risk of a data controller then taking, say, unwarranted investigative action which interferes with or disturbs that person.

Express concern in data protection laws for the interest in anonymity tends to be muted. While most data protection laws provide for the anonymisation of personal data once the need for person-identification lapses, they do not contain rules stipulating that active consideration be given to crafting technical solutions for ensuring transactional anonymity. The closest they come to such a stipulation is in rules embodying the minimality principle, particularly those providing that personal data must not be 'excessive' in relation to the purposes for which they are processed. At the same time, though, data protection discourse is increasingly showing express

concern for the interest in anonymity. Numerous policy documents issued in recent years, together with several pieces of legislation, specifically provide for securing the interest.[594]

As for legal manifestation of the interest in informational self-determination, this is most obvious in those provisions of data protection laws which prohibit the processing of personal data without the consent of the data subject, or which give the latter a right to object to processing. The interest is also clearly manifest in rules providing data subjects with access and rectification rights. An indirect manifestation of the interest is found in those provisions setting out the principles of purpose specification and fair and lawful processing, together with rules on notification duties. The connection is indirect because implementation of these principles cannot be seen as a direct exercise of information control on the part of data subjects; primary responsibility for implementing the principles is given to data controllers. Nevertheless, implementing the principles will help to increase the possibility for persons to determine what information is collected on them and how that information shall be used.

The above provisions typically refrain from giving data subjects an absolute right to dispense with data on themselves as they see fit. For example, the requirement of data subject consent is usually laid down as just one of several alternative prerequisites for data processing. Thus, the above provisions are better viewed as manifestations of an interest in informational co-determination as opposed to self-determination.

Regarding legal manifestation of the interest in insight, this comes through strongly in provisions on data subjects' access rights and data controllers' notification duties. The same applies for the interests in accessibility and comprehensibility of information systems.

Legal manifestation of the interest in outflow control is most prominent in provisions dealing directly with disclosure limitation. Slightly more indirect manifestation of the interest is found in rules requiring the consent of data subjects to data processing and provisions for rectification and erasure rights.

The latter provisions embody also a direct concern for securing the interest in identificational self-/co-determination. Further manifestation of this interest is arguably found in provisions such as Art 13(1)(g) of the EC Directive which permits restrictions on access rights insofar as is necessary for 'the protection of the data subject'. Moreover, several of the policies of data protection authorities appear to have put weight on the interest when restricting, for example, the manner in which researchers can make contact with potential respondents to research surveys.[595] At

---

594 See further Chapter 18 (section 18.4.3).

595 With respect to practice of the Norwegian Data Inspectorate and Ministry of Justice, see, eg, cases 86/372 & 87/792 presented in Bygrave, *supra* n 37, 86–90. In these cases, the Inspectorate and Ministry set limits on both the number and form of attempts by researchers to contact certain groups of potential survey respondents – in the one case, former patients of a psychiatric clinic; in the other

the same time, there appears to be a paucity of provisions in data protection laws which expressly set out a right 'not to know' certain types of information. However, principles 5.6 and 8.2 of CoE Recommendation No R (97) 5 on the Protection of Medical Data (adopted 13.2.1997) open up for the development of such a right in relation to medical (including genetic) data generally.[596] Potential for developing such a right would seem also to be contained in Art 13(1)(g) of the EC Directive (mentioned above).

Many of the provisions and policies mentioned in the immediately preceding paragraph also show a concern for securing the interests in inflow control, non-information and attentional self-determination. Manifestation of these interests is found as well in rules providing data subjects with a right to object to certain types of data processing, especially those involving direct marketing.[597]

Concern for the interest in civility is especially apparent in those provisions of data protection laws which embrace the principles of fair and lawful processing and purpose specification. It is further apparent in provisions setting out access rights for data subjects and corresponding notification duties for data controllers. And it is apparent in provisions that give data subjects a right to object to fully automated decision making and to direct marketing.

There is a relatively small number of provisions in which the interest in pluralism is obviously discernible. The interest is clearly manifested in those few German data protection laws that are expressly concerned with ensuring 'informational equilibrium' between legislative and executive organs of government.[598] More indirect manifestation of the interest is found in those few laws with provisions aimed at preventing the creation of information systems that can easily be turned to serve dictatorial interests in the event of foreign invasion or war.[599] The interest also emerges in some of the policies adopted by data protection

---

(Cont.)
case, former clients of child-welfare agencies. With respect to the latter group, for example, the Inspectorate held that revisitation of their past lives could have disturbing psychological consequences for their ability to start afresh.

596 A right not to be informed of information collected about one's health is also set down in Art 10(2) of the CoE's 1997 *Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine* (ETS No 164); in force 1.12.1999. Some countries have biotechnology legislation providing, in effect, this sort of right with respect to the results of genetic testing: see, eg, ss 6-4 & 6-7 of Norway's *Medical Use of Biotechnology Act* (*Lov om medisinsk bruk av bioteknologi av 5 august 1994 nr 56*).

597 See espec Art 14(b) of the EC Directive, set out in Chapter 18 (section 18.4.5). Note also Art 12(1) of the EC Directive on telecommunications privacy which states that 'use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent'. Article 13(1) of the upcoming Directive on privacy of electronic communications is in similar terms. See further *infra* n 782 and accompanying text.

598 See Chapter 2 (section 2.3).

599 See Chapter 3 (section 3.8).

authorities, particularly those setting limits on the processing of large amounts of data relating to large numbers of persons.[600] At the same time, though, the interest underlies the basic thrust of data protection laws – as intimated in the Final Report of the Bellagio Conference.[601]

The interest in democracy also underlies the general thrust of all data protection laws, in that the latter help to secure confidence on the part of citizens that their participation in public affairs will not result in personal risks arising out of the registration of their activities. We find more direct manifestations of the democracy interest in those provisions creating access rights for data subjects and notification duties for data controllers. As Simitis points out, the democracy interest also figures centrally in those (few) laws that attempt specifically to secure 'informational equilibrium' between the legislature and executive.[602]

As for the interest in rule of law, the entire body of data protection laws may be viewed as an embodiment of this interest by the very fact that they subject certain forms of data processing to legal regulation. All of the laws' basic principles may also be viewed as embodying the interest inasmuch as they are concerned with securing accountability, foreseeability and/or proportionality in relation to data processing. We find some express recognition of these views in the data protection instruments of the CoE.[603]

The interest in balanced control is not obviously manifest in current data protection laws, though aspects of it can arguably be read into some of their provisions. For instance, provisions setting out data controllers' notification duties indirectly embody a concern to counterbalance control with guidance. Provisions concerned with ensuring information security and data validity indirectly embody a desire to counterbalance external control with internal control. Further, aspects of the interest show through in some of the policies adopted by data protection authorities,

---

600 To take one example, the policies of Australia's federal Privacy Commissioner with respect to regulating the data-matching practices of government agencies have been partly grounded on recognition of the fact that 'data-matching tends to increase the level of information surveillance of the population at large by Government bodies': Privacy Commissioner, *Regulation of Data-Matching in Commonwealth Administration – Report to the Attorney-General* (Sydney: Privacy Commissioner, September 1994), 5.

601 *Supra* n 591.

602 Simitis, *supra* n 56, para 18.

603 See the preamble to the CoE Convention ('Considering that the aim of the Council … is to achieve greater unity between its members, based in particular on respect for rule of law …'), and para 11 of the Explanatory Memorandum to *Recommendation R (91) 10 on the Communication to Third Parties of Personal Data Held by Public Bodies* (adopted 9.9.1991) ('the drafters of the recommendation are seeking to emphasise that a legal framework is essential before any communication may be effected. In so doing, they are seeking to avoid the existence of a grey zone, or a situation between law and non-law, wherein vague administrative practices or policies operate'). A clear concern for upholding the rule of law in the context of data-processing practices is also demonstrated in the case law developed pursuant to Art 8(2) of the ECHR: see further Bygrave, *supra* n 102, 270ff.

especially those dealing with data-matching practices.[604] Also noteworthy is s 35(2)(4) of the draft Bill proposed by the Skauge Committee for a new data protection law in Norway. This provided that the Data Inspectorate, when assessing the necessity of setting down conditions for the licensing of certain data-processing operations, should take into consideration the extent to which planned advisory/guidance measures exist which are reasonably proportional to control measures.[605]

Concluding commentary on the above catalogue

The above catalogue is essentially a distillation of *assumptions* about some of the concerns of persons generally. As such, the catalogue is a type of abstract profile.[606] The assumptions have a variety of origins that help to lend them objective (inter-subjective) validity: most notably, existing legal rules (particularly those in data protection laws), the results of public opinion surveys, and the interest catalogues canvassed in the previous section. Yet they unavoidably rest in part also on my own (subjective) observations of human needs and preferences.

What is perhaps most problematic with the interest catalogue is that it is *prima facie* global in application: it does not distinguish, for instance, between the interests of different national, cultural or ethnic groups. However, these problems are mitigated by the fact that the catalogue refrains from ranking the extra-legal importance of the interests in relation to each other and in relation to other interests.

The catalogue lists well over twenty interests. This is a large number of interests relative to previous catalogues. Some of these interests could be collapsed together. That this has not been done is in order to highlight the multifaceted character of data protection concerns from the viewpoint of data subjects. The complexity and length of the catalogue is a reflection of the fact that data protection concerns are themselves complex and wide-ranging.

At the same time, many, if not all, of the interests in the catalogue are also protected to varying degrees by a range of other legal rules that often antedate the emergence of data protection laws. For example, rules on negligence and judicial review of administrative decision making have long been concerned with aspects of the quality of information, though these aspects traditionally have not been expressly framed in terms of the quality concept. To take another example, the interest in

---

604 See, eg, the line taken by the Norwegian Data Inspectorate and Ministry of Justice in case 91/1563 (set out in Bygrave, *supra* n 37, 126–129). In this case, the Inspectorate and Ministry prohibited a data-matching operation that would have involved exclusively retrospective control of welfare entitlements, but allowed instead control measures that operate in advance of entitlements allocation.

605 See NOU 1997:19, 169. While such a provision ended up being omitted from the *Personal Data Act*, the provisions of the latter (espec ss 34–35) are sufficiently open-ended to permit the type of assessment proposed by the Skauge Committee. Note also Ot prp 92 (1998–99), 130 (stating that the assessment types listed by the Skauge Committee will be relevant under the Act).

606 I am indebted to Dag Wiese Schartum for this point. The concept of 'abstract profile' is explained in Chapter 17 (section 17.2).

identificational self-determination is partly upheld by long-standing rules on defamation, though, again, these rules have traditionally eschewed explicit concern for such an interest. The important point is that the interests in the catalogue tend not to be *uniquely* the concerns of data protection laws.

Undoubtedly, the interest catalogue presented above is too cumbersome to function usefully as a rhetorical device in popular political debates. However, the catalogue is by no means too cumbersome to function usefully in academic discourse about the rationale and limits of data protection concerns. Neither is it too cumbersome to function usefully as a guide for data protection authorities, legislators and other policy makers in assessing or developing law and policy on data protection.

The catalogue provides a considerably more sophisticated depiction of the interests related to information quality than is found in the catalogues presented in section 7.2.4. Particularly noteworthy in this regard is the catalogue's explicit focus on the quality of *information systems* – a focus that all too often has been absent from data protection discourse. The relatively detailed treatment of group 1 interests is called for in the face of the trend towards electronic interpenetration and of problems with the quality of information used by many organisations.[607]

The catalogue is also considerably more extensive in its coverage of group 2 interests than are the other catalogues presented in section 7.2.4. Indeed, the catalogue could be expanded even further in this regard. For instance, several of the values listed in section 7.2.2 – namely, individuality, emotional release, self-evaluation and (social) stability – could be incorporated more explicitly in group 2. That this is not done is because these values are implicit in the interest catalogue as set out above.

Not all of the interests in group 2 can properly be said to lie close to core data protection concerns as expressed in current legislation. This is especially so with the interest in balanced control. It is also somewhat the case with the interests in attentional self-determination and non-information. All of these interests are included, though, because some traces of them are discernible in current law and policy on data protection. They are also included in order to indicate avenues along which such law and policy might develop in the future – particularly given the trends identified in Chapter 6 (section 6.2).

The division of the catalogue into two groups of interests reflects the basic difference between each group. Unlike the interests in group 2, the interests in group 1 are primarily technical-organisational in orientation. They pertain first and foremost to the field of data security. This distinction, however, should not overshadow the fact that realisation of group 1 interests is, in practice, important for the realisation of many of the group 2 interests.

The interests in the catalogue will not always be in harmony with each other. For instance, attempts to further the interest in data validity by allowing organisations to

607 See Chapter 6 (section 6.2).

reference personal data with multi-context PINs can potentially weaken the interest in non-transparency insofar as the PINs enhance possibilities for linking personal data from different registers.[608] To take another example, attempts to further the interests in predictability and insight by allowing, say, providers of telecommunications services to register and store, for billing purposes, detailed information about subscribers' private telephone calls can potentially clash with the interests in autonomy and pluralism.[609] To take yet another example, the interests in non-interference (non-information) and attentional self-determination can be detrimentally affected by measures aimed at safeguarding the interest in informational self-determination (eg, when a data controller is forced to contact data subjects in order to ask for their consent to data processing).[610] The former interests can additionally be affected by measures aimed at enhancing the interest in non-transparency (eg, through making it difficult for an organisation to collect data on a person from another organisation); for if an organisation is unable to collect personal data held by another organisation, it might end up attempting to gain the data directly from the data subject.

The catalogue does not provide guidance for resolving such interest conflicts as it refrains from indicating the respective importance of each interest. This omission is

608 This clash of interests is well-illustrated in two cases handled by the Norwegian Data Inspectorate and Ministry of Justice: see cases 92/2967 & 93/1619, set out in Bygrave, *supra* n 37, 170–171. Both cases concerned applications from mobile telephone companies for permission to reference their customer data using the unique 'birth number' ('fødselsnummer') assigned every individual by the State. The companies pointed out that use of such numbers would ensure correct identification of customers, thereby reducing the possibility of fraud and cases of mistaken identity. The Inspectorate refused permission, holding that registration of the numbers was not objectively justifiable pursuant to s 6(1) of the PDRA. On appeal, the Justice Ministry upheld the Inspectorate's decision on the grounds that 'increased use of birth numbers will be perceived by many to be a violation of integrity' ('økt bruk av fødselsnummer vil for mange oppfattes som en integritetskrenkelse'). Nevertheless, the Ministry acknowledged that registration of the numbers would enhance the quality of the customer data.

609 As illustrated by case 92/2899 dealt with by the Norwegian Data Inspectorate and Ministry of Justice: set out in Bygrave, *supra* n 37, 136–140. In this case, Norway's principal telecommunications service provider sought permission to register and store more detailed data on telephone calls partly in order to give subscribers a better picture of the basis for their respective telephone bills. Permission was refused by the Inspectorate mainly for fear that the planned system would be detrimental to the interests in autonomy and pluralism. The Justice Ministry overturned the Inspectorate's decision on appeal, expressing confidence that the system would not have the effects predicted by the Inspectorate.

610 Again, this point is illustrated by a case dealt with by the Norwegian Data Inspectorate and Ministry of Justice: see case 94/2686, set out in Bygrave, *supra* n 37, 213–216. The case involved an application by a criminologist for permission to register, for research purposes, personal data extracted from police files on persons charged with receiving stolen property. The Inspectorate decided to allow registration only upon the basis of prior consent by each data subject. On appeal, the Justice Ministry overturned the Inspectorate's decision, partly on the ground that requiring the criminologist to contact the data subjects in order to ask for their consent would violate their 'integrity'.

grounded in a belief that the weighting given each interest must be largely context-dependant. I refer here to what is written in section 7.2.4. On this point, it is also worth noting that data protection laws themselves tend not to prescribe how such interest conflicts are to be resolved. Indeed, they usually do not recognise on their face any possibility of such conflicts. Concomitantly, they often omit to indicate which of the interests are more important than the others, instead referring simply to the interests as a largely undifferentiated group.[611] Consequently, data protection authorities and other bodies charged with overseeing implementation of data protection laws are frequently left with fairly free reins to resolve such interest conflicts as they see fit.

Not only each interest's relative importance must be determined on a case-by-case basis; also the degree to which each interest is threatened by data processing will depend on the particular circumstances of each processing operation. Important factors here include:[612]

1) the *content* and *nature* of the data (eg, to what do the data refer?; how comprehensive are they?);
2) the *source* of the data (eg, do they come from the data subject or a third party?; how reliable is the source?);
3) *to whom* the data are communicated (eg, to what extent is that person or organisation known by, or under the control of, the data subject(s)?;
4) what limits are imposed on that person/organisation's re-disclosure of the data?;
5) to what extent can the person/organisation be trusted to interpret the data correctly?;
6) *how* the data are communicated and registered (manually?; by computer?; in encrypted form?).

7.3 Interests of Data Controllers

Many of the interests in the catalogue presented in the preceding section are shared by data controllers in either the private or public sectors. All of the group 1 interests will typically fall within this category. Data controllers will also share one or more of the group 2 interests insofar as they support the needs and values of which the interests are an expression or insofar as they see such interests as capable of serving other interests they have.

The latter point is well exemplified in the efforts of private corporations to use data protection as a tool for retaining and/or expanding their respective customer bases. These efforts commonly involve the development by a corporation of a formalised, publicly available, data protection policy aimed at showing customers

611 See, eg, Arts 1(1) and 7(f) of the EC Directive.

612 See further Rasmussen, *supra* n 467, 66–70.

(current and potential) that the corporation handles customer data in a reliable and responsible manner. Less commonly, the efforts involve a corporation invoking data protection rules in order to prevent its competitors from engaging in conduct that is detrimental to its business interests.[613]

The importance attributed by data controllers to realising the data protection interests they share with data subjects will not necessarily be the same as that attributed by the data subjects themselves. Concomitantly, the effort (time, money and other resources) which a data controller is prepared to put into realising the interests will not necessarily suffice to realise the interests from the data subject's perspective. Further, the goals and values for which data controllers seek to realise the interests will not necessarily be the same as the equivalent goals and values of data subjects.

To take a simple example of these differences, a data controller will often seek to ensure that data are valid not just in order to safeguard the interests of the data subject in privacy, autonomy, etc – indeed, such interests might not figure at all in the controller's agenda of concerns – but to achieve, say, operational efficiency. At the same time, the controller's level of error tolerance in relation to the data could be higher than the data subject's tolerance levels. This might mean in turn that the amount of effort the controller is prepared to put into checking the validity of the data is not enough to ensure a validity level that guarantees satisfaction of the data subject's interest in such validity.[614]

Concern for operational efficiency is just one of numerous interests which data controllers will typically have and which do not figure explicitly in the list of interests given in the preceding sections. Little point is served for present purposes in setting out a detailed list of such interests. It suffices to note that while some of them

---

613 Belgian case law offers two graphic examples of such action. Both examples concerned plaintiff commercial actors (in the one case, two federations of insurance agents; in the other case, a financial credit bureau) instituting actions before the Tribunals of Commerce in Antwerps and Brussels respectively. The actions were brought against other commercial actors (in both cases, banks) for engaging in unfair competition occasioned by the banks' use of a particular strategy for marketing their services at the expense of similar services offered by the plaintiffs. In both cases, the strategy in dispute involved the banks analysing data on their clients which they had acquired in the course of normal banking operations, to offer the clients certain financial services (in the one case, insurance; in the other case, mortgage loans) that undercut the same sorts of services already received by the clients from the plaintiffs. The plaintiffs claimed that the strategy incurred breach of the purpose specification principle laid down in s 5 of the Belgian data protection law and that this breach also resulted in violation of doctrines on fair competition. The judges found for the plaintiffs in both cases. See *Aff OCCH v Générale de Banque*, decided by the Tribunal de commerce de Bruxelles, 15.9.1994; *Aff Feprabel et Fédération des courtiers en Assurances v Kredietbank NV*, decided by the Tribunal de commerce d'Anvers, 7.7.1994. Both cases are reported in (1994) *Droit de l'informatique et des télécoms*, no 4, 45–55. For commentary on the cases, see *ibid*, 55–62.

614 See also AF Westin & MA Baker, *Databanks in a Free Society: Computers, Record-Keeping, and Privacy* (New York: Quadrangle Books, 1972), 295.

lie at least partly latent in the interest catalogue presented in section 7.2.5,[615] many of them do not.

Also noteworthy is that some manifestation of these interests is found in data protection laws. They are most clearly manifest in exemption clauses to the rules embodying core data protection principles,[616] and/or in provisions specifying the considerations to be taken into account by data protection authorities either when carrying out their functions generally,[617] or when exercising their discretionary powers in more specific contexts.[618] More subtle manifestation of a concern to uphold the data-processing interests of data controllers arguably occurs in the very fact that the laws tend to operate with largely procedural rules that do not challenge fundamentally the bulk of established patterns of information use. In the language of road signs, data protection laws tend to post the warning 'Proceed with Care!'; they rarely order 'Stop!'.

The latter points figure prominently in the work of James Rule and several of his colleagues. According to these scholars, data protection laws operationalise an 'efficiency criterion' for safeguarding privacy and related values in the face of increasing bureaucratic surveillance.[619] This criterion allows surveillance to go ahead as long as core data protection principles are met. These principles, Rule *et al* suggest, do not radically threaten organisations' established systems of surveillance; they simply seek to make these systems more efficient, fair and, hence, socially acceptable.[620] As a result, Rule *et al* argue, adherence to the principles facilitates the avoidance of a 'frontal collision' between the privacy demands of the general populace and the surveillance practices of organisations.[621]

The above analysis by Rule *et al* focuses on the development of data protection law and policy in the USA before 1980. It enjoys a high degree of validity in that context. Its validity with respect to other jurisdictions and periods is by no means

---

615 The interest in operational efficiency, for instance, lies latent in the interests in group 1 of the catalogue, while the interest in freedom of expression lies latent in several of the interests in group 2 (particulary the interests in democracy, pluralism and autonomy).

616 See, eg, Art 13 of the EC Directive, permitting derogation from central obligations and rights in the Directive insofar as is necessary to safeguard, eg, 'national security', 'defence' or 'public security'.

617 See, eg, s 29(a) of Australia's federal *Privacy Act* which states that, in carrying out his or her functions, the Privacy Commissioner is to 'have due regard for the protection of important human rights and interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way'.

618 See, eg, s 34 of Norway's PDA which provides that when the Data Inspectorate assesses an application for a license to process personal data, consideration shall be given to whether or not problems which are caused for the individual person by the proposed processing and which cannot be solved satisfactorily by rules prescribed under other parts of the Act, 'are outweighed by *such considerations as favour* the processing' (emphasis added).

619 Rule *et al*, *supra* n 353, espec 71ff; Rule *et al*, *supra* n 352, 65–87.

620 Rule *et al*, *supra* n 353, 71.

621 *Ibid*, 69.

negligible but, in some cases, reduced. At least several data protection regimes – particularly in Europe – provide for the possibility of severely restricting data-processing practices on the basis of application of criteria that are broader than the 'efficiency criterion' described above.[622] Nevertheless, even these regimes are scarcely concerned with stopping or bringing about radical change to the bulk of established data-processing practices.

While concern for privacy and related values has been uppermost in the minds of citizens when they have clamoured for data protection laws to be introduced, this concern has not necessarily been shared to the same degree by the legislators. The latter have been primarily interested in finding a balance between the concerns of citizens as data subjects and the data-processing interests of data controllers (especially government agencies). Legislators' concern for citizens' privacy was perhaps greatest in the early years of legislating for data protection. From the late 1970s, this concern seems to have increasingly lost ground to other, predominantly economic, concerns. Much of the impulse behind the main data protection initiatives undertaken at an international level has stemmed from a desire to harmonise national data protection laws in order to maintain the free flow of data across borders.[623] Concomitantly, national legislators are under increasing pressure to pass data protection laws in order to avoid a situation in which the flow of data into their respective countries is restricted pursuant to the data protection laws of other countries.[624]

In some jurisdictions, work on the enactment of data protection legislation has been motivated to a large extent by a concern to create public acceptance for new or existing information systems. Thus, enactment of Australia's federal *Privacy Act* came about partly from a desire of the federal government to win support for a proposed national PIN scheme aimed largely at reducing fraud of the income-tax system and welfare programmes.[625] Similarly, enactment of the NZ *Privacy Act* was motivated partly by concern to create acceptance for planned and existing data-matching operations aimed at combatting abuse of government services.[626] Further, work on drafting a range of more recent data protection instruments, including the EC Directive and new federal data protection legislation for Canada, has arisen partly in order to engender public confidence in using new systems of electronic commerce.[627]

---

622 See, eg, the Norwegian data protection regime as described in Chapter 18 (section 18.4.7).

623 See Chapter 2 (section 2.3). See also JA Cannataci, *Privacy and Data Protection Law: International Developments and Maltese Perspectives*, CompLex 1/87 (Oslo: Norwegian University Press, 1986), 90–100.

624 See Chapter 6 (section 6.3.2).

625 See Bygrave, *supra* n 5, 138 and references cited therein.

626 See E Longworth & T McBride, *The Privacy Act: A Guide* (Wellington: GP Publications, 1994), 19ff and references cited therein.

627 See *supra* n 421 and references cited therein. Note also the European Commission press release of 25.7.1995 (IP/95/822) accompanying adoption of the EC Directive (citing comments by

In light of the above, together with the observations made in Chapter 6 (especially section 6.3), the predominant interest held by data controllers (and legislators) with respect to data protection laws is arguably to shore up data subjects' *confidence* that data are processed in a secure, responsible way. This interest does not necessarily conflict with the data protection interests held by data subjects, but efforts at realising it can result in a situation whereby the latter interests fail to be legally secured in much more than symbolic fashion.

(Cont.)
Commissioner Mario Monti to the effect that '[t]he Directive will … help to ensure the free flow of Information Society services in the Single Market by fostering consumer confidence …').

8. Concluding Observations for Part II

The preceding chapters of Part II show that the aetiology of data protection laws is complex. In explaining the laws' origins and continued existence, account must be taken of three broad categories of factors: (i) technological and organisational developments in the processing of personal data; (ii) public fears about these developments; and (iii) the nature of other legal rules.

The first of these categories embraces a variety of developments in data processing. The most important of these developments can be summed up in terms of increasing electronic interpenetration of previously distinct organisational spheres. This process involves the following, overlapping trends:

- greater dissemination, use and re-use of (personal) data across traditional organisational boundaries;
- replacement or augmentation of manual control mechanisms by automated control mechanisms.

Corollaries of these trends are increases in:

- the integration of organisations' data-processing practices;
- the re-purposing of (personal) data;
- the potential for misinterpretation and misapplication of these data;
- the potential for dissemination of invalid or misleading data;
- the automatisation of organisational decision-making processes;
- the blurring and dissolution of transactional contours.

A result of these developments is information systems of growing complexity and diminishing transparency, at least from the perspective of data subjects. At the same time, data subjects are rendered increasingly transparent *vis-à-vis* the various organisations with which they deal. Their environs feature an evermore pervasive, subtle and finely spun web of mechanisms by which their activities – both routine and extraordinary – are monitored and controlled. Furthermore, data subjects are placed under increasing risk of being assessed or interfered with on the basis of information that is invalid or otherwise of poor quality.

The catalysts for these developments are partly economic, social and political; ie, they are linked with efforts to enhance organisational efficiency, profitability, prestige and service. Such efforts can be seen, in turn, as symptomatic of a deep-seated concern for reflexivity and rationalisation. The catalysts are also partly technological; ie, they are facilitated and, to some extent, driven by the ever-greater

ability of IT to amass, analyse and disseminate data. Nevertheless, IT plays a double-sided role. It both diminishes and enhances our privacy. It facilitates large-scale and subtle forms of surveillance but can also help us evade such surveillance. It functions as an instrument to cope with complexity at the same time as it helps generate complexity. It is both a steering instrument and a stimulus for entropy and fragmentation. It is an aid to better understanding at the same time as it holds our understanding hostage.

The second category of factors behind the emergence and continued existence of data protection laws consists, firstly, of a congeries of public fears about the effects of the developments outlined above. These fears cluster about three interrelated themes:

- increasing transparency, disorientation and disempowerment of data subjects *vis-à-vis* data controllers;
- loss of control over technology;
- dehumanisation of societal processes.

Feeding these fears are concrete experiences of systematic authoritarian repression (eg, Nazism) and of attempts to undermine the bases of pluralist democracy (eg, Watergate), together with a range of dystopian visions of the future (eg, Orwell's *Nineteen Eighty-Four*). Accumulating evidence of poor information quality also plays a role.

The pervasiveness of the fears reflects a climate of growing distrust of organisations and technology. This growth in distrust reflects in turn a general societal trend whereby human action is increasingly weighed down by awareness of risk.

The adoption of data protection laws (and guidelines) *after* the initial wave of such laws were enacted in the 1970s has been driven by another class of fears as well. These fears are primarily economic in nature and shared by governments and businesses. One of these fears concerns the possibility that transborder data flows will be greatly impeded pursuant to rules in data protection laws aimed at thwarting the flow of data to so-called data havens. Another fear concerns the possibility that, in the absence of data protection laws, the general populace will lack the confidence to participate in systems of electronic commerce, particularly as consumers/ prosumers.

The development of data protection laws has also been shaped by other laws and legal doctrines. To begin with, there is the trite point that data protection legislation would scarcely have been enacted but for perceived failings in the ability of already-existing laws to tackle adequately the problems arising as a result of the two categories of factors outlined above. Secondly, a variety of laws and legal doctrines have served as sources of inspiration for the development of data protection laws by positively providing the latter with a normative basis. We see that data protection legislation is most directly inspired by, and most closely related to, administrative

law and human rights law. The connection with human rights law is primarily found in the central values safeguarded by data protection legislation – privacy, autonomy, integrity and, ultimately, dignity. The connection with administrative law is primarily found in the principles laid down in data protection legislation for safeguarding these values: they are principles that build upon traditional rules on due administrative process – rules that derive in turn from doctrines on rule of law.

If we consider more closely the values safeguarded by data protection laws, we find these to be numerous and varied. From the perspective of data subjects, the concerns of data protection laws fall into two categories. The first category comprises interests that relate to the quality of (personal) information and information systems. The overarching interests here can be summed up in terms of ensuring data validity and information utility, together with information systems' manageability, robustness, accessibility, reliability and comprehensibility. The second category comprises interests pertaining to the condition of persons as data subjects and to the quality of society generally. The overarching interests in this category can be summed up in terms of ensuring privacy, autonomy, civility, democracy, pluralism, rule of law and balanced control. Considerable overlap exists between these interests; moreover, all of them are ultimately grounded in concern for human integrity and dignity. At the same time, potential exists for conflict between them and for conflict between them and the first category of interests.

Many of the above interests will be shared by data controllers, though not necessarily to the same degree nor for the same reasons as with respect to data subjects. Data protection laws also show concern – both implicit and explicit – for securing a variety of other legitimate interests of data controllers which are realised by the processing of personal data. Indeed, the laws tend not to seek to assail the bulk of established systems of administration, organisation and control; rather, they tend merely to seek to manage these systems in a manner that makes them more palatable and, hence, legitimate for the general populace.

Extending the latter point, it can be argued that data protection laws have much the same aim and function as policies of 'sustainable development' have in the field of environmental protection. While data protection laws seek to safeguard the privacy and related interests of data subjects at the same time as they seek to secure the legitimate interests of data controllers in processing personal data, policies of 'sustainable development' seek to preserve the natural environment at the same time as they allow for economic growth. Both policy concepts promote a belief that the (potential for) conflict between these respective sets of interests can be significantly reduced through appropriate management strategies. Concomitantly, both policy concepts can be used to create an impression that the interests of data subjects and the natural environment are adequately secured, even when their respective counter-interests are also secured.

Against the background of the material presented so far, how might we most accurately and concisely sum up the concerns of data protection laws? The most

popular way of summing up these concerns is to hold that data protection laws are essentially about safeguarding privacy and/or informational autonomy/self-determination. Yet, in light of the material covered in Parts I and II, to depict the agenda of data protection laws simply in these terms is to underplay the breadth of data protection interests. While the laws certainly have protection of privacy and autonomy as two of their main concerns, they have other concerns as well. Concomitantly, many of their rules relate only indirectly to the protection of privacy and autonomy. Explanations of the laws' agenda in terms of such protection have most validity if we look at that agenda from the perspective of data subjects. They have less validity if we also take into account the perspective of data controllers.

Might the concern of data protection laws be better summed up in terms of preventing illegitimate discrimination? Such a characterisation has considerable validity. Data protection laws are intended to, and do, grapple with certain discriminatory processes; ie, processes whereby action (typically exclusionary) is taken (or not taken) on the basis of perceived differences between persons (or classes of persons). Profiling is a key instance of such a process – as is made clear in Chapter 17. Hence, the regulation of profiling by data protection laws is implicitly about the regulation of discriminatory processes. This is especially apparent with rules, such as Art 15 of the EC Directive, aimed at controlling fully automated decision making and with rules aimed at enforcing informational relevance. The link between data protection laws and concern for preventing illegitimate discrimination is further underlined by the laws' tendency to apply special measures for classes of data (eg, on race/ethnicity, gender and religion) that are traditionally the subject of anti-discrimination legislation. However, it would be inaccurate to characterise data protection laws as solely or even mainly concerned with preventing illegitimate discrimination. For example, a major concern of the laws is to enhance for data subjects the transparency of an increasingly complex informational environment. This concern cannot be explained solely or chiefly in terms of a desire to prevent undue discrimination; considerations of autonomy, insight/comprehensibility and, at a broader societal level, plurality and democracy play an important role too.

An alternative (though complementary) way of summing up the concerns of data protection laws is to hold that the latter are aimed essentially at ensuring fairness in the processing of personal data and, to some extent, fairness in the outcomes of such processing. This perspective has been championed on both sides of the Atlantic.[628] It has considerable appeal since the bulk of the basic principles of data protection laws can be seen as elaborating a concern for fairness to data subjects. Moreover, relative to the other perspectives outlined above, the notion of fairness better captures the fact

628 See, eg, US Department of Health, Education and Welfare (DHEW), Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington, DC: DHEW, 1973), 41; Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, DC: US Government Printing Office, 1977), 17; Bull, *supra* n 481, 84.

that the laws' regulation of data processing usually involves taking account of, and balancing, the (legitimate) interests of a plurality of actors, of which data subjects are just one (albeit important) category.[629]

It is necessary, though, to elaborate upon what the notion of fairness entails in this context for it is a broad notion with many facets. Here, fairness involves two steps:

1) taking account of all interests that are affected by a particular data-processing operation (or set of operations); then
2) searching for 'right proportions' when safeguarding these interests insofar as the latter conflict with each other.

Looking more closely at step (1), this entails attempting to:

- ensure that each party carrying out or affected by the data-processing operation(s) pays due regard to the interests of the other parties;
- guarantee that all parties have sufficient knowledge of the operation(s) to uphold their respective interests, or at least are given an opportunity of gaining such knowledge;
- provide an opportunity to all parties to present their opinions about the operation(s), preferably before the latter commence;
- ensure that each party acts in a manner that accords with the reasonable expectations of the other parties; and
- ensure that each party takes steps to prevent errors or other weaknesses in the quality of its actions from having a detrimental impact upon the other parties' interests.

These elements of step (1) can be viewed as constituents of a procedural kind of fairness. It is with the fixture of these elements that most of the rules and principles of data protection laws are directly concerned.

However, data protection laws are also concerned with the more substantive type of fairness embodied in step (2) inasmuch as they attempt to prevent the interests of data subjects in privacy, autonomy, integrity, etc being overrun by other interests. In other words, data protection laws are concerned with substantive fairness insofar as they attempt to arrive at a fair result of the processes in step (1) and not just a result that is arrived at fairly.[630]

---

629 Cf US Privacy Protection Study Commission, *ibid*, 21.

630 Of course, it is more difficult to agree about what constitutes a fair result than about what constitutes a fair process. Some people might argue that a fair process necessarily leads to a fair result; others would argue that a fair process is merely a necessary but not sufficient condition for a fair result; still others would argue that a fair process is neither a necessary nor sufficient condition for a fair result.

PART III:
DATA PROTECTION RIGHTS FOR PRIVATE COLLECTIVE ENTITIES

'What is regarded as a legal entity and what social importance is given to it, from what points of view it is taken as needing social protection and what in consequence its rights are – all these are questions which depend entirely on the changing evaluation of the given community and can therefore be ascertained by observation only and can never be guessed by any *a priori* principles.'

– A Nékam, *The Personality Conception of the Legal Entity* (Cambridge, Massachusetts: Harvard University Press, 1938), 116.

9. Background to Issue

9.1 Parameters of the Issue

This part of the book examines the extent to which it is desirable that the processing of information on private collective entities – primarily those that are organised – be controlled pursuant to the regulatory regimes created by data protection laws. For the sake of brevity and convenience, this issue is often described in the following simply in terms of whether or not private collective entities should be given data protection rights.

It bears repeating that the bulk of analysis here is concerned with the rights and interests of *organised* collective entities in the private sector. Accordingly, unless otherwise stated, references to 'collective entities' should be understood as references to entities that are organised. A relatively short analysis of the rights and interests of *non-organised* collective entities is given in Chapter 15.

An organised collective entity is one that is constituted on the basis of the individual members of the entity coming together to set up and maintain the entity through a series of more or less systematic, formalised measures. Legally, there are two main categories of organised collective entities: those that are legal/juristic persons and those that are not. A legal/juristic person (hereinafter termed simply 'legal person') is a body granted certain legal rights and obligations, such that it gains a legal status separate from the persons who constitute and represent it.

Legal persons in the private sector fall within two main classes. The first class embraces business enterprises, which have as their sole or main goal the creation of financial profit. These enterprises range from large, multinational corporations, such as British Petroleum, General Motors and Philips, to small, family-run enterprises, which mainly operate within a single country or district. The other main class embraces what are commonly termed 'non-profit' organisations; ie, organisations that do not have the creation of financial profit as their sole or main goal. The principal aims and activities of these sorts of bodies vary greatly. In their ranks are found: religious bodies, such as the Church of Scientology; charitable or eleemosynary organisations, such as the Salvation Army; educational institutions and foundations, such as private universities and colleges; environmentalist organisations, such as Greenpeace; humanitarian bodies, such as Amnesty International; trade unions and political organisations, such as the Australian Labor

Party; and a range of fraternal associations, including sporting clubs, aesthetic societies and so-called 'brotherhoods', such as the Masons.

With regard to legal persons generally, special mention should be made of one-person enterprises; ie, enterprises owned and operated by only one person, usually for commercial purposes. Strictly speaking, such enterprises are not collective in nature. Hence, one must keep in mind that not all legal persons are a sub-set of the category 'collective entity'.

Organised collective entities which are not formally recognised as legal persons in a particular jurisdiction – for instance, partnerships under Anglo/Australian law – can also be classified according to whether or not they have the generation of financial profit as their primary goal. While the chief *raison d'être* of many partnerships (eg, of accountants and lawyers) is pursuit of profit, a large number of other unincorporated associations are run along non-profit lines with a range of goals and activities at least as varied as the categories listed above in relation to legal persons. These associations range from citizen-initiative groups established to campaign around a particular political issue (eg, nuclear disarmament, prisoners' rights) to sewing groups and card clubs.

Some of the categories drawn above are essentially ideal types and, in reality, by no means hard and fast. For instance, many apparently non-profit organisations are engaged in profit-seeking activity.[631] Moreover, determining whether or not a legal person is properly to be characterised as private or public, is not always easy. This is the case, for instance, with government-owned corporations that compete against other private sector corporations, or with privately-owned corporations that carry out government tasks pursuant to outsourcing agreements.

The processing of data is usually only regulated by data protection legislation when the data can facilitate a person's identification.[632] Accordingly, this part of the book is concerned only with the processing of those data from which a particular collective entity can be identified. In relation to, say, a private corporation, such data can include details on the corporation's

- name, contact address and date of establishment;
- management and ownership structure;
- number of employees and/or members;
- scope and site of its various operations;
- assets, profits, losses and capital turnover;
- plans, strategies and ideology;
- customers and allies;
- products (industrial or otherwise);

---

631 As Conard aptly points out, '[m]any universities and hospitals make a profit from some of their customers in order to lose it on others. The profit aspect is particularly conspicuous in "foundations", some of which are among the ... larger investors [of the USA]'. See AF Conard, *Corporations in Perspective* (Mineola, New York: Foundation Press, 1976), 143.

632 See further Chapter 2 (section 2.4.1).

- consumption of resources; and/or
- transgressions of the law.

Some of this information might be easily linked not only to a particular corporation but also to particular individuals attached to the latter. These individuals could be attached in several ways: as employees (from manager/director status and downward), investors (shareholders, sponsors), members and customers. Some of the above types of information (eg, information on corporate assets, profits, losses and capital turnover) could be readily available to the general public. Other types of information (eg, information on corporate plans and strategies) could be subject to duties of confidentiality which limit its disclosure to certain parties.

A broad spectrum of organisations are interested in accessing and using various aspects of this information. These organisations include governmental regulatory authorities, credit-rating agencies, business competitors, trade unions, environmental and consumer protection groups. They are interested in using this information for a range of purposes, such as

- general planning and statistics;
- providing financial support for corporations (in the form of loans, subsidies, insurance, etc);
- levying taxes on corporations;
- ensuring that corporations comply with laws (eg, laws concerned with environmental safety or the keeping of financial accounts);
- selling products to corporations.

Similar comments can be made for other types of collective entities.

The issue of whether or not information on collective entities (including those that are non-organised) should be safeguarded pursuant to data protection laws can only be resolved properly by canvassing a multiplicity of factors. These factors include:

- the extent to which data on collective entities are protected under other types of laws;
- the practical experiences had by those countries that have enacted data protection laws expressly protecting data on collective entities; and
- at a more theoretical level, the extent to which collective entities have interests that need to be safeguarded by data protection legislation.

The last of these factors brings us to an important characteristic of collective entities (including those that are non-organised[633]): they can be regarded either as being independent of, and greater than, the sum of their individual parts, or they can be reduced to the particular constellation of individual persons who make up these parts. This characteristic can be termed the ‘duality’ of collective entities. Because of it,

633 Though see Chapter 15 (section 15.2).

consideration must be given to the possibility and desirability of protecting data on collective entities in order to provide better protection for the individuals who constitute or are otherwise linked with them, *and* in order to safeguard possible interests of their own. If collective entities do have data protection interests of their own, one should also consider the extent to which these interests are similar to the data protection interests of individual persons.

The duality of collective entities is but a reflection of the fact that the way in which we perceive such entities is no simple, straight-forward matter. As Gareth Morgan has shown, we tend to perceive organisations by using metaphors that often work at a subconscious, intuitive level.[634] Morgan identifies a range of such metaphors: eg, organisations as machines, as organisms, as brains, as cultures, as political systems, as pyschic prisons, as processes of flux and transformation, as instruments of domination. These metaphors are not just interpretive constructs; they also provide frameworks for policy and action. Thus, when analysing the data protection interests of collective entities, we must not lose sight of the influence of these metaphors. A plausible, working hypothesis in this respect is that certain of these metaphors – notably those of organisations as machines and as instruments of domination – tend to pervade the thinking of those persons who argue against giving data protection rights to organised collective entities, while other metaphors – notably that of organisations as organisms – tend to pervade the thought of those persons who are in favour of giving such rights to these entities.

When analysing collective entities' possible data protection interests, account needs also to be taken of the great variety of such entities (independent of metaphorical variety), the multifarious nature of information about them, and the large range of contexts in which this information is used. To treat collective entities – and data on them – as an undifferentiated mass would seem misguided. As shown above, collective entities are not all constituted for the same purposes. Neither do they all play the same economic, political, legal and social roles, nor have the same goals and resources. One needs, though, to consider the extent to which the nature of data protection laws requires differentiating between various kinds of collective entities in order for the laws to function.

All of the above factors are elaborated upon in subsequent chapters of this Part. Unfortunately, there have not been, to my knowledge, any other in-depth studies carried out which satisfactorily take into account all of these factors. As noted in the Introduction, the decisions taken in most countries on whether or not particular collective entities (notably, private corporations) should be given data protection rights, seem to have been made without an extensive and thorough study of the issue first being undertaken. Concomitantly, much of the debate on the issue has been rather shallow.

---

634 G Morgan, *Images of Organization* (London: Sage Publications, 1986).

The hitherto most detailed and systematic treatments of the issue which I have come across are a report written for the OECD in 1981 by Edmund Hogrebe,[635] and two reports written for the EC Commission – one in 1980 by a group of French data protection experts (Bancilhon *et al*),[636] the other in 1998 by Douwe Korff.[637] These are supplemented by a small number of reasonably balanced yet briefer analyses.[638] All of the studies deal mainly with data protection rights for legal persons, not collective entities generally. Most of them make little attempt to set out or analyse the scope and practical consequences of those countries' data protection laws that presently encompass legal person data. This detracts from their ability to draw meaningful and firm conclusions as to the most appropriate legal mechanism(s) for protecting data on legal persons and other types of collective entities. For many of the studies, such an ability is also hampered by the fact that they were undertaken just after the enactment of most of the data protection statutes that protect legal person data; hence, they could only make a tentative appraisal of the practical consequences of this legislation. The report by Korff, though, is relatively extensive and up-to-date in its treatment of practical consequences.

It should be emphasised that the analysis in this Part is not concerned primarily with issues of statutory technique and drafting. It is concerned, first and foremost, with the propriety of applying the principles of data protection law to data on collective entities rather than with the particular legislative format such an application should take. Moreover, it is less concerned with arguing for a conclusive answer to the issue of whether or not collective entities should be given data

---

635 E Hogrebe, *Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues*, Report for the OECD Working Party on Information, Computer and Communications Policy (DSTI/ICCP/81.25). A summary of Hogrebe's report is to be found in 'Company Data Regulation Foreseen under National Data Policies' (1981) 4 *TDR*, no 8, 9–10.

636 F Bancilhon, J-P Chamoux, A Grissonnanche & L Joinet, 'Das Problem natürliche Person/andere rechtliche Einheiten', in *Studie über Datenschutz und Datensicherheit*, final report to the EC Commission by the Gesellschaft für Mathematik und Datenverarbeitung, the Institut de Recherche d'Informatique et d'Automatique and the National Computing Centre, May 1980, vol 3. I have only had access to the German version of the report, which was originally written in French. Most of the main points in the report are reproduced in J-P Chamoux, 'Data Protection in Europe: The Problem of the Physical Person and the Legal Person' (1981) 2 *J of Media Law and Practice*, 70–83.

637 Korff, *supra* n 16.

638 See Y Poullet & P Poullet, 'Applicabilite aux Entreprises d'une Legislation protectrice des Données', paper presented at a conference entitled 'Banque de Données, Entreprises, Vie Privée', Namur, Belgium, 25–26 September 1979; J Wright, 'Protection of Corporate Privacy' (1983) 6 *TDR*, no 4, 231–234; H Rumpf, 'Datenschutz für juristische Personen und Personenvereinigungen?' (1984) 13 *Datenverarbeitung – Steuer – Wirtschaft – Recht*, 135–143; L Tuner, 'Gehört ein Datenschutz für juristische Personen ins allgemeine Datenschutzrecht?' (1985) *DuD*, no 1, 20–27; IN Walden & RN Savage, 'Data Protection and Privacy Laws: Should Organisations be Protected?' (1988) 37 *Int & Comparative L Quarterly*, 337–347; Henke, *supra* n 86, 71–75; Blume, *Personregistrering*, *supra* n 93, 326–328; NOU 1997:19, 53–54; A Rossnagel, A Pfitzmann & H Garstka, *Modernisierung des Datenschutzrechts*, report for the German Federal Ministry of the Interior (Bundesministerium des Innern), September 2001, 64–67, <http://www.bmi.bund.de/downloadde/11659/Download.pdf>.

protection rights than with creating a general framework for analysing all aspects of the issue. It seeks to explore perspectives and examine the viability of arguments that debate on the issue has raised.

Nevertheless, a basic thesis informs the analysis. In very general terms, this thesis is that the core principles of data protection law are logically *capable* of being extended to protect data on collective entities (organised and non-organised). Further, collective entities are capable of sharing most, if not all, of the interests of data subjects which data protection laws typically safeguard. Whether or not the basic principles of these laws *should* be extended to protect collective entity data can only be determined for a particular country on the basis of a consideration of the *need* for extending such protection. This factor of need can be broken down into several other factors:

1) the economic, political and social roles that the various types of collective entities *actually* play in the country concerned;
2) the economic, political and social roles that the country *desires* the various kinds of collective entities to play;
3) the extent to which giving collective entities data protection rights would promote the chance of these entities fulfilling these desired roles; and
4) other aspects of the country's legal system and culture, including the manner in which its various laws currently protect data on different sorts of collective entities.

9.2 Early Enthusiasm for Protecting Collective Entity Data

The notion that collective entities should be given data protection rights appears to have enjoyed greatest popularity in the 1970s; ie, during the earlier stages of discussion on privacy and data protection issues. Much of the groundwork for the notion was laid in the late 1960s in North America by Alan Westin. In his book, *Privacy and Freedom*, Westin argues that privacy serves similar functions for organisations as it does for individuals, though he refrains from discussing whether or not organisations should be given the same *legal rights* to privacy as individuals.[639]

It is difficult to gauge the influence of Westin's analysis of the need for 'organizational privacy' on subsequent debate over collective entities' rights to privacy and data protection. Surprisingly, very few contributors to this debate make any explicit reference to Westin's pioneering treatment of the issue. Nevertheless, several other individuals and committees who/which were amongst the first in their respective countries to address privacy and data protection issues, thought like Westin that certain kinds of collective entities have a need for privacy and/or data

639 Westin, *supra* n 335, 42–51. For further analysis, see Chapter 12 (section 12.2.2).

protection. Notable examples are Wilhelm Steinmüller in Germany,[640] Ragnar Dag Blekeli[641] in Norway, the Younger Committee[642] and Paul Sieghart[643] in the UK, Stanley Benn[644] and the NSW Privacy Committee[645] in Australia, and the so-called 'Vienna Working Group' ('Wiener Arbeitskreis') in Austria.[646]

The first data protection law ever enacted made no distinction between data on natural and legal persons. This was the *Data Protection Act* passed in 1970 by the German *Land* Hessen.[647] Towards the end of the 1970s, four countries – Norway, Denmark, Austria and Luxembourg – enacted national data protection laws expressly covering data on both legal and natural persons. Iceland followed suit in 1981. The enactment of these laws fueled predictions that the legislative wave of the future, at least in the field of European data protection, would encompass legal person data in addition to data on natural persons.[648]

These predictions were not borne out by events. The overwhelming majority of national data protection laws passed after the early 1980s expressly cover data on individuals only. In this period, only two countries have enacted general data protection laws expressly covering both legal and natural person data: Switzerland in 1992,[649] Italy in 1996. Moreover, several of the countries that initially passed laws

---

640 See, eg, W Steinmüller, 'Fragestellungen der internationalen Datenschutz-diskussion', in G Stadler (ed), *Datenschutz*, Proceedings of the Vienna Conference on Data Protection held by the Austrian Commission of Jurists in April 1975 (Vienna: Österreichische Juristen-Kommission, 1975), section 4.3.2 (published without pagination); W Steinmüller, 'Stellenwert der EDV in der Öffentlichen Verwaltung und Prinzipien des Datenschutzes' (1972) 2 *Öffentliche Verwaltung und Datenverarbeitung*, 453, 461.

641 See, eg, Blekeli, *supra* n 505, 24.

642 The UK Committee on Privacy (the Younger Committee), *Report of the Committee on Privacy*, Cmnd 5012 (London: HMSO, 1972), 179 & 183.

643 Sieghart, *supra* n 335, 134.

644 Benn, 'The Protection and Limitation of Privacy', *supra* n 590, 603–604, 609.

645 NSW Privacy Committee, *Privacy Protection: Guidelines or Legislation?* (Sydney: NSW Privacy Committee, 1980), 6.

646 'Begriffsbildung im Datenschutz', document dated 19.12.1974 and set out in both Stadler, *supra* n 640 (no pagination) and (1975) 5 *Öffentliche Verwaltung und Datenverarbeitung*, 91–92. Members of the working group were Alfred Berger, Walter Dohr, Gerhart Pawlikowsky and Gerhard Stadler.

647 *Hessisches Datenschutzgesetz vom 7 Oktober 1970* (see espec s 5(3)). The second of the German *Länder* to pass data protection legislation, Rhineland-Palatinate, took a similar approach: see *Gesetz gegen missbräuchliche Datennutzung (Landesdatenschutzgesetz) vom 24 Januar 1974* (espec s 1(1)). Both Acts have since been replaced by laws limited to protecting data on individuals. Indeed, none of the German *Länder* have data protection laws expressly covering legal person data.

648 Such predictions are expressed in HP Gassmann, 'Privacy Implications of Transborder Data Flows: Outlook for the 1980s', in LJ Hoffman (ed), *Computers and Privacy in the Next Decade* (New York: Academic Press, 1980), 109, 111; H Seip, 'More Countries to Protect Legal Person Data' (1982) 5 *TDR*, no 2, 105.

649 For constitutional reasons, Switzerland's federal *Data Protection Act* only regulates the processing of data by federal government authorities and by private persons and organisations. Well before the passage of this Act, though, many of the Swiss cantons had enacted laws, regulations and/or

expressly protecting data on collective entities, have recently abolished or reduced such protection.[650]

At the international level, considerable support existed in some fora during the 1970s for giving individuals and particular types of collective entities broadly similar rights to data protection. Hondius writes that, in 1971, the International Association of Lawyers submitted to the CoE two proposals for an international convention on privacy protection both of which sought to protect under the one agreement data concerning natural and legal persons.[651] In 1979, a Subcommittee on Data Processing and Individual Rights set up by the Legal Affairs Committee of the European Parliament expressed some sympathy for providing legal persons with data protection rights but felt that such a move ought to be deferred until more research into the issue had been completed. At the same time, the Subcommittee was strongly in favour of protecting data relating to non-organised groups of persons.[652] The findings of the Subcommittee were followed up by the European Parliament's Resolution of 8.5.1979 on the protection of the rights of the individual in the face of technical developments in data processing, point 7 of which states:

> 'the protection of data relating to legal persons, and notably to undertakings, *might* be necessary for the smooth operation of the common market, and that it should – in an appropriate form – be guaranteed also to political, trade union and religious groups.'[653]

Appended to the Resolution are a set of principles recommended by the Parliament as forming the basis for EC norms on data protection. Principle 17 stipulates:

> 'Data relating to groups of individuals and the rights of such groups within the ambit of these principles shall be accorded the same protection as personal data and the rights of individuals within the meaning of the above-mentioned principles.'[654]

This principle seems largely to have been ignored in the follow-up work of the EC Commission in drafting the main EC Directive on data protection. Nevertheless,

---

(Cont.)
guidelines regulating the activities of their administrative agencies in respect of data on both legal and natural persons.

650 See further section 9.4.

651 Hondius, *supra* n 55, 97 and references cited therein. Neither of the two proposals was realised. Hondius intimates that this was on account of the proposals lumping too many issues together: *id*.

652 European Parliament, Legal Affairs Committee, Subcommittee on Data Processing and Individual Rights, *Report on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing* (the 'Bayerl Report') (EP Doc 100/79, PE 56.386, 4.5.1979), 28.

653 OJ C 140, 5.6.1979, 34, 36 (emphasis added).

654 *Ibid*, 38.

some concern for collective entities is found in the EC Directive on telecommunications privacy and the coming Directive on privacy of electronic communications. Most of the key provisions in these instruments expressly protect the interests of legal persons in addition to natural persons.[655]

The express extension of basic human rights to collective entities has precedent in international law. For instance, Art 34 of the ECHR (as amended by Protocol No 11) allows the European Court of Human Rights (ECtHR) to hear complaints from 'any person, non-governmental organisation or group of individuals claiming to be the victim of a violation ... of the rights set forth in the Convention …'. Hence, there is a *possibility* of a (private sector) collective entity bringing an action for interference with *its* alleged rights under the Convention's Art 8(1).

On this point, the ECHR is to be contrasted with the ICCPR, which appears to protect the rights of individual, natural persons only. Article 2(1) of the ICCPR obliges State Parties to the Covenant to respect and ensure to 'all individuals' the rights set out in the Covenant. Use of the term 'individuals' is claimed as indicating that the rights in the ICCPR may only be enjoyed by individual natural persons.[656] Moreover, unlike Art 34 of the ECHR, the first Optional Protocol to the ICCPR provides only 'individuals' a right to file complaints about violations of the Covenant. Nevertheless, 'measures taken by a state party against a juridical entity might constitute a violation of the Covenant if they infringe upon the rights of individuals'.[657] At the same time, the above references to the term 'individuals' might not deprive collective entities of any possibility of enjoying in their own right (ie, independent of their individual members) protection under the ICCPR. Some of the Covenant's provisions, including Art 17 on protection of privacy,[658] are formulated in terms of '[n]o one …', a phrase that is sufficiently broad to encompass collective entities.[659] As shown below, the Strasbourg organs have extended to collective entities several of the rights in the ECHR which are formulated as belonging to '[e]veryone'. More generally, the Strasbourg organs have taken a broad, evolutive view of the scope of the provisions in the ECHR, overriding somewhat the

655 See further Chapter 10 (section 10.2).

656 See T Buergenthal, 'To Respect and to Ensure: State Obligations and Permissible Derogations', in L Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (New York: Columbia University Press, 1981), 73; M Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Kehl am Rhein/Strasbourg/Arlington: Engel, 1993), 39. See also F Volio, 'Legal Personality, Privacy and the Family', in Henkin, *op cit*, 185, 441, n 1 ('The Covenant deals with ... the rights of rational, physical persons, not of corporations, associations, or other legal persons').

657 Buergenthal, *ibid*. See also Nowak, *ibid*, 40.

658 See Chapter 6 (section 6.4.1).

659 A separate issue is whether the remainder of such provisions – in particular, references to concepts like 'privacy' – are capable of being applied to collective entities. For discussion of the applicability of the privacy concept to such entities, see Chapter 12 (section 12.2).

literal import of the wording used.[660] It is conceivable, if not probable, that the Human Rights Committee will take a similar line for the benefit of collective entities.[661]

No definitive decision has yet been made by the ECtHR on whether or not a collective entity – be it a corporation, association or more loosely organised group – may bring an action for alleged interference with its putative right to respect for private life under Art 8(1). As for the European Commission of Human Rights (ECommHR – now abolished), its line on the issue was somewhat confusing.

In *Mersch and Others v Luxembourg*, the ECommHR accepted that two political organisations in Luxembourg (the League for the Defence of the Rights of Man and the Socialist Workers' Party) were able to qualify as victims of an alleged interference with Art 8(1) rights incurred by police monitoring of their communications.[662] The Commission appeared to consider the two organisations as enjoying protection under Art 8 in their own right, though this is not entirely certain. Further, in *G and E v Norway*, the Commission held that 'a minority group is, in principle, entitled to claim the right to respect for the particular life style it may lead as being 'private life', 'family life' or 'home'' under Art 8(1).[663] Although the facts of this case did not concern data protection issues,[664] the Commission's decision portends the possibility that members of a minority group could bring an action for alleged interference with the group's putative right to respect for private life under Art 8(1) on account of certain practices involving the use of data on the group as such. Nevertheless, it is difficult to envisage a situation in which such practices also would not give rise to actions for interferences with the Art 8(1) rights of each of the group members as individuals.

Later decisions of the ECommHR show a reluctance to allow collective entities – particularly legal persons – direct protection pursuant to Art 8. In *Open Door Counselling and Dublin Well Woman v Ireland*, the Commission rejected an argument by Open Door Counselling Ltd that the company itself had a right to respect for private life under Art 8, though the Commission seemed not to cut out all

---

660 See generally JG Merrills, *The Development of International Law by the European Court of Human Rights* (Manchester: Manchester University Press, 1993, 2nd ed), espec chapt 4; Harris, O'Boyle & Warbrick, *supra* n 589, 5ff.

661 See also Nowak who, whilst viewing most of the rights in the Covenant as being formulated in such a way as to relate only to individuals, recognises that solid arguments exist for allowing collective entities (including legal persons) to lay claim to at least some of these rights: Nowak, *supra* n 656, 40. He does not elaborate on this point, however, in relation to Art 17 specifically.

662 *Mersch and Others v Luxembourg* (1985) Appl 10439/83, 10440/83, 10441/83, 10452/83, 10512/83 & 10513/83, 43 DR 34, 113–114. The case was not passed on to the Court for assessment on the merits as the Commission found the interference justified under Art 8(2).

663 *G and E v Norway* (1983) Appl 9278/81 & 9415/81, 35 DR, 30, 35.

664 The case concerned a claim by two Norwegian Lapps that the construction of the Alta dam in northern Norway was in violation of, ia, Art 8. The Commission found that even if the Alta dam project interfered with the applicants' private life, the interference was justified under Art 8(2).

possibility of legal persons having such a right.[665] A similar line was taken in *Church of Scientology of Paris v France*, with the Commission stating that Art 8 'has more an individual than a collective character' yet refraining from exhaustively determining the issue.[666]

The data protection laws of most CoE Member States, along with the CoE Convention, do not expressly safeguard data on collective entities. Hence, no evidence exists of a European consensus in favour of protecting these data and capable of inspiring the ECtHR to read such safeguards into Art 8.

Nevertheless, there is abundant case law of the Strasbourg organs accepting the ability of some types of collective entities to enjoy the right to 'freedom of expression' under Art 10, and the rights to 'freedom of peaceful assembly and to freedom of association' pursuant to Art 11.[667] In addition, several decisions have been made concerning the ability of collective entities to invoke Art 9(1), which provides that '[e]veryone has the right to freedom of thought, conscience and religion'. It has been held that a religious body may invoke Art 9 but that other types of collective entities may not.[668]

---

665 *Open Door Counselling and Dublin Well Woman v Ireland* (1992) A 246, Annexed Opinion of the Commission, para 64.

666 *Church of Scientology of Paris v France* (1995) Appl 19509/92, admissibility decision of 9.1.1995, para 1, unpublished. For details of the case, see Korff, *supra* n 16, 14, 19 & 20.

667 With regard to freedom of expression, see, eg, the decisions of the Court in *Autronic AG v Switzerland* (1990) A 178 (allowing a limited company pursuing commercial ends to invoke Art 10) and *Open Door Counselling and Dublin Well Woman v Ireland* (1992) A 246 (allowing two limited companies engaged in non-profit activities to invoke Art 10). With regard to freedom of association and assembly, see generally C Tomuschat, 'Freedom of Association', in RStJ Macdonald, F Matscher & H Petzold (eds), *The European System for the Protection of Human Rights* (Dordrecht/Boston/London: Martinus Nijhoff, 1993), 493ff, and cases cited therein. Tomuschat notes that Article 11 protects associations independent of whether or not they formally possess legal personality separate from their constituent members. However, it does not protect public sector organisations. Neither does it encompass unorganised groups without specific common objectives nor groups constituted merely on the basis of cultural or ethnic ties. According to Tomuschat, there is also some doubt that the right to freedom of association protects purely commercial enterprises.

668 See, eg, the decisions of the ECommHR in the following cases: *X and Church of Scientology v Sweden* (1979) Appl 7805/77, 16 DR 68, 70 (deciding that a church body is capable of exercising the right to freedom of religion under Art 9(1) 'in its own capacity as a representative of its members'); *Swami Omkarananda and the Divine Light Zentrum v Switzerland* (1981) Appl 8118/77, 25 DR 105 (deciding that an association with religious and philosophical objects is also capable of exercising the right to freedom of religion in Art 9(1)). Cf the Commission decisions in *Company X v Switzerland* (1979) Appl 7865/77, 16 DR 85 (deciding that a corporate body with commercial goals – in this case a printing company – cannot enjoy or exercise the rights referred to in Art 9(1)); *Vereniging Rechtsvinkels Utrecht v the Netherlands* (1986) Appl 11308/84, 46 DR 200; *Verein 'Kontakt-Information-Therapie' and Siegfried Hagen v Austria* (1988) Appl 11921/86, 57 DR 81 (both decisions denying non-commercial associations with idealistic, albeit non-religious, goals the enjoyment of the right to freedom of conscience under Art 9(1)). In the last-mentioned decision, the Commission also held that the right in Art 3(1) not to be subjected to degrading treatment or

It could be strongly argued that while the concepts of, and rationales for, freedom of expression, association and assembly are sufficiently broad to be used by collective entities, the notion of, and rationale for, 'respect for private and family life, home and correspondence' are not. This can have been the view taken by the European Court of Justice (ECJ) when it held that 'the protective scope' of Art 8 'is concerned with the development of man's personal freedom and may not therefore be extended to business *premises*'.[669] However, the reference to business 'premises' only (ie, to a type of location as opposed to a type of activity or organisation) casts some uncertainty over whether or not the ECJ views Art 8 as incapable of extending to business enterprises or collective bodies generally. This uncertainty is heightened by ambiguous wording in other decisions reached by the ECJ.[670] The view taken in *Hoechst* regarding the inapplicability of Art 8 to cases involving interference that occurs on business premises, has not been followed by the ECtHR. The latter (along with the ECommHR) has held that a police search of a lawyer's office constituted an unjustified interference with the lawyer's 'private life' and 'home', and thereby a violation of Art 8.[671]

According to the ECtHR, the 'essential' object of Art 8 is 'to protect the individual against arbitrary interference by the public authorities in his private or family life'.[672] In stating this, the Court has probably not shut off all possibility of Art 8 also being used to protect collective entities from such interference, particularly

---

(Cont.)

punishment is by its 'very nature not susceptible of being exercised by a legal person such as a private association': 57 DR 81, 88.

669 Joined Cases 46/87 & 227/88 *Hoechst v Commission of the European Communities* [1989] ECR 2859, 2924 (emphasis added); affirmed in Case 85/87 *Dow Benelux v Commission of the European Communities* [1989] ECR 3137, 3157, and Joined Cases 97 to 99/87 *Dow Chemical Ibérica and Others v Commission of the European Communities* [1989] ECR 3165, 3185-3186. The ECJ in *Hoechst* added on a more general note that 'in all the legal systems of the Member States, any intervention by the public authorities in the sphere of private activities of any person, *whether natural or legal*, must have a legal basis and be justified on the grounds laid down by law, and, consequently, those systems provide, albeit in different forms, protection against arbitrary or disproportionate intervention. The need for such protection must be recognised as a general principle of Community law': *ibid*, 2924 (emphasis added). The Court did not specifically address whether or not this legality principle applies when the alleged intervention in the private affairs of a legal person is occasioned by the processing of data on the entity. In my view, the notion of 'intervention' need not relate exclusively to physical intrusion; a decision taken on the basis of information on a person and which detrimentally affects him/her/it would constitute an 'intervention'.

670 See, eg, Case 136/79 *National Panasonic (UK) Ltd v Commission of the European Communities* [1980] ECR 2033, 2057, para 19, in which the ECJ seems to embrace the view that Art 8 may apply, in theory at least, to legal persons (ie, '... in so far as it [Art 8] applies to legal persons ...').

671 *Niemitz v Germany* (1992) A 251-B. See also *Halford v United Kingdom* (1997) RJD 1997-III, 1004 (confirming that telephone calls made from business premises may be covered by the notion of 'private life' in Art 8(1)).

672 *Case 'Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium'* (1968) A 6, para 7. See also *Marckx v Belgium* (1979) A 31, para 31; *Airey v Ireland* (1979) A 32, para 32.

if protection of the collective entity is viewed as providing fuller protection of the individuals who make up the body. This view is explored in more detail in subsequent chapters.

Whether or not collective entities may invoke the protection of Art 8 will depend largely on how the ECtHR interprets the notions of 'private life', 'home' and 'correspondence'. The last-mentioned notion appears relatively easy to apply to legal persons; the notions of 'private life' and 'home' do not, however, and may restrict the literally broad ambit of 'correspondence' accordingly. Nevertheless, the ECtHR has been wary of exhaustively and narrowly defining such notions.[673] In particular, it has made clear that these notions should not be viewed as strictly relating to the domestic sphere but as capable of embracing business activities too.[674] Also noteworthy is its observation in *Niemitz* that '[r]espect for private life must ... comprise to a certain degree the right to establish and develop relationships with other human beings'.[675] Insofar as collective entities are a manifestation of individuals establishing and developing 'relationships with other human beings', one can strongly argue these entities should be given protection under Art 8. In the event of such protection being given, it is nevertheless likely that State Parties would also be accorded greater scope for interference pursuant to Art 8(2). The Court foreshadowed this in *Niemitz* when it commented that entitlement to interfere under Art 8(2) 'might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case'.[676]

Finally, we should not overlook the possible relevance of other ECHR provisions (besides Art 8) to the data protection interests of collective entities. The processing of data on certain types of collective entities could conceivably breach Arts 9 (freedom of religion), 10 (freedom of expression) or 11 (freedom of association) if the processing prevents the entities or their individual members from exercising their rights under those provisions.[677]

---

673 See generally Bygrave, *supra* n 102, 255ff.

674 See, eg, *Niemitz*, *supra* n 671, paras 29–33. The Court noted particularly that the equally authentic French text of Art 8(1) uses the term 'domicile' for the term 'home', and that the former term has a 'broader connotation' than the latter: *ibid*, para 30. See also *Chappell v United Kingdom* (1989) A 152-A, in which the Court accepted the applicability of Art 8 to a police search-and-seizure operation directed exclusively against the applicant's business. The latter business was organised as a company operation, though the company as such appears to have consisted of little more than the applicant himself. Note too the statement of the (UN) Human Rights Committee that 'home' in Art 17(1) of the ICCPR refers to 'the place where a person resides or *carries out his usual occupation*': General Comment 16 of 23.3.1988 (UN Doc CCPR/C/21/Add.6), para 5 (emphasis added).

675 *Niemitz*, *supra* n 671, para 29. See also the ECommHR decision in *X v Iceland* (1976) Appl 6825/74, 5 DR 86, 87.

676 *Niemitz*, *supra* n 671, para 31.

677 See further Korff, *supra* n 16, 14. Korff cites the ECommHR decision in *Church of Scientology of Paris v France* (1995) Appl 19509/92 (unpublished) as support for this possibility.

9.3 Official Motives for Giving Data Protection Rights to Collective Entities

Little material exists setting out why Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland have enacted data protection statutes expressly regulating the processing of data on certain kinds of collective entities (primarily legal persons) as well as individuals. The reasons found in the preparatory documents and explanatory memoranda accompanying the statutes tend not to have been articulated in great detail or with much precision. These comments apply *a fortiori* with regard to the EC Directive on telecommunications privacy: no specific reasons are given in the Directive or its *travaux préparatoires* as to why the interests of legal persons are expressly safeguarded by certain of its provisions.

However, evidence exists to indicate that extension of protection to data on legal persons can have occurred in at least some cases in order to provide more complete data protection for *both* legal and natural persons. It is misleading to claim for certain, as Chamoux seems to do, that those laws extending protection to legal person data do so only 'in order to better protect physical persons against an attack on their private life'.[678] Some documents point to a broader rationale which at least leaves open the possibility that the interests of collective entities as such have been taken into account. For example, the government Bill for Austria's *Data Protection Act* of 1978 states that data on legal persons are protected because 'the bulk of information on a legal person is ... able to be traced back to information about a physical person', *and* because 'data processing constitutes a threat ... to collective interests'.[679] Similarly, commentary to the corresponding government Bill for the Swiss federal *Data Protection Act* sets out as the main reason for protecting data on both legal and natural persons the fact that data processing can injure the rights of both types of person.[680] One can also read into some of the preparatory works for the Danish data protection legislation a concern about the effects of computerised data processing for both natural and legal persons.[681]

In these documents, we see intimations of a belief that the social, political and economic implications of modern IT are so pervasive that they threaten the interests of not just individuals but also collective entities. This belief is best illustrated in the

678 Chamoux, *supra* n 636, 80. The same claim is made in Bancilhon *et al*, *supra* n 636, 33.

679 '[E]in Gruppenschutz ... [scheint] gerechtfertigt, weil sich einerseits die Mehrheit der Informationen über eine juristische Person auch wiederum auf Informationen über eine physische Person zurückführen lässt, und die Datenverarbeitung andererseits eine Bedrohung auch von Kollektivinteressen darstellt': *Regierungsvorlage* in *72 der Beilagen zu den stenographischen Protokollen des Nationalrates XIV.GP, 17.12.1975*, 22. See also W Dohr, H-J Pollirer & EM Weiss, *Datenschutzgesetz* (Vienna: Manzsche Verlags- und Universitätsbuchhandlung, 1988), 15–16.

680 *Botschaft zum Bundesgesetz über den Datenschutz (DSG)*, 23.3.1988, 20.

681 See espec *Delbetænkning om private registre*, *supra* n 471, 38.

following remark made by Steinmüller in one of his first articles broaching the topic of 'group data protection' ('Gruppendatenschutz'):

> 'Because data processing ... embraces the whole of society, like a second nervous system, it is not just the single individual who counts as one of those affected. Rather, groups and institutions are also affected.'[682]

Expressed alternatively, we see here a belief that individuals and collective entities face, as it were, a common enemy. From this belief, it is only a short step to claim the need for a common defence.

Given their relatively open, processual character, it is not surprising that data protection laws (or their core principles) have been perceived as suitable constituents of such a defence, especially in the 1970s when there was perhaps less dogmatic certainty about the nature and limits of data protection. Manifestations of this logic are found not just in the above-cited statements by Austrian, Swiss and Danish legislators but also in the report of the first body appointed by the British Parliament to investigate privacy problems – the Younger Committee – which claimed that most of the principles it canvassed in relation to the handling of personal information by computers,[683] should apply equally to the handling of non-personal, commercial information, including chemical formulae or sales records.[684] The potential breadth of the defence offered by data protection law is further illustrated by the first *Data Protection Act* of Hessen which, as already noted, sought not only to protect data on both natural and legal persons but also to uphold the informational balance of power between the executive and legislature.

Nevertheless, the fact that the world's first national data protection law – Sweden's *Data Act* of 1973 – covered only the *computerised* processing of data on *individuals* shows that fear in the early 1970s of the repurcussions of computer technology did not always lead to data on collective entities being legislatively protected to the same extent as data on individuals.[685] Yet the data protection interests of legal persons (more specifically, business enterprises – 'företag') were not overlooked entirely in Sweden. For example, explicit account was taken of such interests in the context of credit reporting.[686]

---

682 'Weil Datenverarbeitung ... die ganze Gesellschaft erreicht und erfasst, als gleichsam zweites Nervensystem, ist nicht nur das einzelne Individuum zu den Betroffenen zu zählen. Vielmehr sind auch Gruppen und Institutionen betroffen': Steinmüller, 'Fragestellungen der internationalen Datenschutzdiskussion', *supra* n 640, section 4.3.2 (no pagination).

683 These principles being similar to the core principles of data protection laws: see Younger Committee, *supra* n 642, 183–184.

684 *Ibid*, paras 579 & 591.

685 See further section 9.5.

686 See *Kreditupplysning och integritet*, SOU 1972:79, espec chapt 11, and the resultant *Credit-Reporting Act* (*Kreditupplysningslag*, SFS 1973:1173), presented in Chapter 10 (section 10.2).

In Denmark too there was explicit recognition of the need to protect information on business enterprises in a credit-reporting context. The *Delbetænkning om private registre* notes that the interests of both individuals and private enterprises are potentially affected by credit-reporting activities, and that it is 'legal-technically difficult' ('retsteknisk vanskelig') to distinguish between data on individuals and data on private enterprises in such a context.[687] Recognition of the data protection interests of legal persons in the context of credit reporting seems also to have been a major factor in the decision to give express protection to legal person data under Luxembourg's data protection legislation.[688]

Regarding the Norwegian decision to include legal person data within the ambit of the PDRA, several reasons for this decision were given by the Norwegian Ministry of Justice. To begin with, the Ministry claimed that were the legislation to cover data on physical persons only, the result would be

> 'a register of business enterprises or, for example, a register of ships falling outside the Act if all the enterprises or shipowners are non-personal companies (share companies), while they would be regulated by the Act if one of the registered enterprises is personally owned, or if, for example, there is registered in relation to a share company who its administrative director is.'[689]

The Ministry viewed the result set out above as a 'weakness' with data protection legislation that covers data on natural persons only. The Ministry did not elaborate on why it viewed the result as a weakness. Perhaps it disliked the discriminatory and apparently fortuitous ambit of protection provided by such legislation. The discriminatory aspect seems to be particularly hard to accept when small businesses are involved. And it is perhaps not surprising to find that coverage of legal person data by data protection laws has occurred so far in countries where small business enterprises predominate.[690]

An apparent concern for small business, though, was not the only factor behind the Norwegian decision to extend data protection to legal persons. The Ministry of

---

687 *Supra* n 471, 41.

688 See *Rapport de la Commission spéciale* (27.2.1979), set out in Chambre des Députés, *Projet de loi réglementant l'utilisation des données nominatives dans les traitements informatiques*, No 2131, Session ordinaire 1978–1979 (1.3.1979), 9.

689 '[E]t bedriftsregister eller f eks et skipsregister faller utenfor loven dersom samtlige bedrifter/redere er upersonlige selskaper (aksjeelskaper), mens de reguleres dersom én av bedriftene i registeret er personlig eiet, eller det f eks i forbindelse med et aksjeselskap også er registrert hvem som er administrerende direktør': Ot prp 2 (1977–78), *Om lov om personregistre mm*, 25–26.

690 As Helge Seip, former head of the Norwegian Data Inspectorate, writes: 'in countries where small undertakings play an important role for the economy and for the employment situation in most areas, it seems unnatural and 'artificial' to draw sharp lines of division between the undertaking owned by an individual, and business organized in the form of stockholding companies, foundations, cooperatives etc'. See Seip, *supra* n 648, 106.

Justice argued that although it would be 'a logical alternative' to limit the scope of the proposed Norwegian data protection Act to 'personal information in the sense of information on private life' ('private forhold'), it found difficulties in determining exactly what should qualify as 'private life'.[691] It also found that 'in the light of the content of the proposed provisions, it is in many respects logical to include legal persons'.[692] Though ambiguous, this last statement seems to embrace the view that the principles of data protection law are able to serve the interests of legal persons as well as those of individuals. This view is examined in more detail in Chapters 12–14. A final factor was that Norway would not be alone in including legal persons in its data protection legislation.[693]

At the same time, the Ministry took the view that data on natural persons should not be treated in every respect like data on legal persons as significant public interest attaches to corporate activities. Moreover, the Ministry opined that corporations generally have greater ability to look after their interests than individuals do.[694] Many people would argue it is precisely for these reasons that legal persons should *not* be given any rights under data protection laws. The Ministry, however, felt that the necessary distinctions could be maintained by Norway's data protection authority when exercising its discretionary powers pursuant to the Act. The Ministry also took the view that the Act should distinguish at certain points between business entrepeneurs ('næringsdrivende') and other persons.[695]

Another important factor in the decision of some countries to provide data protection for both legal and natural persons has been the pre-existing legal traditions of these countries. A fundamental premise of the Austrian legal system, for example, is that legal persons are to be treated as far as possible in the same way as natural persons. In this regard, special note should be made of Art 26 of the Austrian *Civil Code*[696] which states in part that legal persons enjoy as a rule the same rights as individuals *vis-à-vis* others.[697]

Much the same situation pertains in Switzerland. Article 53 of the Swiss *Civil Code*[698] provides that legal persons are capable of possessing all legal rights and duties that do not require possession of the 'natural' characteristics of individuals,[699]

---

691 Ot prp 2 (1977–78), 26.

692 '... etter innholdet av de bestemmelser som foreslås er det på mange måter logisk å innbefatte juridiske personer': *id*.

693 *Id*.

694 *Id*.

695 See, eg, ss 18 & 19 of the PDRA presented in Chapter 10 (section 10.1.2).

696 *Allgemeines Bürgerliches Gesetzbuch vom 1 Juni 1811*.

697 Article 26 reads: '... Im Verhältnisse gegen Andere geniessen erlaubte Gesellschaften in der Regel gleiche Rechte mit den einzelnen Personen'.

698 *Schweizerisches Zivilgesetzbuch vom 10 Dezember 1907*.

699 Article 53 reads: 'Die juristischen Personen sind alle Rechte und Pflichten fähig, die nicht die natürlichen Eigenschaften des Menschen, wie das Geschlecht, das Alter oder die Verwandschaft zur notwendigen Voraussetzung haben.'

while Art 52 of the Code extends a 'right of personality' ('Recht der Persönlichkeit') to legal persons.[700] This right of personality, which also embraces individuals,[701] provides one of the main legal bases for the federal *Data Protection Act*.[702] It is also the main legal basis for protecting various types of confidential information under the Swiss *Penal Code*.[703]

Similarly, an important reason behind the Danish decision to provide data protection for both legal and natural persons under the *Private Registers Act* was that both types of persons have already been given, wherever possible, the same rights to confidentiality and security under the Danish *Penal Code*.[704]

Also the Italian decision to provide express safeguards for data on collective entities seems to have been grounded largely on the fact that such entities have already been accorded a right to 'personal identity' in Italian law. In view of such a right, it was felt that a refusal to extend data protection to these entities would be illogical.[705]

At the same time, Giovanni Buttarelli notes a second major reason for the Italian decision; namely, a concern to enhance the general transparency of data processing and, concomitantly, the diffusion of knowledge for the benefit of wider society:

> '[I]n an economic system which aspires to greater diffusion of knowledge, it would have been unacceptable to support the 'secrecy' of databanks and the logical ownership of knowledge rather than a transparency in which the interest in the quality of information constitutes a benefit for the entire society and not just for the data controllers/users.'[706]

---

700 See also U Belser, 'Art. 3', in U Maurer & NP Vogt (eds), *Kommentar zum Schweizerischen Datenschutzgesetz* (Basel/Frankfurt am Main: Helbing & Lichtenhahn, 1995), 75–76.

701 See Arts 27–28 of the Code.

702 M Buntschu, 'Art. 1', in Maurer & Vogt, *supra* n 700, 20ff. For criticism of giving data protection rights to legal persons on the basis of their 'allgemeine Persönlichkeitsrecht' under Art 53 of the Civil Code, see JT Peter, *Das Datenschutzgesetz im Privatbereich* (Zürich: Schulthess Polygraphischer Verlag, 1994), 106ff and references cited therein.

703 *Schweizerisches Strafgesetzbuch vom 21 Dezember 1937*. See, eg, Art 162 of the Code (dealing with protection of trade secrets).

704 'Denmark: Legal Person Coverage' (1986) 9 *TDR*, no 2, 30. See also *Delbetænkning om private registre*, *supra* n 471, 21 & 59. The latest consolidated version of the *Penal Code* is from 2001 (*lovbekendtgørelse nr 808 of 14 September 2001*).

705 See G Buttarelli, *Banche dati e tutela della riservatezza: La privacy nella Società dell'Informazione* (Milan: Giuffrè Editore, 1997), 422, 419 and Korff, *supra* n 16, 32.

706 '[I]n un sistema economico che aspira alla diffusione sempre più ampia dei dati conoscitivi, sarebbe risultato inaccettabile assecondare la 'segretezza' delle banche dati e la logica proprietaria della conoscenza, anziché una transparenza nella quale l'interesse alla qualità delle informazioni costituisce un bene dell'intera collettività più che dei soli fruitori dei dati': *ibid*, 422. The reference to information quality appears to embrace more than just a concern to ensure that information is valid, relevant, etc but that it is processed in conformity with all of the basic principles of data protection set down in Art 6 of the EC Directive and Art 9 of the Italian Act.

This point has seldom been prominent in discourse on the issue of data protection rights for collective entities. Yet it is important and one which is revisited further on this Part. Somewhat paradoxically, it runs counter to one of the main claims advanced as justification for *refusing* the extension of data protection rights to collective entities; namely, that such an extension will lead to a reduction in the transparency of the entities' operations.[707]

Discussion on the rationale for extending the ambit of data protection laws to cover data on legal persons has also focused on the need to resolve what are usually termed the 'mixed file' and 'small business' problems. Explicit references to these problems, however, are sparse in the preparatory works for the statutes in focus here. The 'mixed file' problem concerns the fact that many data registers are organised in such a way that they do not distinguish between information on individuals and information on legal persons, with the result that information on both types of persons is intermingled. Moreover, this intermingling can occur not just at an organisational level. It can also occur more intrinsically, at the level of informational content, because of the fact that some information, which relates *prima facie* to legal persons, is also capable of being linked to particular individuals. This sort of information may be termed 'double-edged'. Information on small legal entities is often of this character. It has been alleged there is a risk of this sort of information being processed without regard to data protection laws if the latter only protect data on individuals.[708] A further allegation is that limiting protection to data on individuals necessitates an expensive and difficult reorganisation of 'mixed file' registers so that information on individuals is segregated from information on legal persons.[709]

As for the so-called 'small business' problem, the background to this is that some small businesses are run as incorporated enterprises while others are not.[710] Those businesses that are incorporated have, of course, the status of a legal person; those that are not, maintain the status of their physical owner(s). It is claimed that if data protection legislation covers only data on physical persons, the individual whose business is not accorded legal person status is given rights under the legislation, while an individual whose business is accorded legal person status may not exercise those rights on behalf of the business, even though the business might be of the same magnitude and type as the former business.[711]

---

707 See further Chapter 13 (section 13.2).

708 See, eg, comments by Edmond Toussing, former head of Luxembourg's data protection authority, cited in GR Pipe, 'Data Protection Implementation – Accomplishments amid Frustration' (1980) 3 *TDR*, no 7, 10.

709 See, eg, PE Cole, 'New Challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws' (1985) 17 *NYU J of Int Law and Politics*, 893, 945.

710 The adjective 'small' refers primarily to the number of individuals running or attached to a business, rather than to the size of a business' assets or scale of operations.

711 See, eg, Chamoux, *supra* n 636, 74–75; Bancilhon *et al*, *supra* n 636, 8.

Finally, mention should be made of North American claims – described, discussed and largely dismissed in Chapter 6 (section 6.3.2) – that enactment of many European data protection laws has been motivated, at least in part, by economic protectionism. These claims tend to focus on those laws that explicitly cover legal person data. Such laws, it is argued, are strong proof of protectionist concerns because they cannot have been passed simply in order to protect the right of privacy.[712] This argumentation seems to rest upon two assumptions: first, that the purpose of 'pure' data protection laws is only to safeguard privacy; and secondly, that privacy as a concept and legal right can only embrace natural/physical persons. As Chapters 7 and 12 show, both assumptions are questionable if not fallacious. In any case, the argumentation ignores the variety of non-protectionist motives (listed above) for protecting data on legal persons.

9.4 Opposition to Data Protection Rights for Collective Entities

Opposition to giving data protection rights to collective entities (primarily legal persons) has far outweighed enthusiasm for giving them such rights. This opposition has been manifest since at least the early 1970s. As noted above, the first piece of national data protection legislation, Sweden's *Data Act* of 1973, expressly covered data on individuals only. This is also the case with the second piece of such legislation, the US federal *Privacy Act* of 1974.

The drafters of both these Acts appear to have viewed them as protecting values that could only apply to individuals. The basic aim of the Swedish Act was expressed in terms of protecting 'personal integrity' ('personlig integritet'),[713] the aim of the US Act in terms of safeguarding 'privacy'.[714] In Sweden, the concept of personal integrity seems largely to have been explicated in connection with individuals' needs only,[715] though some literature exists on the need to protect 'business enterprise integrity' ('företagsintegritet').[716] Little has been written in Sweden specifically on the extent to which the interests covered by the concept of personal integrity are

712 Pinegar, *supra* n 426, 188; Grossman, *supra* n 426, 12, 20; McGuire, *supra* n 426, 4.

713 See espec s 3 of the Act.

714 See espec the preamble and s 2(b) of the Act.

715 See generally the analysis of the concept in S Markgren, *Datainspektionen och skyddet av den personliga integriteten* (Lund: Studentlitteratur, 1984), 35–54; SOU 1993:10, 150ff; and SOU 1997:39, Appendix 4.

716 See, eg, K Ivanov, *Systemutvekling och rättssäkerhet: Om statsförvaltningens datorisering och de långsiktiga konsekvenserna för enskilda och företag* (Stockholm: Svenska Arbetsgivarföreningen, 1986), espec 12; N Rydén, *Företagsintegriteten i datasamhället* (Stockholm: Svenska Arbetsgivareföreningen, 1986); J Freese & S Holmberg, *Datasäkerhet* (Stockholm: Affärsinformation, 1989, 2nd ed), 26–28.

similar to the interests covered by the concept of 'företagsintegritet', but the general feeling probably is that there is little or no similarity.[717]

The failure in the USA to give legal persons data protection rights under the federal *Privacy Act* mirrors the lack of judicial enthusiasm there for extending to corporations legal rights to privacy as such. The bulk of US judicial authority as it presently stands is against allowing corporations to bring legal actions based on breach of their privacy.[718] Reasons for this attitude are: that corporations do not have human emotional traits;[719] lack of judicial precedent;[720] and the availability of alternative remedies.[721]

As an aside, however, privacy law in the USA is fairly volatile and it would not be at all surprising to see in the future an increasing number of judges there extending certain rights to private corporations under the rubric of 'privacy' protection. Judicial precedent for such a development already exists, with some State courts recognising the possibility of corporations successfully asserting privacy actions.[722] The US Federal Court has also held that industrial espionage that cannot

---

717 See, eg, P Seipel, 'Transnational Data Flows', in KE Johansson (ed), *Internationell företagsdataöverföring i juridisk belysning* (Stockholm: Sveriges Industriförbundets Förlag, 1981), 71–72; 'Sweden separates Legal Persons and Protection of Individuals' (1980) 3 *TDR*, no 7, 7; SOU 1993:10, 372; SOU 1997:39, 200. However, Jan Freese, one of Sweden's foremost experts on data protection issues, has favoured data protection rights for legal persons. See, eg, his comments in *Statistik och integritet*, SOU 1994:65, Part 2, 24, and in 'Rapport om skyddet för enskilda personers privatliv – ett mer samlat grepp?', Report for the Swedish Ministry of Justice, delivered 15.3.1995, 3. The latter report is also published in English with the title, 'Report on the Protection of the Private Life of the Individual – A More Comprehensive Grasp?'.

718 See, eg, *Oasis Nite Club, Inc v Diebold, Inc*, 261 F Supp 173, 175–76 (1966); *Vassar College v Loose-Wiles Biscuit Co*, 197 F 982 (1912); *Maysville Transit Co v Ort*, 177 SW2d 369, 370–71 (1944); *Copley v Northwestern Mutual Life Insurance Co*, 295 F Supp 93 (1968); *Ion Equipment Corp v Nelson*, 110 Cal App 3d 868, 878 (1980); *CNA Financial Corp v Local*, 515 F Supp 942, 946 (1981). See also *Restatement (2d) of Torts* (St Paul, Minneapolis: American Law Institute Publishers, 1981), § 651 I, comment c ('Corporations, partnerships and unincorporated associations have no privacy rights and no cause of action for invasion of privacy').

719 See, eg, the decisions in *Vassar*, *Maysville* and *Ion Equipment*.

720 See, eg, *Ion Equipment*.

721 See, eg, the decisions in *Maysville*, *Ion Equipment* and *Copley*. For detailed analyses of these and other US judicial decisions against recognising corporate privacy rights, see AL Allen, 'Rethinking the Rule Against Corporate Privacy Rights: Some Conceptual Quandries for the Common Law' (1987) 20 *John Marshall L Rev*, 607–639; WC Lindsay, 'When Uncle Sam Calls does Ma Bell Have to Answer? Recognizing a Constitutional Right to Corporate Informational Privacy' (1985) 18 *John Marshall L Rev*, 915–935; M Meissner, *Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht* (Frankfurt: Peter Lang, 1998), espec 13–17, 107–127; and CH Lowell, 'Corporate Privacy: A Remedy for the Victim of Industrial Espionage' (1972) 4 *Patent L Rev* (now *Intellectual Property L Rev*), 407–449.

722 See *Midwest Glass v Stanford Dev Co*, 339 NE2d 274, 278 (1975) (corporate privacy claim allowable if sufficient degree of injury); *Dayton Newspapers, Inc v City of Dayton*, 259 NE2d 522, 534 (1970) (privacy right applicable to individuals, corporations, associations, institutions and public officials); *Belth v Bennett*, 740 P2d 638 (1987) (corporations may claim right of privacy under Article II (s 10) of the Montana State Constitution). See also *H & M Assoc v City of El Centro*, 109 Cal App 3d 399

be anticipated, detected or prevented by reasonable means is actionable as a violation of 'commercial privacy'.[723] Some controversy exists over whether corporations are given privacy rights under the US Constitution. The decision of the US Supreme Court in *United States v Morton Salt*[724] has been cited as authority for the proposition that corporations cannot have a constitutional right to privacy.[725] The decision in *Morton Salt*, however, does not hold that corporations cannot enjoy any right to privacy; it holds that corporations cannot 'plead an *unqualified* right to conduct their affairs in secret' and that corporations 'can claim *no equality with individuals* in the enjoyment of a right to privacy'.[726] It has been strongly argued that, far from being denied privacy protection because they lack legitimate privacy interests, corporations are granted privacy rights under the Constitution as long as these are 'consistent with the governmental right to police corporate behaviour, and, to a lesser extent, with the reduced expectation of privacy in a publicly-created entity'.[727] There is, for instance, solid judicial authority for the proposition that corporations are protected from unreasonable searches and seizures under the Fourth Amendment to the Constitution,[728] though it is less clear whether or not corporations have a constitutional right to withhold disclosure of corporate information.[729]

Despite these judicial moves towards giving corporations privacy rights, there has been no move by legislators in the USA (at either federal or state level) to give data protection rights to legal persons or other collective entities. Shifting focus away from the USA, one finds that the overwhelming majority of data protection statutes presently in force in other countries cover data relating only to individuals.

(Cont.)
(1980) (limited partnerships entitled to right of privacy to prevent public disclosure of embarrassing private facts about them).

723 See *E I Dupont de Nemours & Co v Christopher*, 431 F2d 1012 (5th Cir 1970).

724 338 US 632 (1950).

725 See, eg, the decision in *Oasis Nite Club*, *supra* n 718.

726 *Supra* n 724, 652 (emphasis added).

727 Lindsay, *supra* n 721, 926.

728 *Hale v Henkel*, 201 US 43, 76 (1906); *G M Leasing v United States*, 429 US 338, 353 (1977); *Civil Aeronautics Board v United Airlines*, 542 F2d 394, 399 (7th Cir 1976); *Dow Chemical Co. v United States*, 749 F2d 307, 314 (6th Cir 1984). But corporations do not have a right under the Fifth Amendment against self-incrimination: *Hale v Henkel*, 201 US 43, 75–76 (1906); *United States v White*, 322 US 694, 698–700 (1944); *Bellis v United States*, 417 US 85, 90–92 (1974).

729 The Supreme Court has held that corporations are able to assert the constitutional rights of their *members* to resist disclosure of information on these members compelled by government agencies: See, eg, *California Bankers Association v Schultz*, 416 US 21 (1974). Yet, to my knowledge, the only judicial authority for recognising a constitutional right to nondisclosure of *corporate* information is a panel decision of the US Court of Appeals for the District of Columbia: *Tavoulareas v Washington Post*, 724 F2d 1010 (DC Cir, 1984). For criticism of the decision and discussion of its implications, see Lindsay, *supra* n 721, 921–926. The decision has little precedential value.

Moreover, with one exception,[730] all of the hitherto most influential elaborations of data protection principles worked out at an international level are drafted to give express protection to data on individuals only. However, none of these instruments expressly exclude the possibility of individual countries extending protection to data on some types of collective entities. Article 3(2)(b) of the CoE Convention goes the furthest in this regard by providing that State Parties may apply the Convention's provisions to information on 'groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality'. The other international instruments are more reserved. Paragraph 10 of the UN Guidelines states that '[s]pecial provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals'. By contrast, neither the EC Directive nor the OECD Guidelines contain such an options clause, but they do not prohibit States from giving data protection rights to collective entities.[731]

It is also important to note that some of the countries which have had data protection legislation covering data on collective entities have recently abolished or reduced such coverage. Iceland's *Act on the Protection of Individuals with regard to Processing of Personal Data* of 2000 dispenses completely with express protection for such data. This is also the case with Norway's *Personal Data Act* of 2000, though allowance is made for protection for legal person data to be introduced in the future with respect to credit-reporting activities (s 3(4)). As for the Danish *Personal Data Act* of 2000, this retains some safeguards for data on 'enterprises' ('virksomheder mv') but only insofar as these data are processed by a credit-reporting agency or used for the purposes of blacklisting (ss 1(3), 50(1)(3)). By contrast, Austria's *Data Protection Act* of 2000 retains the full ambit of protection for data on collective entities which was provided under the equivalent legislation from 1978. It would appear that Luxembourg will also follow Austria in this regard,[732] though at the time of writing some uncertainty surrounds the final content of the Grand Duchy's coming legislation.

Why are data on legal persons and other collective entities excluded from explicit protection under the majority of data protection instruments? At least six factors need to be taken into account. These factors are sketched briefly below. More detailed analysis of them occurs in Chapters 11–14.

---

730 This is the EC Directive on telecommunications privacy and its successor, the coming Directive on privacy of electronic communications. See further Chapter 10 (section 10.2).

731 Recital 24 of the Directive states that 'legislation concerning the protection of legal persons with regard to the processing of data which concern them is not affected by this Directive'.

732 See *Projet de loi relatif à la protection des personnes à l'égard du traitements des données à caractère personnel* (issued October 2000), espec Arts 1 & 2(b). See also the explanatory memorandum to the Bill (<http://www.etat.lu/SMA/protdon/expose.htm>), espec section II.2.

One factor is that many experts in the field of data protection are of the view that the main values and interests served by data protection laws are only applicable to individuals.[733] As noted above, this factor appears to have played a major role in the decisions of Sweden and the USA not to extend their respective data protection laws to cover the handling of legal person data. It also goes a long way to explaining the decision to drop express protection for legal person data from the new Norwegian data protection legislation.[734]

Secondly, there is a view that many collective entities, particularly corporations, do not need data protection rights because the individuals who constitute them enjoy such rights already,[735] or because the data protection interests of the entities as such are protected sufficiently under other legislation.[736] Accompanying this view is no doubt a perception of many collective entities as robust bodies capable of looking after themselves to a greater extent than are individuals.[737]

Another factor is the natural disinclination of governments to introduce rules that might further curtail their agencies' ability to process information on any sorts of entities.[738]

Fourthly, it is feared that expanding the class of data subjects which are given rights under data protection laws to embrace collective entities will expand the potential of these laws to restrict transborder flows of data that are important for international business transactions.[739]

Fifthly, uncertainty exists over the ways in which extension of data protection rights to collective entities would affect corporate activities, market-place

---

733 See, eg, J Michael, *The Politics of Secrecy* (Harmondsworth: Penguin Books, 1982), 124; Bull, *supra* n 481, 92; Peter, *supra* n 702, 106ff. See further Chapter 12 (section 12.2) and references cited therein.

734 See Ot prp 92 (1998–99), 26; NOU 1997:19, 53–54.

735 A view put forward in, eg, Bull, *supra* n 481, 92–93, and Steinmüller, *supra* n 47, 468, 470 & 673. However, Steinmüller argues that *groups* of persons (presumably those without formal legal status independent of the persons constituting them) need data protection: *ibid*, 469–470, 656ff. Steinmüller indicates also that small legal persons might need protection against the 'informational hunger' ('Informationshunger') of large enterprises: *ibid*, 673. Similarly, he expresses concern about the 'informational imbalance' ('Informationsungleichgewichte') between small and medium-sized business enterprises on the one hand and large enterprises on the other: *ibid*, 468, 470–471, 674.

736 The view of, eg, Peter Nobel: see Nobel, 'Gedanken zum Persönlichkeitsschutz juristischer Personen', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Verlag Stämpfli & Cie, 1990), 411, 425. We also find the view embraced in, eg, NOU 1997:19, 54; *Behandling af personoplysninger*, Bet nr 1345 (Copenhagen: Statens Information, 1997), 167.

737 See, eg, the comments of the Norwegian Ministry of Justice, *supra* n 694 and accompanying text.

738 A point elaborated upon in relation to Australian federal governments in Bygrave, *supra* n 5, 128–153. See also the discussion in Chapter 7 (section 7.3).

739 See further Chapter 11 (section 11.2). Refer also to Chapter 6 (section 6.3.2).

competition and the operation of other branches of the law.[740] This uncertainty is compounded by the paucity of studies on the relationship between data protection and other fields of activity, and on the actual consequences of those laws that presently provide collective entities with data protection rights. In some cases, this uncertainty gives way to specific fears. One such fear is that extending coverage of data protection laws to legal person data would decrease corporations' transparency, thus hindering public control of their activities.[741] Another such fear is that corporations will use their data protection rights to distort economic competition between themselves.[742]

Finally, there is the trenchant opposition shown previously by major business groups to extending the ambit of data protection legislation to cover legal person data. One manifestation of this opposition occurred during debate in 1976 and 1977 on the initial proposal by French legislators to enact data protection legislation covering data on legal as well as natural persons.[743] Under pressure from business groups, the Bill was first amended to limit protection to data relating to non-profit bodies (in addition to individuals), and then amended again so as to exclude protection of data relating to *any* kind of legal persons.[744] Most opposition to the proposal came evidently from IBM, which feared that its corporate competitors would be able to access information stored by it. Similarly, insurance companies and the Bank of France feared that they would run into difficulties in keeping secret their data on the small and medium-sized companies with which they dealt.[745]

Just a few years earlier, (West) German proposals to enact national data protection legislation covering data on both legal and natural persons had also met with opposition from business groups. This opposition seems to have been grounded on a variety of arguments, including the claim that legal persons have no interests worthy of protection under such legislation, and the more pragmatic assertion that coverage of legal person data would lead to high administrative costs for data controllers.[746]

Luxembourg's Chamber of Commerce also came out strongly against its country's enactment of data protection legislation covering data on legal persons. It feared that companies would be forced to disclose sensitive business information to

---

740 This uncertainty was, for instance, a major factor in the hostility of the Norwegian Computer Society (*Den Norske Dataforening*) to the PDRA's coverage of legal person data. See letter of 14.10.1983 (ref 175H) to the Norwegian Ministry of Justice on possible amendments of the PDRA.

741 A fear expressed in, eg, Michael, *supra* n 733, 126; Bull, *supra* n 481, 93; and Nobel, *supra* n 736, 124–125. See further Chapter 13 (section 13.2).

742 See Chapter 11 (section 11.2) and references cited therein.

743 See *Projet de loi enregistré à la Présidence de l'Assemblée nationale le 9 août 1976*, espec s 2(2).

744 L Joinet, 'French Law in Relation to Information Privacy', in *Data Regulation: European and Third World Realities* (Uxbridge: Online Conferences Ltd, 1978), 215, 217.

745 'Focus on France' (1978) 1 *TDR*, no 1, 1, 3.

746 See generally Rumpf, *supra* n 638, 136 and references cited therein.

competitors, and was worried that the legislation would scare companies from investing and operating in Luxembourg.[747]

The International Chamber of Commerce (ICC) has stated in relation to data protection laws that it 'considers the protection of business legal persons in the same way as physical persons is inappropriate, unnecessary and harmful'.[748] It would prefer that data on business legal persons be protected under other branches of law, such as those relating to trade secrets, copyright, torts and contractual obligations.[749]

Dislike of legislation protecting data on legal persons in much the same way as data on individuals appears to be fairly typical of *large* business entities. For example, a survey carried out in 1983 of 89 major multinational corporations found all of these enterprises opposed to data protection laws that extend to legal person data.[750] However, evidence exists to suggest that some of those running small to medium-sized businesses have desired access rights to data kept on them by larger companies so that they can verify the quality of these data.[751] There is also evidence suggesting that some business organisations desire a degree of protection from State demands for information on them.[752] Moreover, in at least one case, an established business group has expressed strong support for giving data protection rights to legal persons.[753]

---

747 See *Avis de la Chambre de Commerce* (12.5.1978), set out in Chambre des Députés: *Projet de loi réglementant l'utilisation des données nominatives dans les traitements informatiques*, No 2131, Session ordinaire 1978-1979 (1.3.1979), 1, 3.

748 ICC, 'Policy Statement on Privacy Legislation, Data Protection and Legal Persons' (1984) 7 *TDR*, no 7, 425, 426.

749 *Id*.

750 Business International Corporation, *Transborder Data Flow: Issues, Barriers and Corporate Responses* (New York: Business International Corporation, 1983), 108.

751 See Chamoux, *supra* n 636, 76–77; Bancilhon *et al*, *supra* n 636, 10–11.

752 See, eg, the preface by the Swedish Employers' Association (Svenska Arbetsgivareföreningen) in Rydén, *supra* n 716.

753 See statements of the Austrian Chamber of Commerce in support of retaining express safeguards for legal person data pursuant to Austria's data protection legislation, cited in Korff, *supra* n 16, 25.

10. Existing Safeguards for Data on Collective Entities Pursuant to Data Protection Laws

10.1 Express Protection

This chapter canvasses the degree to which data protection laws currently regulate the processing of data on collective entities. It first considers the extent of such regulation pursuant to those national data protection Acts that expressly cover data on collective entities. In this analysis, some account is also taken of the ambits of those national Acts which provided express coverage of such data but which have since been repealed.

10.1.1 Legislative points of departure

The majority of the Acts in question span data processing in both the private and public sectors. Denmark was the exception here: only the *Private Registers Act* (which dealt with data processing in the private sector) explicitly covered the processing of data on collective entities. Hence, references below to the 'Danish Act' etc should be read as references to the *Private Registers Act* (hereinafter termed 'PRA') only. The primary reason for not giving express data protection rights to collective entities under Denmark's *Public Authorities' Registers Act* (which dealt with data processing by public sector agencies) appears to have been that the data protection interests of 'business enterprises' ('erhvervsvirksomheder') were perceived as being adequately safeguarded pursuant to other legislation.[754] The *Public Authorities' Registers Act* provided, however, for an extension of protection to data on 'business enterprises etc', at the instigation of the relevant Minister after consulting with the Danish Data Protection Agency (s 3(2)). Such an extension never took place.

All of the Acts expressly protect data on private corporations. Three of the Acts also expressly protect data relating not simply to legal persons in the strict sense but

754 See further *Delbetænkning om offentlige registre*, Bet nr 767 (Copenhagen: Statens trykningskontor, 1976), 154–155; cf 56–57.

also to organisations and groups without formal, legal identities separate from those of their members. Thus, Luxembourg's Act of 1979 protects data on 'any person, public or private corporate body or group of persons' (Art 2) as does its current data protection Bill (Art 2(b)). Austria's Act protects data on 'any natural or legal person or association' (s 4(3)). Italy's Act covers data on 'any natural or legal person, or any other body or association' (Art 1(2)(f); cf Art 1(2)(c)).

As for Denmark's PRA, this was interpreted by the Danish data protection authority as covering data on associations that do not have formal status as legal persons, as long as the association stands out as an 'independent entity' ('selvstændig enhed') and has some degree of internal organisation.[755] A similar situation appears to have pertained with respect to Norway's PDRA. Interpretation of the exact ambit of both pieces of legislation on this point, though, was and is complicated by a dearth of clear-cut statutory requirements in Norwegian and Danish law determining when an association ('forening' and/or 'sammenslutning') is to be considered as attaining the status of an independent legal subject.[756]

Austria's previous legislation, the *Data Protection Act* of 1978, initially covered only data on legal persons (in addition to individuals), plus data on 'associations under commercial law' ('handelsrechtliche Personengesellschaften'), such as partnerships. In 1986, however, the Act was amended to include data on associations of persons generally ('Personengemeinschaften'), including associations, such as citizen initiative groups, 'without formal legal personality in themselves'.[757] This extension was grounded on a recognition of the 'increasing social relevance' ('zunehmende gesellschaftliche Relevanz') of the activities of such groups.[758]

---

755 This and the following information from the Danish Data Protection Agency was sent to me in a letter dated 22.2.1994 written by Vibeke Ulf Jørgensen (letter no 0569; ref VUJ/mhn; journal no 1994-701-001). I did not receive an answer from the Icelandic Data Protection Commission (Tölvunefnd) on the question of whether or not it took a similar view to the interpretation of 'association' in the Icelandic legislation: see letter from the Commission, *infra* n 818.

756 See further, eg, G Woxholth, *Foreningsrett* (Oslo: Ad Notam Gyldendal, 1999, 2nd ed), 42, 45ff, 517 & 529. According to Woxholth, a 'sammenslutning' comes into existence for the purposes of Norwegian law when two or more persons gather together to undertake an activity for a common purpose and membership of the resultant association gives rise to internal rights and duties. Woxholth notes, though, that one probably cannot set down formalised requirements for membership in such associations (such as payment of membership fees, duty to participate in administration etc). Nevertheless, certain minimum criteria must also be met in terms of the *extent* and *duration* of activity pursued by such an association, and in terms of the degree of *integration/co-ordination* involved in pursuing association goals. Woxholt adds that it is difficult to describe these criteria in detail but gives several examples of groups that, in his opinion, would not normally qualify as a 'forening', and hence as a 'sammenslutning'; namely, 'ad-hoc' groups and actions (eg, demonstration processions and signature campaigns), sewing groups, card clubs and other, similar sorts of social clubs. *Ibid*, 43, 529–530.

757 BGBl No 370/1986.

758 *Regierungsvorlage 1985*, cited in Dohr *et al*, *supra* n 679, 17.

It seems that most, if not all, of the Acts in question fail(ed) to expressly safeguard data on non-organised collective entities.[759]

The data protection laws of Austria, Luxembourg, Switzerland and Italy cover *all* data on the collective entities they expressly protect. This was also the case with Norway's PDRA, but not the Danish PRA nor the 1989 Icelandic Act. The latter legislation applied only to data concerning 'private affairs, financial affairs or other affairs of individuals, institutions, companies or other legal persons that it is reasonable and natural to keep secret' (s 1(3)). Similarly, the Danish PRA only embraced 'private or financial' data on collective entities which 'may reasonably be demanded to be withheld from the general public' (s 1(1)). In practice, though, the above qualifications in the Danish and Icelandic Acts probably did not result in any great reduction in the scope of these Acts compared to the scope of the other five countries' Acts. This is not just because of the broad phrasing of the qualifications but also the practical difficulties in determining which kinds of data it is *not* reasonable to keep confidential. These difficulties are accentuated by the obvious fact that a great deal of data of an apparently trivial nature can, when combined with other data, reveal much about the private and/or financial affairs of either collective entities or individual persons.

10.1.2 DISCRIMINATORY PROVISIONS

Although the Acts in question have (had) as a common point of departure the express protection of data on designated collective entities, they tend(ed) to discriminate at various points between the scope of that protection and the scope of protection they afford(ed) for data on individuals.

Under the Italian Act, for example, no requirement exists to notify the national data protection authority of the processing of data on legal persons or other associations (Art 26(1)).[760] Such data are also exempted from the general restrictions on transborder data flow set down in Art 28.[761] Only individuals are said to be

---

759 With respect to the Italian legislation, see Buttarelli, *supra* n 705, 160. With respect to the Swiss federal legislation, see *Botschaft*, *supra* n 680, 26; Belser, *supra* n 700, 76. With respect to the Norwegian PDRA, see letter of 10.9.1980 (ref 80/580-2 AF/NM) from the Data Inspectorate to Schibsted-gruppen. Regarding the Danish PRA, see letter of the Danish Data Protection Agency, *supra* n 755.

760 This exemption is difficult to reconcile with the apparent concern of Italian legislators to increase the general transparency of data processing operations: see *supra* n 706 and accompanying text.

761 However, Art 21(3) (in conjunction with Art 31(1)(l)) empowers the Italian data protection authority to prohibit the disclosure or dissemination of these data (also across national borders) if disclosure/dissemination 'would conflict with a substantial public interest'. See also Buttarelli, *supra* n 705, 423. Nevertheless, disclosure/dissemination will ordinarily be permitted if 'the data relate to the carrying out of economic activity, subject to the applicable rules concerning trade- and business secrecy' (Art 20(1)(e)).

protected under Art 17, which prohibits certain applications of automated profiling in line with Art 15 of the EC Directive.[762] Further, with respect to processing of data on collective entities (especially business corporations), greater scope exists for derogation from the basic requirement in Art 11(1) that processing may occur only if the data subject consents. This is because consent is not required when processing 'involves data whose source are public registries, directories, agreements and papers which are open for consultation by the general public' (Art 12(1)(c)) or 'involves data related to the performance of business' (Art 12(1)(f)).[763]

Another obvious instance of discrimination occurred in the Danish PRA which did not provide collective entities access rights except in relation to information that credit-reporting agencies kept on them (s 11).[764] The reason for this restriction was to prevent collective entities from gaining knowledge of the contents of the databanks possessed by possible competitors.[765] The Bill for the Italian Act also refrained from providing access rights to collective entities for a similar reason.[766] However, this omission was reversed in the final stages of enactment such that the Act gives fairly broad access rights to collective entities as well as individuals (see Arts 13–14).

Yet another obvious point of discrimination arises with respect to the rules that place extra limits on the processing of certain types of especially sensitive data; eg, data on a person's race, religion, sexual habits and criminal record.[767] Most of these sorts of data can only relate to individuals. However, some of the listed data – primarily those concerning political activities and legal offences – are conceptually capable of being connected with collective entities. Several other listed types of especially sensitive data might also be attributed to collective entities. These are data on philosophical, religious and trade union activities/opinions. Nevertheless, the former Danish and Icelandic Acts characterised their respective lists of especially sensitive data as only concerning the 'purely private' affairs of 'individual persons' (see ss 3(2) & 4(1)) of the Danish Act and s 4(1) of the Icelandic Act). Similarly, all of the equivalent data categories in Austria's *Data Protection Act* of 2000 are described as pertaining only to 'natural persons' (Art 4(2)).

By contrast, commentary to the Bill for the Swiss legislation indicates that some such data could relate to legal persons. The commentary first notes that the data listed as sensitive (or, more accurately, as 'especially worthy of protection' ('besonders schützenswerte')) in Art 3 of the Bill concern natural persons but then notes that an

762 See Buttarelli, *supra* n 705, 425. Article 15 is described and analysed in Chapter 18 (section 18.3.1).

763 *Id*.

764 Originally, the Danish Act did not grant *any* persons a right of access, except in relation to the databanks of credit-reporting agencies. As a result of amendments to the Act in 1987 (see Law No 383 of 10.6.1987), a general right of access was inserted (s 7a) for the benefit of individuals (though it did not extend to data kept non-electronically).

765 See Blume, *Personregistrering*, *supra* n 93, 88 and references cited therein.

766 See Buttarelli, *supra* n 705, 424–425 and references cited therein.

767 See further Chapter 3 (section 3.8).

exception to this rule 'is represented by, for example, data on a philosophically oriented enterprise or on the punishment of a legal person'.[768]

This was probably also the position under the Norwegian PDRA, though there is a paucity of material addressing the issue. The fact that the PDRA referred to data on political and religious 'belief' ('oppfatning') as opposed to 'activity' (see ss 6(2)(1) & 9(1)(1)) would indicate *prima facie* that such data could not pertain to a collective entity *per se*, given the mental/subjective connotations of 'belief'. Yet the distinction between activity and belief seems rather artificial in this context. Does it make practical sense to claim, for example, that the fact a private corporation gives money to a particular political party can only be information on the corporation's political activities as opposed to political opinion or beliefs? To take another example, how should one classify information concerning political goals that have been set down in a corporation's articles of association but have yet to be fulfilled in practice? Is it appropriate to classify such information as concerning political activities? Or would it be more appropriate to term this as information concerning the corporation's ideology? If the latter question is answered in the affirmative, wherein lies the practical difference between ideology and opinion or belief?

While the distinction between activity and belief might be artificial, another factor could justify a restrictive interpretation of the descriptions of some classes of sensitive data provided in the Acts concerned. Consider the following three types of collective entities: religious bodies, political organisations/parties and trade unions. If the above-cited legal provisions listing data in need of special protection are interpreted literally, almost all types of information (including data of a relatively trivial nature) on these three types of entities may be classified as sensitive and subject to special regulation pursuant to the Acts of Switzerland, Italy and Luxembourg! In relation to the old Norwegian legislation, of course, only data on religious and political bodies could have been accorded this status. In such a situation, these types of collective entities would enjoy, on paper at least, greater data protection than would the individuals constituting them (and individuals generally). Unless these types of collective entities are viewed as warranting such status (which I do not think is the case),[769] the above-cited provisions listing sensitive data in need of

768 'Eine Ausnahme stellt aber beispielsweise die Angabe über ein weltanschaulich ausgerichtetes Unternehmen oder die Bestrafung einer juristischen Personen dar'): *Botschaft*, *supra* n 680, 34. See also Belser, *supra* n 700, 76 & 80; G Arzt, 'Art. 35', in Maurer & Vogt, *supra* n 700, 405. Cf Peter, *supra* n 702, 87 (raising – though not answering – the question whether the list of data in Art 3(c) of the Swiss Act could relate to legal persons).

769 In my readings of the preparatory documents and explanatory memoranda accompanying the Acts in question, and of more general discussions of data protection laws, I have not come across any comments suggesting that these types of collective entities (or collective entities generally) should be given such status. At the same time, I have not come across any reference to the possibility of these types of collective entities being given such status on the basis of a literal interpretation of the relevant wording in the Acts.

special protection have to be read down such that they refer(red) only to a particular sub-category of data on these entities.

Exactly how this sub-category of data should be defined is not easy to determine. One approach is to decide that only information that can be linked to, or reveal the identities of, particular individuals within the collective entities in question is to be given special protection as sensitive data. This approach would provide, in practice, a level of protection that is similar to the protection provided by the Danish and Icelandic Acts. It cuts out the possibility of providing special protection for data that can be especially sensitive for a collective entity and/or individuals within the entity, but that cannot reveal the identities of particular individuals. A broader approach, which would also provide special protection for the latter sort of data, is for the relevant authorities to draw up a list of data types (concerning the collective entities in question) that shall be regarded as insufficiently sensitive to justify special protection. These data types could include the name, address, program and financial capital of, say, a political organisation, but again, only as long as these data could not allow identification of particular individuals. Data types not mentioned in the list could then be treated *prima facie* as subject to special protection. At the same time, provision could be made for assessment (eg, by the relevant data protection authority) of the sensitivity of these data on a case-by-case basis, with the possibility of special protection being denied some of them.

A final example of discrimination is taken from Norway's PDRA, which effectively allowed for more efficient distribution of credit information concerning 'business entrepeneurs' ('næringsdrivende') than was the case for credit information on persons/organisations not engaged in business (see ss 18(2) & 18(3)).[770] The Act also stipulated that when a credit-rating agency supplies or confirms, in writing, credit information concerning a person who is *not* a business entrepeneur, it must at the same time notify that person, free of charge, of the content of the information (s 19). The Norwegian Ministry of Justice rationalised this discriminatory treatment by claiming that business entrepeneurs generally have greater resources than those not engaged in business, and greater possibilities for protecting their interests.[771] At the same time, it should not be overlooked that the term 'business entrepeneur' can encompass individuals as well as collective entities. In other words, it was not legal or collective personality as such that led to the discriminatory treatment provided for in ss 18 and 19; it was pursuit of a particular type of activity, and the supposed resources of those persons/entities engaged in that activity. Moreover, not all legal persons are classified as 'business entrepeneurs' pursuant to Norwegian law. Many foundations ('stiftelser'), for example, fall outside the category of 'nærings-

770 Note too that the standard licensing conditions issued by the Data Inspectorate for credit-reporting activity permit credit-reporting agencies to register more types of information with respect to business entrepeneurs than with respect to non-business persons/organisations.

771 'De næringsdrivende har generelt større ressurser enn ikke næringsdrivende og større muligheter for å ivareta sine interesser': Ot prp 2 (1977–78), 92.

drivende',[772] and these would presumably be given the same rights pursuant to ss 18 and 19 as individuals who are not engaged in business activities.

10.1.3 DISCRIMINATORY PRACTICES

The above points of discrimination are not the only instances in which the processing of data on collective entities is/were regulated differently to the processing of data on individuals, pursuant to the Acts in focus here. Regulatory discrimination between the two types of data pursuant to at least some of these Acts can also occur in the way the relevant data protection authority exercises its discretionary powers. This is exemplified in the practice of the Norwegian Data Inspectorate. When laying down conditions for its licensing of personal data registers pursuant to the PDRA, the Inspectorate occasionally differentiated between what it allowed with respect to data on individuals and what it allowed with respect to data on legal persons.[773]

10.2 Sectoral Express Protection

In some countries, collective entities have been given rights as data subjects in relation to a particular type of data processing, notwithstanding that the main data protection Acts in these countries expressly protect data on individuals only.

France is an example here. Its 1978 Act on data protection does not expressly regulate the use of data on collective entities. Accordingly, the right of access set out in Art 34 of the Act may be exercised, on its face, by individuals only. This was confirmed by a decision of France's data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), in 1980.[774] In 1984, however, the CNIL modified its position slightly to take into account plans by municipal councils to collect and store data on the business enterprises located in their respective districts. The purpose of setting up these databases was to give the councils a better idea of the commercial and industrial possibilities in each of their municipalities. In response to the plans, the CNIL imposed upon the councils a duty to inform business

---

772 See further discussion by the Norwegian Ministry of Justice on the meaning of 'næringsdrivende' pursuant to s 24(1) of Norway's *Foundations Act* of 1980 (*Lov om stiftelser 23 mai 1980 nr 11*), in W Matheson & G Woxholth (eds), *Lovavdelingens uttalelser* (Oslo: Juridisk Forlag, 1990), 249–252.

773 Compare, eg, points 2.5.2 and 2.5.3 of license 92/2899-30 (issued 22.12.1997 to Telenor) which laid down stricter conditions for the erasure of data on private, individual customers of Telenor than for data on corporate customers.

774 See *Délibération no 80-10* of April 1980. The CNIL's position on this matter was upheld in a decision by the Council of State (*Conseil d'État*) denying the Church of Scientology any rights pursuant to Art 34. See judgement of 15.2.1991 by the Council (10th and 3rd divisions/*sous-sections*), req n 68639: *Église de scientologie de Paris* (reported in *Tableaux de Jurisprudence* (1991), vol IV, 132).

enterprises of the existence of any such database relating to the enterprises, so that legal representatives of the enterprises (company directors, partners or shareholders) could check the data and correct them if necessary.[775] The reason given by the CNIL for its decision had to do with ensuring high data quality. In the opinion of the CNIL, the diversity of information sources for the databases would render it difficult for the councils to ensure, on their own, that the databases are correct and up-to-date. Hence, 'the widest use of access and rectification rights should be guaranteed'.[776]

Another example arises in Swedish law. Sweden's main data protection legislation – initially the *Data Act* of 1973 (now repealed) and now the *Personal Data Act* of 1998 – does/did not expressly protect data on collective entities. However, legal persons are given several rights as data subjects under Sweden's *Credit-Reporting Act*.[777] The latter allows legal persons to find out what information on them is held by credit-reporting agencies (ss 10–11). It also places a duty on these agencies to rectify false or misleading information they hold on legal persons (s 12). Nevertheless, the Act discriminates between legal and natural persons in several respects. For instance, the right of private individuals to gain access to information held by credit-reporting agencies is more extensive than the equivalent right of legal persons (and individuals engaged in business).[778]

Information on financial debts owed by legal persons is given some protection under Sweden's *Debt-Recovery Act*.[779] This Act provides that agencies specialising in debt-recovery on behalf of others must be licensed by the Swedish Data Inspection Board before being able to operate (s 2). The Act sets out general rules on the manner in which debt-recovery operations should be executed. From a data protection perspective, the most important of these rules are found in ss 10a and 11. Section 10a provides that data registers which are used for debt-recovery activities requiring a licence, and which contain information on debtors, can only be used for

---

775 *Délibération no 84-28 du 3 juillet 1984 relative à la mise en oeuvre par les mairies d'Arcueil, Gentilly, Ivry-sur-Seine, Villejuif et Vitry-sur-Seine, d'un fichier d'enterprises.*

776 'Considérant que la diversification des sources d'informations du fichier en rend la mise à jour particulièrement malaisée; que pour remédier à cet inconvénient, il y a lieu de garantir l'exercice le plus large du droit d'accès et de rectification': *ibid.* In the same decision, the CNIL also held that natural persons (including legal representatives of a company) have a right of access to information in these databases which relates to them as individuals; for example, in their capacity as directors, shareholders or associates of a company. However, they are not allowed access to information when this might infringe commercial secrecy.

777 *Kreditupplysningslag* (SFS 1973:1173).

778 Private individuals are allowed access not just to the factual data that credit-reporting agencies hold on them but also to the actual assessments made of their credit-worthiness along with the identities of those who have requested the assessments. Legal persons (and individuals engaged in business) have no right of access to the latter two types of information. For criticism of this anomaly, see GA Westman, 'Varför får inte företagaren besked?', in *Rätten att få vara ifred – tio år med datainspektionen* (Lund: Studentlitteratur, 1983), 63–65. The anomaly did not exist under Norway's PDRA (see s 20(1)).

779 *Inkassolag* (SFS 1974:182).

other purposes if permitted by the Data Inspection Board. Section 11 imposes upon those working in debt-recovery agencies a duty not to disclose or exploit information they have gained concerning, amongst other things, professional or business secrets.

Next, mention should be made of the EC Directive on telecommunications privacy. This Directive expressly provides legal persons with some data protection rights, despite the main data protection Directive – which the former Directive is intended to 'particularise and complement' (Art 1(2)) – expressly safeguarding data on individuals only.[780] The telecommunications privacy Directive is drafted to provide protection for the 'legitimate interests' of legal persons in their role as 'subscribers' to 'telecommunications services' (Arts 1(2) & 2(a)).[781] Relevant safeguards include the following:

- a requirement for telecommunications service providers to inform subscribers of any risks to network security and of any possible remedies, including costs involved (Art 4(2));
- a duty for EU Member States to ensure confidentiality of telecommunications (Art 5(1));
- a requirement that traffic data relating to subscribers be erased or anonymised except insofar as the data are necessary for billing purposes and interconnection payments (Art 6(2));
- a restriction on the processing of the above data for marketing purposes – service providers can use the data for the marketing of their *own* services, if the subscriber consents (Art 6(3));
- a right for subscribers to receive non-itemised bills (Art 7(1));
- a right for subscribers to be provided with the possibility of stopping automatic call-forwarding by third parties to subscriber terminals (Art 10)).

At several points, the Directive draws a distinction in its protection of the interests of individuals as opposed to legal persons. For example, the Directive's provisions restricting the use of automated calling machines (see Art 12) are expressed to apply, as a point of departure, only with respect to subscribers who are natural persons (Art 12(3)). A similar delimitation in the ambit of protection occurs also in relation to the entry of data in public directories over subscribers (see Art 11). In both cases,

---

780 Recital 13 of the telecommunications privacy Directive makes clear that the Directive's protection of legal persons does not entail an obligation on EU Member States to extend the scope of the main data protection Directive to cover legal person data.

781 The term 'telecommunications service' is defined as 'services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting' (Art 2(d)). Such a definition is broad enough to encompass Internet and other on-line services. However, certain of the Directive's provisions employ terms, such as 'call' and 'line', which give the impression that regulation is intended of ordinary (albeit digital, as well as analogue) telephone services only. For example, the phrase 'traffic data' in Art 6(1) is limited to data 'processed to establish calls' (as opposed to, say, data processed to establish 'communications' or 'connections').

however, EU Member States are required to guarantee that the 'legitimate interests' of legal person subscribers are 'sufficiently protected' (Arts 11(3) & 12(3)). Nevertheless, Member States are given greater leeway to determine individually the extent to which the safeguards provided in both articles are to benefit legal person subscribers in addition to individuals.

The Directive on telecommunications privacy is in the process of being replaced by a new Directive concerning the protection of privacy in the context of 'electronic communications'.[782] The basic aim of the new legislation is to broaden and fine-tune the scope of the principles laid down in the former Directive so that they apply, regardless of the particular technologies used, to the provision of all publicly available electronic communications services (other than broadcasting) falling within the scope of EC law (see particularly recital 4). Like its predecessor, the coming Directive provides express protection for the 'legitimate interests' of legal persons in their role as 'subscribers' (Art 1(2)). This protection parallels the safeguards outlined above in relation to the telecommunications privacy Directive. Concomitantly, it fails on basically the same points (ie, entry of data in subscriber directories and use of automated calling systems: see Arts 12 and 13(1) respectively) to be commensurate with the protection afforded subscribers who are natural persons. Another area where the protection extends, as a point of departure, only to natural persons relates to unsolicited communications for the purposes of direct marketing (Art 13(3)).

The above features of the EC legislation may be contrasted with the policy thrust of Germany's *Teleservices Data Protection Act* of 1997.[783] The Act was passed as one element of a broader legislative package to regulate electronic information and communication services – summed up under the concept of 'teleservices' ('Teledienste').[784] Although the Act is not intended to derogate from Germany's

---

782 *Directive 2002/ …/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* – hereinafter termed 'Directive on privacy of electronic communications'. As of 10.5.2002, the Directive has not been finally adopted. The provisions cited here are from the Common Position (EC) No 26/2002, adopted by the Council on 28.1.2002 (OJ C 113 E, 14.5.2002, 39).

783 Long title: *Act on the Protection of Personal Data Used in Teleservices* (*Gesetz über den Datenschutz bei Telediensten*); adopted 22.7.1997; in force 1.8.1997.

784 The legislative package deals with a wide range of issues, including digital signatures and legal protection of databases. For overviews of the whole legislative package as initially enacted, see S Engel-Flechsig, FA Maennel & A Tettenborn, 'Das neue Informations- und Kommunikations-dienste-Gesetz' (1997) *Neue juristische Wochenschrift*, 2981–2992; U Wuermeling, 'Multimedia Law – Germany' (1998) 14 *CLSR*, 41–44. For an overview of just the *Teleservices Data Protection Act* (as initially enacted), see S Engel-Flechsig, 'Teledienstedatenschutz' (1997) 21 *DuD*, 8–16. The Act was recently amended by Art 3 of the *Electronic Commerce Act* of 2001 (*Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14.12.2001*). For analyses of the Act as amended, see eg, P Schaar, 'Neues Datenschutzrecht für das Internet' (2002) *DVR*, no 1, 4–14; H Rasmussen, 'Datenschutz im Internet' (2002) *CR*, no 1, 36–45. The notion of 'teleservices' is defined broadly to cover 'all electronic information and communication services which are designed for the individual use of combinable data such as characters, images or sounds and are based on transmission by means of telecommunication' (s 2(1) of the *Teleservices Act* (*Teledienstegesetz*)).

Federal Data Protection Act of 1990, it *prima facie* initially went further than the latter by expressly providing (organised) collective entities with the opportunity of exercising certain data protection rights in their capacity as teleservice 'users'.[785] However, these rights were apparently not given in order to protect the data protection interests of collective entities as such; rather, they were given on account of the fact that usage of teleservices would often be *formally* linked to collective entities at the same time as *actual* usage would be by individuals.[786] The safeguards provided by the Act were and are primarily directed at the latter usage and data on such usage. Thus, the scope of the Act was and is described as the protection of 'personal data' used in teleservices (s 1(1)), with the term 'personal data' being understood in the same way as it is defined in s 3(1) of the *Federal Data Protection Act* – ie, as data relating to individuals.[787]

Despite this legislative point of departure, the Act first appeared to give collective entities considerable opportunities to exercise data protection rights in relation to the processing of personal data. For instance, the power of consent to such processing in s 3(1) seemed open to exercise by collective entities. Section 3(1) stipulates:

> 'Personal data may be collected, processed and used by providers for performing teleservices only if permitted by this Act or some other regulation or if the user has given his consent.'

Moreover, in some cases, collective entities appeared capable of drawing direct benefit from the data protection measures stipulated because the latter did not revolve

---

(Cont.)
Examples of such services which are mentioned in the legislation are telebanking, telegaming and provision of Internet access. However, certain types of telecommunication, broadcasting and mass media services that could fall within the above definition are expressly exempted from coverage by the legislation (see further s 2(4)). Mass media services, such as pay-per-view television, are subjected, nevertheless, to a set of data protection rules pursuant to Part III of the 1997 *Interstate Agreement over Media Services* (*Staatsvertrag über Mediendienste*; in force 1.8.1997). These rules largely mirror those in the *Teleservices Data Protection Act*.

785 Teleservice 'users' were originally defined as 'natural or legal persons or [organised] associations of persons requesting teleservices' (s 2(2)).

786 See Engel-Flechsig, *supra* n 784, 11 ('Damit will das Gesetz nicht den persönlichen Schutzbereich der datenschutzrechtlichen Bestimmungen erweitern, sondern es trägt den veränderten Nutzungsformen bei Telediensten Rechnung. Es sichert so die Geltung der datenschutzrechtlichen Bestimmungen für personenbezogene Daten auch dann, wenn als 'Nutzer' eine juristische Person oder Personenvereinigung auftritt'). Cf *Gesetzentwurf der Bundesregierung; Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste* (Deutscher Bundestag, 13 Wahlperiode, Drucksache 13/7385, 9.4.1997), 22 (commenting merely that '[d]er Begriff des 'Nutzers' ist weit gefaßt, um die Schutzfunktionen des Gesetzes bereits im vorvertraglichen Bereich greifen zu lassen'). Cf also Rossnagel, Pfitzmann & Garstka, *supra* n 638, 65 (indicating that the extension of protection to legal persons reflected the fact that they enjoy protection for the confidentiality of their telecommunications under Art 10(1) of the *Basic Law*).

787 See also Engel-Flechsig, *ibid*, 11; Engel-Flechsig, Maennel & Tettenborn, *supra* n 784, 2986.

simply around the processing of *personal* data but around the processing of data more generally and/or the technical features of the information systems that support teleservices. However, these potential benefits for collective entities have now been largely eliminated in the recent amendments to the Act instituted by Art 3 of the *Electronic Commerce Act*. Most notably, the definition of 'user' in s 2(2) of the Act has been changed to embrace only natural persons. The rationale for this change is to ensure that the scope of the Act is fully in line with the ambit of the *Federal Data Protection Act*. At the same time, though, the change cuts against the grain of the above-mentioned EC legislation.

10.3 Indirect Protection

This section deals with the extent to which data protection laws can provide indirect safeguards for organised collective entities, independent of whether or not the laws expressly regulate data on such bodies. Thus, the discussion in this section is mainly relevant for those laws that do not give collective entities express data protection rights.

The chief means of providing indirect protection of organised collective entities is through the definitions of 'personal data' (or 'personal information') in the laws concerned.[788] The basic criterion for data to be 'personal' pursuant to data protection laws is that of identifiability; ie, the potential of data to enable identification of a particular person.[789] As shown in Chapter 2 (section 2.4.1), such a criterion is very elastic. Indeed, it is impossible to determine exhaustively in the abstract what may qualify as 'personal data' or 'personal information'. Hence, whether or not an item of information relating directly to a collective entity may also qualify as information relating to an individual can only be assessed in the light of all of the circumstances of the particular case. The outcome of this assessment will vary in tact with technological-organisational developments. The outcome will also be influenced by the biases and policy objectives of the particular party undertaking the assessment.[790]

At the same time, it is clear that data protection laws will usually protect data on an identifiable individual even if the data are also linked to a particular collective entity. Less clear is the extent to which *other* data on that collective entity will thereby become 'personal'. The latter issue resembles the issue of the extent to which, say, data on a person's property will become classified as 'personal' once an initial link between the person and an aspect of the property is made.[791] In the absence of a requirement that 'personal data' (or 'personal information') relate to a

788 There are several other means of indirect protection but these are primarily relevant for non-organised collective entities. See further Chapter 15 (sections 15.4–15.5).

789 See further Chapter 2 (section 2.4.1).

790 See further Chapter 11 (section 11.3.3).

791 See the discussion in Chapter 2 (section 2.4.1).

particular sphere of a person's life or activities, there is potential, at least in theory, for a large amount of data linked primarily to a collective entity to be classified as 'personal' once the entity is linked to an identifiable individual. However, this potential is cut back significantly by the difficulty of linking such data to *one* individual as opposed to a group or class of individuals.[792] For this reason, it is often assumed a great deal of information on large corporations could never qualify as 'personal information' pursuant to data protection laws not expressly covering such information.

Nevertheless, the requisite link between information on, say, a particular company and information on an individual will be relatively easy to establish in the case of a company formed and run by just one individual (ie, a one-person enterprise; sole trader); it will be even easier if the company bears that individual's name as there is then no need for auxiliary information to link the company with the individual. In such cases, information revealing the identity of the company is likely to be judged as 'personal information' relating to that individual – at least in some jurisdictions. In this regard, it is pertinent to refer to a 1985 decision of the German Federal Court (Bundesgerichtshof).[793] The decision concerned a case in which a man attempted to prevent information on the financial status of a company established and run solely by him, being regarded as information on his own credit-worthiness. The Court held in part that the information on the financial situation of the company could also be regarded as information concerning the credit-worthiness of the individual, and hence as 'personal information' pursuant to Germany's *Federal Data Protection Act* of 1977.[794]

The opposite line has been taken by the NZ Complaints Review Tribunal in the case of *C v ASB Bank Ltd*.[795] In this case, financial information about what was essentially a one-person company was held not to constitute personal information pursuant to the NZ *Privacy Act*. The term 'personal information' is defined as 'information about an identifiable individual' (s 2). The Tribunal accepted the proposition that 'all transactions on a company's bank statements are the transactions of the company, not of any individual, no matter how identified with the company the individual may be'.[796] While this refusal to lift the corporate veil is faithful to the

---

792 Note, though, the variations in the stringency of the individuation requirement referred to in Chapter 2 (section 2.4.1).

793 Decision of 17.12.1985 reported in (1986) 2 *RDV*, 81–83.

794 It is not clear from the case report whether or not the company bore the man's name but this factor seems to have been irrelevant for the outcome of the decision. Cf Dammann, *supra* n 157, para 43 ('Daten einer Kapitalgesellschaft sind ... nicht ... zugleich Daten eines Gesellschafters, weil es sich um eine Ein-Mann-GmbH handelt (a.M. soweit es sich um kreditrelevante Verhältnisse handelt, auch bei GmbH, die nach Gesamtbild im Innenverhältnis Personengesellschaft ist ...').

795 Decision No 21/97 of 24.7.1997, reported in (1997) 4 *PLPR*, 116.

796 However, the Tribunal also held that '[t]here may be circumstances in which it is possible to hold that information that appears not to be about an identifiable individual becomes personal information if

long line of jurisprudence stemming from the House of Lords' decision in *Saloman v A Saloman and Co Ltd*,[797] it is problematic in a data protection context. Such a formalistic approach detracts unnecessarily from the flexibility inherent in the definition of 'personal information' in the NZ *Privacy Act*, along with the equivalent definitions in many other data protection laws. One can only hope that the Tribunal's approach is not followed elsewhere.[798] In any case, it is doubtful that the approach conforms with the wording and spirit of the EC Directive's definition of 'personal data'.[799]

Establishing the requisite link between an individual and what is, properly speaking, a collective entity will be more difficult than with respect to a one-person enterprise, even if the collective entity is made up of a fairly small number of individuals. In this regard, it is instructive to consider data relating to the following kinds of collective entities:

1) an entity (eg, corporation) which bears the name of one of the individuals who composes it but is not under the exclusive control of that individual;
2) an entity (eg, partnership) which bears the names of all or several of the individuals who compose it but is not under the exclusive control of any single one of these individuals;
3) an entity (eg, corporation) which does not bear the name(s) of any of the individuals who compose it but is, in reality, controlled by only one of them;
4) an entity (eg, corporation) which does not bear the name of any of the individuals who compose it, is not controlled by any single one of them alone, but is, nevertheless, *popularly* perceived as being so controlled.

In each case, to what extent may data revealing the identity of the entity concerned – let us say the data relate primarily to the entity's annual net earnings and/or investments – be regarded as information relating to an individual person and hence 'personal information' pursuant to data protection laws that expressly cover data on individuals only? In the following, no attempt is made to resolve this issue conclusively for each of the four cases; the analysis is more conjectural. The

---

(Cont.)
other personal information is not intelligible without it, particularly, for instance if the personal and non-personal information appears on the same document or in the same set of information'.

797 (1897) AC 22.

798 Cf the claim by Nigel Waters that the Tribunal's approach would probably be followed in Australia: see (1997) 4 *PLPR*, 116. Waters goes so far as to claim that '[i]t is doubtful if Australian businesses even in their worst nightmares could envisage a privacy regulator or courts so radical as to uphold an interpretation of a privacy law at variance with this NZ decision': *id*. With respect, this claim is overly bold.

799 The definition is set out in Chapter 2 (section 2.4.1). Note too that the *travaux préparatoires* to the new Norwegian and Swedish data protection Acts (neither of which expressly protect legal person data) indicate that data on one-person enterprises are covered by the legislation. See Ot prp 92 (1998–99), 102; NOU 1997:19, 54; SOU 1997:39, 341.

conjectural element follows partly from the fact that the issue has scarcely been examined in data protection discourse.

In case 1, the named individual is essentially a mere figurehead for the corporation. There is no direct correlation between that person and the activities giving rise to the income and/or investment data. Thus, the data cannot really be linked to just that individual. These factors would point to a conclusion that the data are not 'personal' for the purposes of data protection law.[800] Nevertheless, the fact that the corporation bears the person's name can give the impression (albeit falsely) that the data in question are related exclusively to the named individual. Moreover, the data could reflect (negatively as well as positively) on the person's character. These latter two factors would point to a conclusion that, at least in *lex ferenda* terms, the data ought to be treated as 'personal' pursuant to data protection law. Yet are either of the latter factors relevant in terms of *lex lata*? Arguably, the last-mentioned factor is not relevant in this regard; rather, what is decisive is the existence or not of a connection between data and a given individual. In this case, such a connection does exist, primarily on account of the prominence of the individual's name, but the connection is objectively incorrect. Does this lack of objective validity matter? Recalling the discussion of this point earlier in the section, data protection laws with definitions of 'personal data' (or 'personal information') not embracing mere opinions probably do not allow data to become 'personal' primarily on the basis of a *mis*perception that the data are so capable. The situation might be different, though, with respect to those laws that allow for opinions to qualify as personal data; it is undoubtedly different with respect to those laws allowing for *false* opinions to qualify as such. And, at least as a matter of *lex ferenda*, there are solid grounds for arguing that such misperception should be legally relevant if it is socially significant; ie, is shared by many people and has possibly adverse consequences for the individual concerned.

As an aside, it is worth noting a view of the official committee appointed by the Norwegian government in 1970 to look into data protection problems associated with the private sector. The committee proposed legislation that would protect data on individuals only.[801] In this regard, it took the view that the simple fact a piece of information on a corporation reveals the name of an individual (eg, the managing director of the corporation) should not of itself bring that piece of information within the scope of the proposed legislation. According to the committee, its proposed legislation would only protect such information upon two conditions: (1) that the information told something of the individual's character; and (2) that the information was of more than a 'neutral' and 'non-sensitive' nature.[802] The Committee did not make clear, though, whether it considered these conditions as cumulative or

800 Such a conclusion appears to be embraced in the *travaux préparatoires* to Sweden's *Personal Data Act*: see SOU 1997:39, 341.

801 See *Persondata og personvern*, NOU 1974:22, 45ff.

802 Ibid, 46.

alternative. Neither did it go into detail as to what information it considered to be 'neutral' and 'non-sensitive'. I do not have empirical evidence showing whether or not the definitions of 'personal information' in current data protection laws are or would be read down in line with the committee's stance. Even if they were to be or are read down in such a way, it is quite possible this would mean, in practice, little reduction in the amount of information protected by the laws. This is for two related reasons. First, there is the practical difficulty of distinguishing between 'sensitive' and 'non-sensitive' personal information. Secondly, information linking an individual to a corporation will often be capable of reflecting, accurately or otherwise, on the character or personality of the individual. This will be especially so in the case of those individuals who have (or are perceived as having) control over the activities of the corporation. Yet even the mere fact that an individual chooses to work for a corporation can be enough to stamp him or her as being of a particular character. For example, persons who work for a corporation producing and marketing goods that are generally regarded as both unhealthy and unnecessary (eg, tobacco products), could be viewed as callous, particularly if they are perceived as *choosing* to work for such a corporation.

In case 2, it is unlikely that the data are 'personal', simply on account of the fact that the data cannot be exclusively linked to *one* of the individuals in question. Nevertheless, the fact that the data are connected to *named* individuals, together with the possibility that the data can tell us something about the character of these persons, are grounds for arguing that, at least in terms of *lex ferenda*, the data should be treated as 'personal' for the purposes of data protection law.[803]

As for case 3, the data could be 'personal' if (i) auxiliary information exists to link the corporation as such to the individual in control of it, and (ii) the data relate to activity that can be attributed exclusively to that person.[804] In corporations with multiple levels of management, the second-mentioned condition will rarely be satisfied. Yet we must remember there are different types of control: eg, one can have control in the sense of being finally responsible for the actions of others; or one can have control in the sense of determining the final result of a given process, but without determining every step in that process; or one can have control in a more direct way – ie, one actively steers and determines every step in a given process. It will be easiest to establish that data are 'personal' under data protection law when the data relate to the result of a process controlled in the last-mentioned manner (assuming, of course, that the control is not shared). Control of the first-mentioned kind is unlikely to suffice. As for the second-mentioned type of control, this might

803 Cf the view expressed in the *travaux préparatoires* to Sweden's *Personal Data Act*: *supra* n 800.

804 Under the NZ *Privacy Act*, however, such data might not be personal even when both criteria are met: see the decision in *C v ASB Bank Ltd*, *supra* n 795. Note also the opinion expressed in the *travaux préparatoires* to Sweden's *Personal Data Act*, *supra* n 800. The latter opinion appears to rule out *ownership* of a legal person as a relevant criterion. It is uncertain, though, if the opinion thereby makes the factor of control also irrelevant.

suffice in some circumstances, depending on, ia, the number of persons involved in the process and the number and nature of management levels concerned.

With respect to case 4, a pertinent example is News Corporation, which is popularly identified with Rupert Murdoch. News Corporation is Murdoch's alter ego in the eyes of many people; all or most of the actions of the corporation are popularly viewed as inseparable from the actions of Murdoch. Accordingly, should not information on, say, the income and/or investments of News Corporation qualify as personal information pursuant to data protection laws that expressly protect data on individuals only? The answer to this question must take account of, ia, the type of control Murdoch exercises in relation to the processes that result in the income and investment data. This factor is covered in relation to case 3. Another issue highlighted in case 4, though, is the legal relevance of the public (mis)perception of Murdoch's role in the corporation: does it trump the above-mentioned control factor, despite its lack of objective validity? This issue is covered in relation to case 1 above.

Using Murdoch's News Corporation as the example here is intentionally provocative: many people would baulk at the idea of according data protection rights to such a powerful (and hard-headed!) entity. The reasons for this reaction – and their validity in a data protection context – are explored more fully in Chapter 13. Arguably less provocative examples (at least for people who support 'green' politics) would be environmental protection bodies such as Bellona (based in Norway and popularly linked to Frederic Hauge) and Sea Shepherd (based in North America and popularly linked to Paul Watson). Nevertheless, it is at the very least doubtful that we can or should discriminate between an entity like News Corporation and the latter entities with respect to resolving the issue taken up here, purely on the basis of differences in economic power and ideology. The relevance of such differences is further discussed in Chapters 13–14.

To sum up, the open and somewhat nebulous manner in which the notion of 'personal data' is legally defined makes it difficult to determine in the abstract what data on collective entities will qualify as personal data pursuant to the relevant law. Nevertheless, the following general principles seem to apply:

- the harder it is to distinguish between the activities of an individual and those of a collective entity, the greater is the chance an item of information on the latter may also relate to the individual, and the greater is the amount of information on the collective entity which potentially relates to the individual;
- it will be harder to distinguish between the activities of an individual and those of a collective entity as the number of individuals attached to the entity decreases and/or as the degree of the individual's control over the entity increases.

11. Consequences of Protecting Data on Collective Entities

11.1 Allegations about Consequences

Numerous allegations have been made concerning the consequences of giving certain types of collective entities (primarily legal persons) rights as data subjects under data protection legislation. This chapter assesses these allegations, particularly in light of experiences from Norway, Austria and Denmark.

The allegations tend to be purely speculative. Few attempts have been made to gather empirical material on the actual effects of those laws expressly protecting data on collective entities in addition to data on individuals. Many of the allegations do not claim that protection of data on collective entities *will* have a particular consequence; they claim, rather, that such protection *could* have a particular consequence. Some allegations, though, are drafted such that they can be read to claim either or both of these things. For example, Colin Tapper has alleged that giving corporate bodies rights under data protection legislation

> 'would certainly raise the profile of such legislation, since they [corporate bodies] could be expected to employ it, and to employ it in extremely dubious and contentious situations.'[805]

Although Tapper does not elaborate on his statement, it could be read as a veiled reference to what is perhaps the greatest fear in relation to giving legal persons data protection rights. This fear is that legal persons could use these rights in a manner that distorts economic competition between themselves. The fear attaches primarily to the right of data subjects to find out what sorts of information relating to them are held by data controllers. It has frequently been alleged that legal persons could use this right to find out what information is kept on them by their competitors. It has also been alleged that from this knowledge, they could deduce information about their competitors' business strategies and 'know-how'. To quote a representative for IBM,

805 C Tapper, *Computer Law* (London: Longman, 1989, 4th ed), 337.

> 'in order to carry out normal business planning it is necessary to make estimates of, for example, purchasing potential of a customer, the production potential, quality, or delivery performance of suppliers and sales activities of competitors. [...] To be obliged by the law to disclose this information to the customer or supplier could damage a business relationship. To disclose to a competitor information you may have on his sales activities, or to disclose to a competitor, for example, the content of a market research file, could well damage one's own sales position. It could certainly reveal one's product development strategy.'[806]

A related allegation is that information on companies which is collected and held by data protection authorities could be divulged to competitors of these companies under FOI laws. The information referred to here is gathered by data protection authorities in the process of inspecting and auditing the files of data controllers.[807]

Another major fear expressed in relation to protecting data on legal persons is that such protection could hinder transborder flows of business data.[808] For instance, it has been alleged that

> 'countries whose privacy laws also protect legal persons can apply restrictions to nearly all data flows to countries such as the United States, where legal persons are not protected because of a lack of reciprocal protection.'[809]

It has also been alleged that protecting legal person data will increase the workload of data protection authorities, 'with the effect that the data protection interests of individuals could not be properly taken care of'.[810] Concomitantly, it has been claimed that protection of legal person data will increase the workload of legal persons in their capacity as data controllers: not only will legal persons have to observe various legal requirements when processing data on individuals, they will also have to observe such requirements when processing data on other legal persons. According to Rutgers, this will make data-processing more expensive and cumbersome.[811] The extra expense, he alleges, could be most problematic for small business enterprises:

---

806 Citation in European Parliament, Legal Affairs Committee, Subcommittee on Data Processing and Individual Rights, *Verbatim record of the public hearing on data processing and the rights of the individual*, Brussels, 6.2.1978 (PE 52.496), 154.

807 See, eg, TM Rankin, 'Business Secrets across International Borders: One Aspect of the Transborder Data Flow Debate' (1985) 10 *Canadian Business LJ*, 213, 224–225.

808 See also Chapter 6 (section 6.3.2).

809 C Hoyle, 'Legal Aspects of Transborder Data Flow' (1992) 8 *CLSR*, 166, 170.

810 TM Rutgers, 'Privacy Legislation, Data Protection, and Legal Persons', in *Transborder Data Flows*, Proceedings of an OECD Conference held December 1983 (Netherlands: OECD/Elsevier, 1985), 393, 395–396. See also ICC, *supra* n 748, 426.

811 *Ibid*, 395. See also ICC, *supra* n 748, 426.

> '[i]n a society where (personal or other small) computers are used more and more by small businesses the burden of complying with protective legislation (registration of files, license, duty to inform etc) might be difficult to bear and perhaps relatively more of a problem for them than for large businesses.'[812]

At the same time, Rutgers claims that legal persons do not receive any practical benefits to offset these costs of protecting legal person data:

> 'to date [1983], as far as is known, there have been no cases of abuses of business data that could have been avoided by including ... legal persons in data protection legislation.'[813]

Finally, several allegations have been made concerning the consequences of *not* giving data protection rights to collective entities (again, primarily legal persons). The first two of these allegations relate to the so-called 'mixed file' problem described in Chapter 9 (section 9.3). As noted there, it has been alleged there is a risk of double-edged information (ie, information relating *prima facie* to collective bodies but also capable of being linked to particular individuals) being processed without regard to data protection laws if the latter only protect data on individuals.[814] It has also been claimed that enacting data protection laws that only protect data on individuals necessitates reorganising 'mixed file' registers so that information on individuals is segregated from information on collective bodies, and that this process can be expensive and difficult.[815]

The third allegation relates to the so-called 'small business' problem, also described in Chapter 9 (section 9.3). As noted there, it has been claimed that if data protection legislation covers only data on physical persons, an individual who runs a small business not accorded legal person status will be given rights under the legislation, while an individual whose business is accorded legal person status may not exercise those rights on behalf of the business, despite the business perhaps being of the same size and type as the former business.[816]

---

812 *Ibid*, 397.

813 *Ibid*, 396. The same claim is made by the ICC: *supra* n 748, 426. Similarly, Chamoux writes (in 1980) that '[t]here has been no open, concrete case which can ... prove definitely the necessity for a specific protection of companies with regard to computer files ...': Chamoux, *supra* n 636, 74. See also Bancilhon *et al*, *supra* n 636, 17.

814 See Toussing, *supra* n 708, 10.

815 See Cole, *supra* n 709, 945.

816 See Chamoux, *supra* n 636, 74–75; Bancilhon *et al*, *supra* n 636, 8.

11.2 Actual Consequences

11.2.1 SURVEY METHOD

The discussion in this section is largely based upon the results of a survey I carried out on the practical consequences of data protection legislation of Norway, Austria and Denmark expressly covering data on certain types of collective entities in addition to individuals. The survey was conducted in 1992–94 in two stages. First, the Norwegian Data Inspectorate (DI) was sent a questionnaire on the consequences of protecting data on legal persons pursuant to the *Personal Data Registers Act*. Secondly, the Inspectorate's response to the questionnaire[817] was supplemented by follow-up interviews with senior officers of the Inspectorate and by information contained in its annual reports and archives. The focus of the questionnaire (and follow-up interviews) on legal persons rather than collective entities generally is mainly a reflection of the focus of public debate in this context.

The questionnaire was also sent to data protection authorities in the other countries (with the exception of Switzerland and Italy) that have data protection laws covering legal person data, but the responses from these authorities were poor. The data protection authority of Luxembourg did not respond at all, while the Danish Data Protection Agency (DPA) and the Icelandic Data Protection Commission (DPC) stated they had neither sufficient time nor resources to respond.[818] A positive response, however, was given by the Austrian Data Protection Commission, though the answers tended to be brief.[819] I did not attempt to supplement or qualify them by follow-up interviews or with other material.

The lack of response by the Danish DPA is compensated to some extent by information gathered from (i) the DPA's annual reports, (ii) an internal note by the DPA on actual cases involving legal persons using data protection rights,[820] and (iii) a personal interview carried out on 8.6.1994 in Oslo with a DPA legal officer at the time, Jette-Marie Sonne. This information is referred to in the discussion below where appropriate.

---

817 The response was sent to me in a letter dated 25.1.1992 (ref 91/2997-2 KBK/HH), written by Knut-Brede Kaspersen, then Senior Advisor at the Inspectorate.

818 Letter sent by DPA on 16.1.1992 (letter no 0184; ref CD/jd); letter sent by DPC on 8.9.1992 (ref JT/-). It is worth noting that the DPC also wrote in its letter that there has been 'practically no discussion' in Iceland on the issues addressed in the questionnaire.

819 The response was sent in a letter dated 30.3.1992 written by Dr Walter Dohr.

820 'Notat om virksomheder og klagesager i relation til lov om private registre og lov om offentlige myndigheders registre' (CAG/24.03.1997).

11.2.2 ACCESS RIGHTS

In the survey questionnaire, each of the relevant data protection authorities was asked whether or not it knew of any instances of legal persons using information access rights provided under its country's data protection legislation to find out what sort of information about them was held by their business competitors. The Norwegian and Austrian data protection authorities replied that they did not know of any such instances.[821] Each authority was also asked whether or not it had heard of any complaints that legal persons had used their information access rights pursuant to data protection law such that they had learned important confidential information about competitors' business strategies and 'know-how'. Again, the Norwegian and Austrian data protection authorities replied that they were not aware of any such complaints.

The information access rights provided in the data protection legislation of Austria, Iceland, Norway, Switzerland and Italy are not absolute.[822] The legislation allows data controllers and/or data protection authorities to resist use of these rights by data subjects. Whether or not access will be allowed is often dependant on a weighing up of the various interests at stake in the particular case. The Swiss Act is especially detailed on this point. It stipulates that access to information can be denied, limited or delayed pursuant either to a formal law or to the demands of third party interests (Art 9(1)). A federal government agency can also limit access if this is necessary to serve dominant public interests, particularly the internal or external security of the Swiss Confederacy, or because access would be at cross-purposes with investigations into criminal or other matters (Art 9(2)). Data controllers in the private sector can also deny, limit or delay access to data insofar as is necessary to serve their *own* 'dominant' interests and as long as the data are not passed on to third parties (Art 9(3)). Further, the Swiss Act provides that those in the media industry can deny, limit or delay access to personal data if the data are used exclusively for publication purposes, and access would either disclose information sources, disclose plans for (future) publications or endanger the 'free formation of public opinion' ('die freie Meinungsbildung des Publikums'; Art 10(1)). Those working in the media industry can also limit access to personal data in cases where the data form part of a databank used exclusively as a 'personal work tool' (Art 10(2)).

The equivalent provisions of the other countries' respective Acts are not as detailed. For instance, Norway's PDRA provided that the right of access did not

821 Note too the Norwegian Data Inspectorate's general impression that access rights pursuant to the PDRA tended to be little used: see, eg, St meld 103 (1981–82), *Datatilsynets årsmelding 1981*, 12; St meld 23 (1985–86), *Datatilsynets årsmelding 1984*, 6–7; St meld 48 (1987–88), *Datatilsynets årsmelding 1987*, 13; St meld 37 (1989–90): *Årsmelding for Datatilsynet 1989*, 20.

822 Luxembourg's Act would seem to be an exception here: on its face, Art 20 of the Act gives data subjects unqualified access rights. It would be surprising, though, if derogations from these rights have not been laid down pursuant to the Act's general licensing regime or its regulations.

apply to registers used only for statistical, research or general planning purposes, or to *manual* registers kept by data controllers from the *private* sector (see generally s 7).[823] Section 7(5) of the Act also empowered the Data Inspectorate to set out exceptions to the right on a case-by-case basis.[824]

In the latter regard, the Norwegian DI exempted IBM in 1983 from an obligation to provide access to two of the corporation's computerised registers (see case 80/392). The registers in question were a register over companies (and their computer facilities) that had been supplied with computer equipment either by IBM or its competitors, and a register of IBM's own customers. Both registers were used by IBM for marketing purposes. In reaching its decision, the DI stressed that the registers contained information on legal persons only and were used in a 'competitive situation'.[825] The decision shows that the DI was aware of the need to preserve company secrets, and concerned to ensure Norwegian data protection law did not disturb economic competition between companies.

Interestingly, IBM seems to be the only private corporation to have asked the DI for exemption from the access rights provided under the *Personal Data Registers Act*.[826] The fact that other private corporations failed to seek such exemption can mean they were not anxious about these rights being used to their disadvantage or that they were unaware of these rights. Either account meshes well with the DI's above-cited impression that data subjects generally do not make use of their access rights. At the same time, it would not have been easy for data controllers to get permission from the Inspectorate to withhold data from corporations to which the data relate. The Inspectorate claimed that, as a general rule, it only allowed such restriction of access rights in very special circumstances.[827]

In the survey questionnaire, each data protection authority was also asked whether or not there had been any cases in which business information contained in its inspection records, put together after completion of data protection audits, has been disclosed under FOI legislation. Both the Norwegian and Austrian data protection authorities replied in the negative. However, neither of these authorities provided clear answers as to whether or not such disclosure *could* have occurred.

With respect to Norway, it is highly unlikely such disclosure could lawfully take place. Norway's *Act on Openness of Administration* (hereinafter 'AOA')[828] provides that any person may demand access to 'case documents' ('saksdokumenter') in the

---

823 Note, however, s 1-5 in the main regulations to the PDRA (*Forskrifter i medhold av lov om personregistre mm 21 desember 1979*) which gave *employees* in the private sector a right of access to data on them kept in manual personnel registers. However, this provision was of little relevance for the access rights of collective entities.

824 See too s 1-4 of the main regulations to the Act.

825 Datatilsynet, *Årsmelding 1983*, CompLex 4/84 (Oslo: Universitetsforlaget, 1984), 16.

826 According to Knut-Brede Kaspersen, Head of the Inspectorate's Legal Section, in a personal interview of 28.6.1999.

827 Again, according to Kaspersen in the same interview.

828 *Lov om offentlighet i forvaltningen 19 juni 1970 nr 69*; in force 1.7.1971.

possession of a public administrative body (s 2). However, certain documents and information are exempted from this rule, including (but not limited to):

- documents used by an administrative body for 'internal case preparation' ('interne saksforberedelse')(s 5(1));
- information that is subject to a legal duty of confidence (s 5a(1));
- documents that, if made public, would counteract public control or regulatory measures, or would entail a risk that such measures could not be executed (s 6(2)(c)).

The bulk of the DI's inspection records would probably fall under at least one of these exemptions. Somewhat surprisingly, the AOA does not provide an explicit exemption for information relating to trade secrets and other sensitive business information. The Act originally contained such an exemption but this was taken out when the Act was amended in 1982, on the grounds that the exemption was unnecessary.[829] It was argued that such information comes within the exemption provided by s 5a of the Act (set out above). This is because Norway's *Administrative Procedures Act* (hereinafter 'APA')[830] imposes an obligation on persons who carry out service or work for an administrative organ to keep confidential certain matters with which they become aquainted in connection with that service or work (see s 13 of the Act). This obligation of confidence embraces, amongst other things, information on technical devices/procedures and business matters, the secrecy of which is 'competitively significant' ('av konkurransemessig betydning') for the party concerned (s 13(2)).[831]

A more limited right to gain access to information held by public administrative bodies is provided by s 18 in the APA. This provision gives a party to a case involving an administrative decision the right to gain access to the case documents. This right does not extend to documents used by an administrative organ for 'internal case preparation' ('interne saksforberedelse'), though it does extend to those parts of these documents that contain 'factual information' ('faktiske opplysninger'),[832] unless this information is of no significance for the case decision or is contained in other documents to which the party has access. One could expect that a considerable proportion of internal documents are made up of 'factual information' (as defined above), thereby reducing the scope of the exception from the right of access to internal documents. At the same time, though, s 19(1)(b) exempts from the right of access provided in s 18 any documentary information relating to technical devices,

829 See Ot prp 4 (1981–82), 33–35; Eckhoff & Smith, *supra* n 36, 490.

830 *Lov om behandlingsmåten i forvaltningssaker 10 februar 1967*; in force 1.1.1970.

831 For a detailed treatment of the ambit of s 13(2), see, ia, A Frihagen, *Offentlighetsloven* (Bergen: Frihagen, 1994, 2nd ed), vol II, 64–73.

832 The term 'factual information' is interpreted broadly to include information based to a large degree on subjective assessments of fact situations, but not information which consists of legal assumptions/classifications: see Ot prp 3 (1976–77), 79; Eckhoff & Smith, *supra* n 36, 487–488.

production methods, trade secrets, business analyses and reports which is of such a nature that it can be exploited by others in their own business activities.[833]

11.2.3 TRANSBORDER DATA FLOWS

In the survey questionnaire, each data protection authority was asked whether or not protection of legal person data under its country's data protection legislation had caused any major problems for transborder data flows. The Norwegian DI replied there had been no such problems. The Austrian DPC did not respond to the question. As for Denmark, neither the annual reports of the DPA nor its internal note mention one case in which the agency acted to prevent transborder flow of legal person data, and Sonne stated she knew of no such case.

Two main factors would appear to account for the absence of problems in Norway. First, the DI has rarely exercised its power to prevent transborder data flows.[834] Secondly, a great deal of transborder data flow has probably occurred without the knowledge or permission of the DI.[835] According to Sonne, the same sorts of factors appeared to account for the absence of problems with regulating flows of legal person data out of Denmark.

There appear to have been only two cases in which the Norway's DI actively regulated the transborder flow of data on legal persons.[836] The one case (case 93/2317) concerned plans by the credit-reporting agency, Dun & Bradstreet Soliditet, to transfer its agency's register of enterprises ('foretak') to Pennsylvania. The Inspectorate first decided to allow the data to be transferred to the USA for a test-period of one year on the condition that Dun & Bradstreet Soliditet: (i) provided the Inspectorate during this period with more details about how the transferred data were

---

833 Eckhoff & Smith note, however, the possibility for a party to a case to gain access to case documents that come within the exemption set out in s 19(1)(b) of the APA: Eckhoff & Smith, *supra* n 36, 490. This could be done by claiming access to the case documents under the AOA. As noted above, s 5a of the latter Act disallows access to documents which are subject to a duty of confidence; s 13(b)(1) of the APA, however, states that case documents may be still be accessed by a party to the case even if they are subject to a duty of confidence. Eckhoff & Smith comment, though, that the legislators can hardly have intended to allow such circumvention of the exemption set out in s 19(1)(b) of the APA. Hence, they argue (correctly, in my opinion) that the AOA should be interpreted in such a way as to prevent it from allowing a party to gain access to case documents that the party could not access pursuant to s 19(1)(b): *ibid*, 490. See also Frihagen, *supra* n 831, 91. The protection for business information found in the APA and AOA is supplemented by ss 7–8 of Norway's *Marketing Act* (*Lov om kontroll med markedsføring og avtalevilkår 16 juni 1972 nr 47*) and ss 294 and 405a of the *Penal Code*. For commentary on the scope of these provisions, see TC Løchen & A Grimstad, *Markedsføringsloven med kommentarer* (Oslo: Tano Aschehoug, 1997, 6th ed), 132ff.

834 According to an interview of 28.6.1999 with Knut-Brede Kaspersen, Head of the Legal Section of the Data Inspectorate. See also, eg, Djønne, Grønn & Hafli, *supra* n 563, 158.

835 Djønne, Grønn & Hafli, *supra* n 563, 159; Ellger, *supra* n 75, 361–362.

836 Confirmed by Kaspersen in the same interview, *supra* n 834.

to be used in the USA; and (ii) gave registered enterprises the opportunity to refuse to have information on them transferred to the USA.[837] Dun & Bradstreet Soliditet were also informed that it remained responsible under Norwegian law for the use of the data transferred to Pennsylvania.[838] The Inspectorate subsequently issued a permanent allowance for the transfer on the condition that the data would be processed in accordance with the rules that would ordinarily apply were the data to remain in Norway.[839]

The other case (case 88/282) is legally more interesting. It stems from 1988 when the DI discovered that a credit-reporting agency, Esselte Soliditet, had transferred its database on business entrepeneurs ('næringsdrivende') from Norway to Sweden without first notifying the Inspectorate.[840] The DI ordered the agency to transfer the database back to Norway. The agency complied with this order. The DI stated that its decision in this case arguably breached Art 12(2) of the CoE Convention, but it took the view that the decision could be justified pursuant to Art 12(3)(a) of the same Convention.[841] According to the Inspectorate, the credit information it prevented from being transferred to Sweden fell within a special category of data specifically regulated by the PDRA.[842] While this claim is true, Art 12(3) cannot be invoked when such data are transferred to State Parties providing 'an equivalent protection'. It can be argued that Sweden provides such protection as it has legislation on credit reporting which expressly regulates use of legal person data.[843] On the other hand, it can be argued that Sweden does not provide equivalent protection because the rights given to legal persons under the Swedish *Credit-Reporting Act* are not as extensive as those that were provided under the Norwegian PDRA.[844] In informing Esselte Soliditet of its decision to disallow the transfer of data to Sweden, the Inspectorate wrote: '[p]lacement of the register [over business enterprises] in Sweden can involve a weakening of data protection which is little to be desired'.[845] This statement appears to indicate that the Inspectorate did not view

---

837 See letter of 1.2.1994 (ref 93/2317-3 HK/-) from the DI to Dun & Bradstreet Soliditet.

838 *Id*.

839 See letter of 16.9.1994 (ref 93/2317-5 ÅMB/-) from the DI to Dun & Bradstreet Soliditet.

840 St meld 33 (1988–89), *Årsmelding for Datatilsynet 1988*, 16.

841 The gist of both provisions is set out in Chapter 4 (section 4.4). Insofar as the case concerned data on legal persons only, the relevance of both provisions was contingent on Norway having declared that it applies the Convention to the processing of such data (see Art 3(2)(b)). Norway issued a declaration on 20.2.1984 that it extends coverage of the Convention to information on 'associations and foundations'. Surprisingly, Norway has not yet withdrawn this declaration despite the fact that its new legislation, the *Personal Data Act*, largely dispenses with express protection for such data. For similar declarations by other States, see *infra* n 854 and accompanying text.

842 *Supra* n 837, 16.

843 See Chapter 10 (section 10.2).

844 See *supra* n 778 and accompanying text.

845 'Plassering av registeret i Sverige kan innebære en svekkelse av personvernet som er lite ønskelig': see letter of 7.3.1988 (ref 88/282-2 RP/-).

the level of data protection in Sweden as 'equivalent' to that of Norway but it fails to indicate precisely the reason(s) for this view.

The Inspectorate has never issued an explicit, comprehensive statement as to what constitutes 'equivalent' protection to Norwegian data protection law. This omission is perhaps not surprising as making valid comparisons of one country's legal system with those of other countries is difficult.[846] Nevertheless, the omission creates significant legal uncertainty for both data controllers and data subjects. Contributing to this uncertainty is the failure of the CoE Convention's Explanatory Report to provide guidance on the meaning of the phrase 'equivalent protection' in Art 12(3) of the Convention.

How are we to understand that phrase? How are we to apply the criterion/test it embraces, particularly in the context of transborder flow of data on legal persons and collective entities more generally? To take the latter question first, application of the equivalency criterion obviously requires an assessment of the *range*, *content* and *effect* (including enforceability) of countries' respective rights regimes in the field of data protection.[847] Further, equivalency can only be properly assessed on a case-by-case basis taking into account all the circumstances of the proposed data transfer.[848]

As for the meaning of 'equivalent protection', it seems safe to assume that the phrase does not mean identical protection; equivalence permits some variation in format and, to a lesser extent, substance.[849] It also seems safe to assume that the notion of equivalence denotes a more stringent and less flexible standard of protection than the notion of adequacy in Arts 25–26 of the EC Directive.[850] Some uncertainty remains, though, about exactly how much variation the former notion permits. Is data protection legislation that does not explicitly protect legal person data

---

846 For an instructive elaboration of such difficulties in the context of data protection, see CD Raab & CJ Bennett, 'Protecting Privacy Across Borders: European Policies and Prospects' (1994) 72 *Public Administration*, 95–112.

847 See also the approach of the Data Protection Working Party with respect to application of the adequacy criterion in Arts 25–26 of the EC Directive: Data Protection Working Party, *supra* n 308, espec chapt 1.

848 Some support for this can be drawn from the Explanatory Report for the Additional Protocol to the Convention (see *supra* n 278), paras 26–27 (stipulating that the 'adequacy' of protection in the recipient country or organisation must be assessed case by case 'in the light of all the circumstances relating to the transfer'). This parallels the approach adopted pursuant to Art 25(2) of the EC Directive: see Chapter 4 (section 4.4).

849 See also para 67 of the OECD Guidelines' Explanatory Memorandum which indicates that the phrase 'equivalent protection' in para 17 of the Guidelines is to be understood as 'protection which is substantially similar in effect ... but which need not be identical in form or in all respects'. Much the same understanding of equivalency also informs German data protection law: see generally Simitis, *supra* n 56, paras 88ff. Cf EC Commission, *supra* n 316, 5 (footnote 6) (suggesting that 'equivalent protection' requires 'complete juristic similarity').

850 This is also the view of other legal commentators: see, eg, Schwartz, *supra* n 312, 473 & 487; R Ellger, 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 2)' (1991) 7 *RDV*, 121, 131; EC Commission, *supra* n 316, 5 (footnote 6). For further analysis of Arts 25–26, see the works cited *supra* n 316.

at all to be regarded as providing 'equivalent protection' to legislation that does protect such data? Is data protection legislation that explicitly provides legal persons with *some* – but not *all* – of the data protection rights provided by another country's law(s) to be regarded as giving 'equivalent protection' to the latter law(s)? Are some data protection rights to be regarded as carrying more weight than others in the process of weighing up one country's law(s) against another country's law(s)? Is legislation that does not provide legal persons with, say, access rights but provides them with all the other usual rights of data subjects to be regarded as providing 'equivalent protection' to legislation that gives legal persons access rights as well?

As for the first of the above questions, there can be little doubt of a negative answer.[851] The subsequent questions, though, are somewhat more difficult to answer conclusively. While the notion of equivalency probably permits some differences in the form and content of the rights regimes under comparison, these differences must be very minor such that they do not lead to substantial differences in the effective level of protection offered. For instance, a right laid down in a code of conduct that is not legally binding can scarcely be regarded (at least *prima facie*) as equivalent to a legally binding right.[852] Moreover, the recipient country's data protection regime must effectively provide *all* of the *core* rights provided by the sender country's law; ie, all those rights embodying the basic principles of the latter law.[853] Hence, there cannot be real equivalency where one country's law provides legal persons with access rights and the other country's law effectively does not. This notwithstanding, there might be some room for small differences in terms of the scope of each law's exemptions to these rights but where exactly the line should be drawn here is impossible to determine in the abstract.

The important point emerging from this discussion is that application of the equivalency criterion pursuant to the Convention may lead to restrictions on the transborder flow of data on legal persons and collective entities more generally. At the same time, though, insofar as the restrictions concern only data on legal persons or other collective entities, their legitimacy under the Convention is contingent upon the relevant State Party declaring its intention to apply the Convention to the processing of such data. It will be recalled from Chapter 9 (section 9.3) that the Convention permits State Parties to unilaterally extend application of the Convention to information relating to 'groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality' (Art 3(2)(b)). Only Austria, Italy, Norway and Switzerland have issued declarations extending coverage of the

851 See also the policy of the Norwegian DI in the above-cited Esselte Soliditet case. This line appears also to have been adopted by Austria: see Korff, *supra* n 16, 25–27 and references cited therein.

852 A similar line is taken with respect to the equivalency criterion in German data protection law: see Simitis, *supra* n 56, para 91.

853 Again, a similar line is taken with respect to German data protection law: *ibid*, para 92.

Convention to legal person data and, in some cases, data on other collective entities too.[854]

Any restrictions that are applied pursuant to the 'equivalency' standard in Art 12(3) are to pertain primarily to data flow between State Parties to the Convention. Article 12(3) does not apply to data flow from these States to other countries. Indeed, the Convention currently allows State Parties to determine for themselves the criteria for restricting data flow in the latter context. However, once the Additional Protocol to the Convention (adopted in May 2001) enters into force,[855] data flow from a Contracting to non-Contracting State will be governed by rules very similar to Arts 25–26 of the EC Directive (see Art 2 of the Protocol). Thus, the basic criterion applied will be one of 'adequacy' rather than 'equivalency' of protection. The former criterion seems more flexible than the latter; as noted above, 'adequacy' probably permits greater variation in the format and substance of protection provided by the recipient of data. Nevertheless, the questions that arise in relation to that criterion are unlikely to be answered much differently from those provided above in relation to the meaning of 'equivalent'.

What impact will the EC Directive have on transborder flows of data concerning just legal persons or other collective entities? It will be recalled that the Directive differentiates between two main classes of transborder data flows: those within the EU (and EEA) (Art 1(2)) and those from EU (and EEA) Member States to third countries (Arts 25–26).[856] It will be further recalled that privacy-related restrictions on transborder data flow are prohibited in Art 1(2). However, this prohibition does not prevent the restriction of flows of data that are not personal pursuant to the definitional criteria of Art 2(a). This means that EU (and EEA) Member States with data protection laws expressly safeguarding data on collective entities retain the possibility of restricting the transfer of such data to Member States that do not afford 'equivalent protection' for the data,[857] without breaching Art 1(2) of the Directive (unless, of course, the data in question can also be linked to specific individuals). Nevertheless, such restrictions might infringe EC rules on transborder trade, particularly the rules in Art 49 *et seq* of the EC Treaty which are aimed at ensuring the free movement of services within the internal market.[858]

---

854 For Austria, see Declaration of 30.3.1988 (extending coverage to all of the entities listed in Art 3(2)(b)). For Italy, see Declaration of 28.3.1997 (also extending coverage to all of the entities listed in Art 3(2)(b)). For Norway, see Declaration of 20.2.1984 (extending coverage to 'associations and foundations' only). For Switzerland, see Declaration of 2.10.1997 (extending coverage to simply 'legal persons'). For a full list of declarations etc, see <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=>.

855 *Supra* n 278.

856 See further Chapter 4 (section 4.4).

857 See Art 12(3)(a) of the CoE Convention.

858 See generally Nugter, *supra* n 75, chapt IX. Cf Korff, *supra* n 16, 52ff (arguing that such restrictions may very well be legitimate under Community law).

As for the rules in Arts 25–26 on data flows to third countries, again, these do not apply to data on corporate or collective entities only. Thus, the issue of how to interpret the criterion of 'adequate protection' in Arts 25–26 does not need to be addressed with respect to such data.

11.2.4 ORGANISATIONAL BURDENS

The survey questionnaire contained several questions on the organisational burdens of protecting data on legal persons. Each data protection authority was asked whether or not the coverage of legal person data increased its workload, such that it had less time and resources to ensure that data on natural/physical persons were sufficiently protected. The Norwegian and Austrian authorities replied in the negative. According to Sonne, the Danish Data Protection Agency had a similar experience.

Each authority was also asked whether or not the application of its country's data protection Act to data on legal persons resulted in a major increase in administrative expense and procedures for data controllers in the private and/or public sector. Again, the Norwegian and Austrian authorities replied in the negative.[859] Sonne was unable to answer this question in respect of Denmark.[860]

Negative replies were given by the Norwegian and Austrian authorities to the question of whether or not there had been any pressure from business groups to amend data protection legislation so that the latter expressly protected data on individuals only. According to Sonne, there was an absence of such pressure in Denmark too.

11.2.5 THE 'MIXED FILE' AND 'SMALL BUSINESS' PROBLEMS

As noted in section 11.1, the so-called 'mixed file' problem concerns two allegations. One allegation is that there is a risk of double-edged information being processed without regard to data protection laws if the latter only protect data on individuals. Presumably, such processing might occur because those in control of the information believe (or claim to believe) that it relates only to collective bodies. While this risk undeniably exists in theory, gauging exactly how real it is in practice is extremely difficult. The survey questionnaire did not address the allegation directly. One can plausibly assume the risk would be decreased by appropriate publicity campaigns

---

859 In its annual report for 1990, the DI also commented that coverage of legal person data had not led to any significant burden for the Inspectorate or the rest of society: see St meld 43 (1990–91), *Om personvern – erfaringer og utfordringer og om Datatilsynets årsmelding for 1990*, 33.

860 We should also be wary of taking for granted the veracity of the answers of the Norwegian and Austrian authorities to this question. See further section 11.2.6.

alerting controllers and processors of data on collective entities to the possibility of such data also being capable of identifying particular individuals.

The other allegation is that protecting data merely on individuals necessitates an expensive and difficult reorganisation of 'mixed file' registers so that data on individuals are segregated from data on collective bodies. This allegation was addressed in the survey questionnaire. The Austrian DPC responded that it had not observed any difficulties in differentiating between data on legal and natural persons. The Norwegian DI did not provide a direct response here. However, an interview I held on 28.6.1999 with Knut-Brede Kaspersen, Head of the Inspectorate's Legal Section, revealed that the Inspectorate had not received notice of difficulties in differentiating between data on legal and natural persons.

Also noteworthy is the claim of the ICC that 'there is seldom any difficulty in segregating the data of legal and physical persons'.[861] However, the empirical basis for the ICC's claim is uncertain. Further, such segregation is unlikely always to prove straightforward particularly given the difficulty (elaborated upon in Chapter 10 (section 10.3)) in determining what exactly qualifies as physical person data or legal person data pursuant to data protection law.[862]

At the same time, segregation is also required in relation to data protection Acts safeguarding data on both individuals and collective entities. Servicing a request by an individual for access to data on him-/herself pursuant to such Acts (as well as Acts covering information on individuals only) necessitates a process of locating and identifying these data. This process will involve having to segregate these data from other classes of stored data, some of which could relate to collective entities. I have not come across reports of this process being rendered difficult when collective entity data are required segregated from data on individuals. Weighing up all the above factors, the segregation problem is probably fairly minor in practice.

As for the 'small business' problem, it will be recalled this refers to a claim that if data protection legislation covers data on natural persons only, the individual whose business does not have legal person status is given rights under the legislation while an individual whose business is accorded legal person status may not exercise those rights on behalf of the business, even though the business might be of the same magnitude and type as the former business. This allegation was not directly addressed in the survey questionnaire. However, the gravity of the problem is surely reduced if the data protection legislation adopts a broad and flexible definition of what constitutes information on individual, natural persons. Such a definition would allow information relating primarily to an incorporated business (or other type of legal entity) to be treated as personal information if the information can also be linked to a particular individual. Many data protection laws expressly covering data

861 ICC, *supra* n 748, 426.

862 Cf Rossnagel, Pfitzmann & Garstka, *supra* n 638, 66 (noting that technological–organisational developments – particularly the advance towards 'ubiqitous computing' – will make it increasingly hard, as a practical matter, to differentiate between legal person data and data on individuals).

on natural persons only, would seem to operate with such a definition, though as elaborated on in Chapter 10 (section 10.3), some uncertainty pertains to the exact nature of the link that is required between the data and an individual before the data can fall within their ambit. In general, however, establishing the requisite link should be easier the smaller the number of individuals is who are running or connected to the business. Accordingly, the 'small business' problem could well be somewhat of a misnomer. It seems clear, for instance, that a considerable amount of data on a one-person company are likely to be covered.[863]

11.2.6 CONCLUSIONS ON SURVEY RESULTS

The information presented in section 11.2 shows that the practical consequences of Norway extending data protection rights to legal persons *appear* not to have been as harmful or burdensome (for either the collective entities concerned, data protection authorities or individuals) as some people have predicted. This would also *seem* to be true for Austria and Denmark. Yet one should exercise caution when drawing firm conclusions here. The empirical basis for drawing any such conclusions is fairly thin. Moreover, some of the responses received from the questionnaire leave unanswered a large number of questions as to *why* the extension of data protection rights to legal persons appears to have been without detrimental, practical consequences in Norway and Austria.

For example, the responses to the questionnaire reveal that coverage of legal person data by the data protection laws of Norway and Austria has not been overly burdensome for the data protection authorities or legal persons in the two countries, but the responses do not indicate why this has been the case. We can envisage several hypotheses to explain the apparent lack of burden. One hypothesis could be that many data registers containing data on legal persons also contain data on individuals; hence, these registers would have to be regulated by data protection law even if the latter protected data on individuals only. A second hypothesis could be that many data controllers in Norway and Austria are/were unaware of the fact that the data protection laws of their respective countries extend(ed) to regulate data on legal persons; hence, they do/did not bother to notify the Norwegian or Austrian data protection authority when they process(ed) such data. A third hypothesis could be that legal persons rarely complain(ed) to the Norwegian or Austrian data protection authority about breaches of their data protection rights. Accepting the validity of the latter hypothesis leads, in turn, to further questions: eg, do/did legal persons rarely complain because (i) they do/did not know of these rights, or (ii) the rights are/were rarely breached, or (iii) they are/were largely indifferent to, or do/did not suffer from, such breaches? Finding reliable data to test the validity of the above hypotheses and

863 Cf the decision of the NZ Complaints Review Tribunal, *supra* n 795.

to answer the above questions is essential if we are to gain a complete and accurate picture of the practical consequences of extending data protection rights to legal persons in Austria and Norway.

It should also be remembered that I only attempted to canvass the experiences of (a few) data protection authorities. No attempt was made to canvass, say, private corporations' views on the consequences of the laws in question. At the same time, one would expect that private corporations experiencing major practical problems with the laws would bring these problems to the notice of the relevant data protection authorities. As Hogrebe has pointed out, data protection authorities are a 'good, if not the best, source of information as regards an overall evaluation of the concrete practical problems which might occur at the level of individual companies'.[864] This is because these authorities 'would receive directly any objections which private companies might have due to practical problems with the compliance with legal person data protection'.[865]

No matter how comprehensive any survey of practical consequences might be, one would always have to exercise caution in extrapolating from Norwegian (and/or Austrian, Danish, etc) experiences in extending data protection rights to certain kinds of collective entities. It would be foolish to claim, for instance, that as there appear to have been few, if any, problems in giving legal persons data protection rights in Norway (and/or Austria, Denmark, etc) then there will also be few, if any, such problems in other countries. There is evidence to suggest that the nature of the consequences of extending data protection rights to collective bodies in a particular country depends greatly on the nature of the corporate and legal cultures in that country.

For example, the apparent absence of problems associated with giving legal persons data protection rights under Norway's PDRA appears to have been due partly to the careful manner in which the Data Inspectorate implemented the Act. The lack of problems appears also to have been due to the fact that legal persons in Norway showed little interest in exploiting their rights under the legislation. This lack of interest could reflect in turn a lack of awareness of the legislation,[866] but it might also reflect the relatively unlitigious and unaggressive character of Norwegian corporate culture. Eckhoff writes, for example, that those who demand access to government-held information pursuant to Norway's *Act on Openness in Administration* (AOA) have not pursued their demands as aggressively as many of those who demand access to information pursuant to the equivalent legislation in the USA.[867] While numerous court cases have arisen concerned with corporations' attempts to gain access to business information pursuant to the US federal *Freedom*

---

864 Hogrebe, *supra* n 635, 5.

865 *Id*.

866 The Data Inspectorate stated, in response to the survey questionnaire, that it thought Norwegian companies generally had little detailed knowledge of the PDRA.

867 T Eckhoff (& E Smith), *Forvaltningsrett* (Oslo: TANO, 1994, 5th ed), 451.

of Information Act of 1970,[868] Eckhoff and Smith write that, to their knowledge, there has not been a single Norwegian court case in which the application of Norway's AOA has been at the centre of dispute; administratively-handled complaints centred on the Act also seem to have been seldom.[869] Of course, drawing firm conclusions about the reasons for this apparent national difference in litigation levels is difficult. Even so, it gives some grounds for envisioning that, were corporations in the USA given data protection rights, their attempts to exploit these rights would be much more aggressive and contentious than has been the case in Norway.

This does not necessarily mean, though, that such attempts would be crowned with success or would result in significant distortions of competition between enterprises. The outcome of such attempts would depend on a combination of many factors. These factors include the manner in which the legislative provisions are formulated and the manner in which they are interpreted and implemented, not just by data subjects and data controllers, but also by data protection authorities and other arbitrators. Moreover, it is possible that if the latter consistently beat back aggressive and contentious corporate attempts to exploit data protection rights then the scale and intensity of these attempts would diminish over the long term, thereby diminishing pressure on both arbitrators and data controllers.

Nevertheless, we should be aware of the possibility of legal persons (or other organised collective entities) being more aggressive than they have been in Norway, in exploiting any data protection rights they are given. This aggression might result, at least in the short term, in a situation in which data controllers, data protection authorities and other relevant bodies are burdened to a greater extent than seems to have been the case in Norway.

11.3 Actual Cases of Data Protection for Organised Collective Entities

In this section, summaries are given of actual cases in which the Danish and Norwegian data protection authorities acted to regulate the processing of data on organised collective entities. The cases summarised below do not constitute the entire body of cases involving protection of such data by these authorities. However, all of

868 5 USC § 552. For overviews of these cases, see, eg, Lindsay, *supra* n 721, 926–935; Rankin, *supra* n 807, 228–246.

869 Eckhoff & Smith, *supra* n 36, 436; Eckhoff (& Smith), *supra* n 867, 451; cf Frihagen, *supra* n 831, 282. Nevertheless, the Ombudsman has handled a number of complaints centred on the AOA: see, eg, Frihagen, *ibid*, 280–281, 414–416 and references cited therein. It would also seem that the Ministry of Justice's Legal Section (Lovavdeling) has resolved a number of complaints by giving its opinion on the matter in question; such opinions tend to carry significant weight in practice: *ibid*, 278 and references cited therein.

the following cases are mentioned in the authorities' annual reports. One can reasonably assume, therefore, that these cases were seen by the two authorities either as being representative of other cases or as involving important decisions of principle.

The following presentation is not concerned with the merits of the decisions made in each of these cases. Rather, it is concerned with showing there is a wide variety of people and organisations interested in information on collective entities and, correspondingly, a wide variety of contexts in which data protection laws can be implemented to safeguard this information.

11.3.1 DENMARK

Case 1

In its annual report for 1992, the Danish DPA describes a case in which a bank planned to match its corporate customer data records with other records of legal person data gathered by a private information agency.[870] The latter records were compiled from data found in various publicly accessible registers, such as the Central Enterprises Register run by the Danish Bureau of Statistics. The records embraced comprehensive data on companies, including their respective names and addresses, dates of establishment, branches of activity, numbers of employees, and profit and loss accounts. The main reasons for the bank's matching plans were to update its own customer data records and to engage in a selective marketing of its services *vis-à-vis* companies that were not already customers. The planned matching would utilise search criteria that did not allow for identification of individuals attached to the companies.

The DPA only permitted matching to go ahead in relation to data on companies that were already customers of the bank. The Agency found that matching data on other companies with the aim of marketing would breach ss 3(1) and 4(2) of the *Private Registers Act* (PRA). These provisions permitted organisations to register and disclose data to the extent such registration and disclosure were a 'natural' part of the organisations' 'normal' activities. Thus, for the DPA, the planned utilisation of the non-customer data fell outside the natural part of the normal operations of a bank.

Case 2

In its annual report for 1990, the DPA writes of a case concerning the activities of two local environmentalist organisations.[871] The organisations applied to the DPA for permission to set up a data register over the effects of various production processes

---

870 See Registertilsynet, *Årsberetning 1992* (Copenhagen: Registertilsynet, 1993), 96–98. All following references to the case are taken from this part of the DPA's report.

871 See Registertilsynet, *Årsberetning 1990* (Copenhagen: Registertilsynet, 1991), 81–83. All following references to the case are taken from this part of the DPA's report.

on the natural environment. The aim of the register was to catalogue, highlight and compare the degree to which various companies and business enterprises carry out their work in an environmentally friendly manner. Data to be set down in the register included the name and address of each company/enterprise, its ownership structure, financial state and field of activity, the products it makes and resources used to make them, the pollution/industrial waste created in its production processes along with the measures it takes to reduce or get rid of such waste, and details of any cases in which it has been accused of breaching environmental protection laws. These details were to be passed on to the media and public authorities in order to stimulate debate over environmental issues and bring pressure on polluting industries to adopt cleaner production methods.

The DPA approved of the general purpose of the planned register but was concerned to ensure the various data appearing in it were correct. Accordingly, the Agency stated that only data supplied by the companies/enterprises themselves could be registered, along with data that could be collected from official, publicly available sources, such as the Bureau of Statistics. The DPA also requested that prior to setting up the register, the environmentalist organisations send to the Agency details on the location of those responsible for running the register, and on the measures that would be taken to make the register secure from unauthorised access. Finally, the DPA stated it could not allow the registration and disclosure of information concerning possible legal offences committed by a company/enterprise.

The Agency justified the latter restriction by stating that such registration and disclosure would breach ss 3(1) and 4(2) of the PRA.[872] It seems, therefore, that the Agency held the registration and disclosure of legal offences committed by a company/enterprise as not being a natural part of the environmental organisations' normal activities (!). In addition, the DPA held that the registration and disclosure of this information would breach ss 3(2) and 4(1) which placed strict limits on registration and disclosure of certain classes of sensitive data, including data on legal offences. Yet both provisions were formulated such that they only embraced data relating to individuals. Hence, the application of the two provisions in this particular case seems awkward. However, according to Jette-Marie Sonne, the Agency only applied ss 3(2) and 4(1) in relation to information on the legal offences of *one-person* enterprises. The Agency allegedly held such information as protected by these provisions because the information related, in effect, to identifiable individuals.[873]

Case 3

In its annual report for 1989, the DPA describes a case concerning an association set up to collect and distribute information on publishing companies and their respective

872 The gist of these provisions is set out above under case 1.

873 According to Sonne, this rationale for the application of ss 3(2) and 4(1) was only to be found in the Agency's internal case documents, which are not available for public inspection.

publications.[874] Members of this association were primarily large enterprises that marketed themselves and their products by placing advertisements in the printed media. Information collected by the association on publishing companies and their respective publications was continually updated and sent out in the form of a newsletter to association members eight to twelve times per year in order to guide the members in placing their advertisements. The newsletter was also sent to the association's sister organisations in the other Scandinavian countries and, on some occasions, to the Danish police.

The newsletter included information on the prices charged by the various publishing companies for placing advertisements in their respective publications and on actual experiences association members had with these companies. Such experiences included cases in which companies allegedly misled, deceived or cheated association members.

The DPA held the activities of the association to be largely in accordance with the *Private Registers Act*. At the same time, it set down limits on these activities. Citing ss 3(2) and 4(1) of the Act, the DPA held that any information relating to the possible commission of legal offences by a publishing company could not be registered or passed on without the consent of the company itself, unless this was allowed by another law. The Agency also held that any such information a company had already collected must be erased pursuant to s 23(1). The Agency went on to state that, pursuant to ss 3(6) & 3(7), the association must refrain from blacklisting companies in its newsletter, without first applying for permission to do so from the DPA. Finally, the Agency held that information published in the newsletter must be set out in a neutral manner and be based on objective, verifiable criteria.

It is interesting to observe that the DPA applied ss 3(2) and 4(1) in this case. As noted in relation to case 2, these provisions applied *prima facie* to protect sensitive information on individuals only. Yet in this case, the DPA applied the provisions for the benefit of publishing companies. In case 2, the Agency applied these provisions for the benefit of companies/enterprises owned and run by single individuals. According to Sonne, the case 3 documents fail to indicate whether or not the publishing companies were one-person enterprises also.

Case 4

In its annual report for 1989, the DPA refers to a case concerning a computer-service bureau acting additionally as an address vendor.[875] The bureau ran a register containing information on some 350,000 private business enterprises and public institutions. This register contained the names, addresses and telephone numbers of these enterprises and institutions, along with information on their respective size,

874 See Registertilsynet, *Årsberetning 1989* (Copenhagen: Registertilsynet, 1990), 74–77. All following references to the case are taken from this part of the DPA's report.

875 See Registertilsynet, *supra* n 874, 60–62. All following references to the case are taken from this part of the report.

branch of activity, number of employees, financial turnover, share capital, imports and exports, and names and titles of their key personnel. The bureau applied for permission from the Inspectorate to allow its clients (which were private business enterprises) to match their own customer registers with the bureau's register. The matching would give the clients the chance to add significant information to their own customer registers which would then assist them in the marketing and sale of their products.

The DPA allowed the planned matching to occur, subject to several conditions. Any information produced as a result of the matching could only be used for marketing purposes. Further, all one-person enterprises listed in the above-mentioned registers had to be informed that information on them might be matched (cf PRA, s 4(5)).

Case 5

In a case from 1988, five local trade councils asked a school for commerce and business to conduct a survey of business enterprises located in the councils' respective districts.[876] The results of the survey were to be stored on the school's computer system. The DPA held that the planned register of business enterprises should not be established until it was made clear exactly who would be responsible for maintaining and running the register and hence liable for possible breaches of the *Private Registers Act*. The DPA also held that neither the school nor any ordinary computer-service bureau could be accorded responsibility because establishment of this type of register could not be considered a natural part of the normal activities of either organisation. Accordingly, the five local trade councils formed a special association to take responsibility for establishing and running the register.

Case 6

The DPA reported a case in 1981 concerning an organisation set up by two trade unions to register details on the wages paid out by various companies to their respective employees.[877] The Agency permitted registration, deeming this to be a natural step in the normal activities of a trade union (cf PRA, s 3(1)).

11.3.2 NORWAY

Case 1

In 1985, Norway introduced measures to cease direct trade with South Africa. One measure proposed by the Norwegian parliament was to pass a law allowing for the establishment of a register over Norwegian shipping companies that continued to ship goods to South Africa in breach of trade sanctions. A provision in the proposed

876 See Registertilsynet, *Årsberetning 1988* (Copenhagen: Registertilsynet, 1989), 60–61. All following references to the case are taken from this part of the report.

877 See Registertilsynet, *Årsberetning 1981* (Copenhagen: Registertilsynet, 1982), 78–79.

law also allowed for the register to be made public. This provision was criticised by the Data Inspectorate when it was asked for its comments on the proposed law.[878] The DI stated that the provision represented a modern version of the pillory. It expressed unease over publicising the contents of the register as a means of bringing public moral pressure to bear on shipping companies so they would halt activities that were not forbidden by other laws at the time. The proposed law was not enacted.

Case 2

In 1990, the Norwegian postal service sought permission from the DI to set up a central register of company addresses.[879] It planned to retrieve these addresses from a database maintained by the Norwegian Central Bureau of Statistics. Although the DI had no objections to the setting up of such a register, it refused to allow retrieval of company addresses in the manner planned. The Inspectorate held that the Central Bureau of Statistics is only allowed to store and process data for statistical purposes, and that the proposed use of the data by the postal service would involve exploitation of the data for commercial purposes. The DI added, however, it did not object to the postal service retrieving company addresses from another source.

Case 3

In 1990, a Norwegian credit-reporting agency proposed to include as part of its standard credit rating of a company or person information on the number of times a company/person had been the subject of previous requests for credit information.[880] The DI disallowed the proposal, holding that such information did not properly constitute credit information.

Case 4

In 1987, a Norwegian firm sought permission from the DI to set up a database containing detailed information on approximately 5000 Norwegian companies.[881] The firm planned to collect the information from these companies over the telephone. The database was to hold data on each company's structure, products and services, business turnover, number of employees, managerial staff and computer system. The firm wanted to sell these data to suppliers of computer equipment, and also use the data in telemarketing operations it carried out on behalf of other firms.

The DI refused permission to set up the proposed database. In the DI's opinion, such a database would increase the risk that company secrets are divulged, and that

878 See Datatilsynet's letter of 7.10.1985 to the Norwegian Department of Trade and Shipping (ref: 85/1024-2 ED/-). See also St meld 29 (1986–87), *Datatilsynets årsmelding 1985*, 7.

879 See St meld 18 (1992–93), *Årsmelding for Datatilsynet 1991*, 12. All following references to the case are taken from this part of the report.

880 *Id.* The case is also described in Bygrave, *supra* n 37, 105–106.

881 See St meld 48 (1987–88), *Datatilsynets årsmelding 1987*, 5. All following references to the case are taken from this part of the report.

the information in it concerning companies' computer systems could be exploited by outsiders for illegal purposes.

11.3.3 CONCLUSIONS ON THE ABOVE CASES

The cases set out above show it is wrong to claim that past Norwegian and Danish data protection legislation has not been of any practical benefit for organised collective entities (as data subjects) and for the individuals who constitute them. In some of the cases, however, it is somewhat difficult to assess the extent to which this practical benefit was due to the fact that the legislation *expressly* regulated the processing of data on organised collective entities. This difficulty arises partly because of uncertainty over the exact content of the registers and collective entity data subjected to regulation in the above cases.[882] The difficulty also arises because of uncertainty over the exact ambit of data protection laws that do not expressly regulate the processing of data on collective entities – a point elaborated upon in Chapter 10 (section 10.3).

Nevertheless, it appears doubtful that in all or most of the cases set out above, the data protection authority concerned would have been legally able to step in and regulate the processing of the information in question, if the relevant data protection law did not expressly extend to data on collective entities. Hence, the fact that the Norwegian and Danish data protection laws expressly covered such data would seem to have given the two countries' data protection authorities an extra leg to stand on when challenging the way in which private and public sector bodies process information. In particular, it made it easier for the two authorities to place limits on information processing in a situation where:

1) uncertainty existed over whether or not the information in question may qualify as information relating to individuals; but
2) it was certain the information related to (organised) collective entities; and
3) the processing of this information could adversely affect the entities concerned and thereby the individuals constituting them.

Similarly, in this sort of situation, the chance of *data controllers* taking the necessary data protection measures is clearly increased by the fact that the data protection laws expressly extended to data on collective entities.

Moreover, in the above sort of situation, the action causing injury to a particular collective body and to the individuals attached to it, might be directed only at the collective body as such. In this case, there might be no legal redress for the

882 More precisely, the important question here concerns the degree to which these registers and data allow(ed), directly or indirectly, identification of particular individuals. I managed only to get access to the relevant case documents of the Norwegian DI, and these fail to provide a clear answer to the question. The relevant case documents of the Danish DPA are not available for public inspection.

individuals *qua* individuals because the action that caused injury was directed only at the collective body as such, without singling out specific individuals. Concrete examples of this sort of occurrence can be found in case law on defamation.[883]

As shown in Chapter 10 (section 10.3), it is difficult to determine in the abstract and on the basis of the relevant legislative provisions to what extent data relating *prima facie* to a collective entity may also be linked to a specific individual and thus be characterised as 'personal data' pursuant to data protection laws that refrain from expressly protecting data on collective entities. Nevertheless, as concluded in that chapter, information on most types of collective entities (particularly large ones) is extremely unlikely to qualify as information on specific individuals and hence fall within the protective ambit of the laws concerned. Given that a collective entity as such is incapable of seeking redress for breach of these laws' principles, the individuals attached to such an entity could also be left without such redress when the breach concerns data that cannot be linked to any one of them specifically. This legal shortfall in the protection of individuals' interests would be overcome by extending data protection rights to collective entities as such.

The cases outlined in this section show that there are, and will probably continue to be, a wide variety of occasions in which data protection authorities and legislation could play an active role in regulating the use of information on collective entities. Nevertheless, the number of cases mentioned in the annual reports of the Danish and Norwegian data protection authorities and which involve protection of collective entity data only, is very small compared to the number of cases mentioned in these reports which involve the data protection authorities acting to protect data on individuals only.[884] In some of the cases presented in this section (eg, the case concerning the Norwegian postal service), the practical benefits gained for collective entities as data subjects appear rather minor. At the same time, it would be unrealistic to expect these benefits to approach the spectacular. Data protection rights are, for the most part, basically simple, procedural rules to ensure that certain types of information are processed fairly, responsibly and lawfully. As such, they tend to be

---

883 See, eg, the Norwegian Supreme Court decision of 20.12.1985 concerning defamation of Greenpeace (Rt 1985, 1421). In this matter, Greenpeace's Danish branch sued a Norwegian newspaper for printing an article which characterised Greenpeace as a terrorist organisation. Several members of the branch's steering committee also sued the newspaper for defamation of them personally. The Supreme Court held that only Greenpeace as such could sue for defamation because the newspaper article did not allow for the singling out of individuals within the Greenpeace movement: Rt 1985, 1425. Had Greenpeace as such not been able to sue for defamation, the individuals behind the organisation would have been left without any form of legal redress for the injury they suffered personally. For other examples of similar cases in Norwegian law, see, eg, J Andenæs & A Bratholm, *Spesiell strafferett* (Oslo: Universitetsforlaget, 1996, 3rd ed), 153–154; JH Mæland, *Ærekrenkelser* (Bergen: Universitetsforlaget, 1986), 104ff, 365–367. For examples of similar cases in English law, see, eg, PF Carter-Ruck & HNA Starte, *Carter-Ruck on Libel and Slander* (London: Butterworths, 1997, 5th ed), 56–58.

884 See also the results set out in the internal note of the DPA, *supra* n 820; *Behandling af personoplysninger*, Bet 1345 (Copenhagen: Statens Information, 1997), 167.

rather pedestrian and modest in terms of their character and tangible effect. Yet this does not mean that they (or the principles and ideals they embody) are unimportant, particularly in this age of electronic interpenetration.

12. Data Protection Interests of Collective Entities

12.1 The Privacy-based Argument against Data Protection Rights for Collective Entities

One of the main reasons cited for not extending to collective entities (primarily legal persons) rights under data protection laws has been a claim that these laws protect interests or values relating only to individuals. The proponents of this claim usually sum up these interests or values in terms of 'privacy', sometimes in terms of 'personal integrity'. Accordingly, I term the above claim as the 'privacy-based' argument against extending data protection rights to collective entities. It is with the strengths and weaknesses of this argument that this chapter is mainly concerned.

12.1.1 Elements of argument

The privacy-based argument can be expressed in the form of a syllogism. The first proposition of this syllogism is that the rationale for data protection law is essentially the safeguarding of privacy. The second proposition is that the concept of privacy cannot apply to collective entities. Putting these two propositions together results in the conclusion that data on collective entities cannot qualify for protection under data protection legislation.

The privacy-based argument against giving data protection rights to collective entities is hardly ever expressed along such clear-cut, syllogistic lines. This is because the first of the above-mentioned propositions is rarely set out expressly by the proponents of the argument. Yet embracing the second proposition obviously cannot lead to denial of the appropriateness of giving collective entities rights under data protection laws, unless the first proposition is also embraced.

The privacy-based argument is usually directed not at collective entities generally but at one (albeit large) category of such entities – namely, legal persons. Hence, much of the discussion below focuses on the needs and rights of corporations. However, the argument is also logically applicable to other forms of organised collective entities and even to mere groups. Discussion of the needs and rights of the latter, though, is undertaken mainly in Chapter 15.

An example of the privacy-based argument against giving data protection rights to collective entities can be found in the report of the UK Committee on Data Processing (the Lindop Committee). One of the Committee's reasons for not giving data protection rights to collective entities (primarily legal persons) was that 'privacy is essentially something personal, something for which individuals have a desire, or claim a right'.[885] This seems also to have been the view of the OECD Working Party on Information, Computer and Communications Policy. As one of its grounds for excluding data on collective entities from coverage by the OECD Guidelines, the Working Party stated that

> 'the notions of individual integrity and privacy ... should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality.'[886]

Common for most instances in which the privacy-based argument is run is that the two propositions constituting the argument are set out as mere assertions; little or no attempt is made to argue *why* the propositions are valid. The first proposition (on the relationship between privacy and data protection laws) is examined in detail in Chapter 7 (sections 7.2.1 and 7.2.5). Hence, there is no need to deal with it extensively here. It suffices to say that the discussion in that chapter shows how privacy, whilst being one of the main values safeguarded by data protection laws, is not the only such value. In the present chapter, it is the second proposition (on the application of the privacy concept to collective entities) that requires detailed examination.

12.1.2 RELATIONSHIP BETWEEN PRIVACY AND COLLECTIVE ENTITIES

If one accepts the proposition that data protection laws have the safeguarding of privacy as at least one of their main concerns, how should one determine the type of person/entity embraced by the concept of privacy? An interim answer is: only with difficulty, given the nebulous nature of the privacy concept and the haphazard way in which it is often employed.

There are two main grounds for claiming the concept of privacy cannot apply to collective entities. The first has to do with common usage of the concept, the second with the functions and values served by privacy. As shown below, neither of these grounds completely shuts out the possibility of the privacy concept applying to collective entities.

---

885 Lindop Committee, *supra* n 505, 156, para 18.36.

886 Paragraph 33 of the Explanatory Memorandum to the OECD Guidelines.

Usage of privacy concept

Few would dispute that the concept of privacy is employed in everyday discourse almost exclusively in relation to individuals. This is also the case when it comes to academic discourse. Much of the academic literature on privacy and data protection issues completely ignores the notion or possibility of privacy for collective entities.[887]

Few would also dispute that the vast majority of people associate the concept of privacy primarily with individuals. From this it would not be hard to extrapolate that most people would hesitate about applying the concept to collective entities. Yet it would be hard to extrapolate that most people thereby refuse to accept the concept of privacy as applicable, albeit secondarily, to at least some kinds of collective entities. Of course, some evidence to support the latter extrapolation exists. This is to be found in the statements – cited at the beginning of this chapter – of various committees charged with examining data protection issues. There are also other examples of a refusal to apply the privacy concept to collective entities.[888]

Nevertheless, a considerable number of jurists and philosophers do employ the concept of privacy in relation to organised and/or non-organised collective entities.[889] Many of these persons (eg, Benn, Blekeli, Posner and Stigler) seem to regard this usage of the concept as completely natural and unproblematic in the sense that they do not make any attempt to defend the usage. Many of them come from North America. It could be there is greater acceptance there (at least in some academic circles) than elsewhere of the notion of corporate and/or group privacy.[890]

Expansive potential of privacy concept

The expansive potential of the privacy concept is considerable. This is partly because of its ambiguity, which not only creates a considerable amount of confusion over the concept's proper scope of application but also makes the concept sufficiently pliable to assimilate a range of related concepts, such as secrecy and confidentiality, which have traditionally been employed in relation to the needs and interests of corporate entities.

---

887 Examples are Flaherty, *supra* n 267 and Miller, *supra* n 335.

888 See, eg, Bok, *supra* n 63, 13; LC Velecky, 'The Concept of Privacy', in JB Young (ed), *Privacy* (Chichester: Wiley, 1978), 13, 21.

889 See, eg, D Amann, '*Publicker Industries v Cohen*: public access to civil proceedings and a corporation's right to privacy' (1986) 80 *North Western University L Rev*, 1319–1354; Benn, 'The Protection and Limitation of Privacy', *supra* n 590, 603–604, 609; Blekeli, *supra* n 505, 24; Lindsay, *supra* n 721, 915–935; Lowell, *supra* n 721, 407–49; RA Posner, 'An Economic Theory of Privacy', in FD Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), 333–345; DP Schack, 'The right to privacy for business entities' (1984) 24 *Santa Clara L Rev*, 53–63; Schafer, *supra* n 502, 14; GJ Stigler, 'An Introduction to Privacy in Economics and Politics' (1980) 9 *J of Legal Studies*, 623, 625; Westin, *supra* n 335, 42–51.

890 At the same time, as noted in Chapter 9 (section 9.4), the bulk of judicial authority in the USA is presently against extending to corporations any legal right to 'privacy' as such. Furthermore, federal and State legislators in the USA have not given statutory data protection rights to corporations.

The expansive potential of the privacy concept is strengthened by the fact that the bulk of definitions of privacy are personality-neutral; ie, they are capable, in substance, of applying to legal persons and other collective entities as well as to individuals. The only definitions of privacy that are not personality-neutral are those merely embracing 'intimate' aspects of persons' lives. The use of an adjective like 'intimate' gives the definitions a distinctly emotive, personal connotation that is hard to apply to corporate bodies though not necessarily to all small collective entities.[891] However, these types of definitions are of limited relevance or use for the purposes of data protection law.[892]

Functions and value of privacy

Another argument for refusing to apply the privacy concept (and privacy/data protection rights) to collective entities is that the functions and value of privacy are both originally and inextricably connected to the unique needs of individuals. This argument is clearly exemplified in the work of Stevenson. For Stevenson, the privacy concept is applicable only to individuals because 'the social conventions and legal rights ... established to protect personal privacy are founded on human values and human traits'.[893] Corporations, he continues, 'can make no *direct* claim to the benefits of those social and legal rules, for their fictional 'personalities' do not partake of the characteristics wherein the rules find their basis'.[894]

Harris takes a similar line when arguing against giving incorporated and unincorporated associations a legal right to privacy:

> 'The right [to privacy] was developed to protect human sensibilities, and was grounded on the physical and psychic realities of the ability of human beings to react emotionally. Therefore, it follows that the tort can have no existence where the consequences which gave rise to it cannot occur. [...] Clearly, neither a corporation nor an unincorporated association can feel the distress which is the basis for the protection of the right to privacy.'[895]

---

891 Cf Bok who, while asserting that the concept of privacy is a 'metaphor for personal space' which cannot be applied to 'collective enterprises', concedes that 'group privacy' can exist if the group is small and close-knit, such that the members' own sense of privacy 'blends with an enlarged private space of the group': *supra* n 63, 13. She gives an example of such a group as being 'secret societies' that have as their principal distinguishing feature 'secrecy itself: secrecy of purpose, belief, methods, often membership': *ibid*, 46.

892 See further Chapter 7 (section 7.2.1).

893 RB Stevenson Jnr, *Corporations and Information – Secrecy, Access, and Disclosure* (Baltimore/London: Johns Hopkins University Press, 1980), 51.

894 *Id.*

895 PR Harris, 'A Right to Privacy for Incorporated and Unincorporated Associations?' (1965) 16 *Virginia L Weekly DICTA Comp.* 97, 98.

Much the same line was recently taken by several judges in the decision by the High Court of Australia (HCA) in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*.[896] In refusing to find that a corporation itself may enjoy a right to privacy as such under Australian law, Gummow and Lehane JJ (with whom Gaudron J agreed) held that the sensitivity of corporate entities is peripheral to the proper concern of privacy claims. In their view, as a '*persona ficta* created by law', a corporation necessarily 'lacks the sensibilities, offence and injury to which provide a staple for any developing law of privacy'.[897]

The above type of argument expresses what Allen calls 'metaphysical' and 'teleological' grounds for denying the application of the privacy concept and privacy rights to corporate entities.[898] A metaphysical element is present because the argument 'reflects a theoretical conception of the fundamental essence of corporate existence'.[899] Legal persons are 'deemed incapable of possessing privacy rights both because of what they are and because of what privacy is'.[900] There is also a teleological element in the above statements by Stevenson, Harris and the HCA judges since the statements embody 'a view about the design or purpose of ascribing particular rights'.[901]

A difficulty with accepting the metaphysical ground is that most definitions of privacy are, as pointed out above, personality-neutral. Where the metaphysical ground is strongest is in relation to accounts of the value and functions of privacy rather than of the privacy concept itself. Accounts of the value and functions of privacy are dealt with below. As for the related teleological ground, it suffers from two major problems. In the words of Allen:

> 'First, it [the teleological ground] implies that rights of action are strictly limited by the purposes for which they have been recognized in the past, seemingly and implausibly rejecting the possibility that they may acquire similar or analogous new purposes. Second, it implies that the privacy tort has a distinct purpose which became a matter of settled doctrine early in the life of the action, rather than a developing set of purposes subject to flexible interpretation in response to and demanded by practical concerns.'[902]

---

896 [2001] HCA 63.

897 *Ibid*, para 126. See further LA Bygrave, 'A right to privacy for corporations? *Lenah* in an international context' (2002) 8 *PLPR*, 130–134.

898 See Allen, *supra* n 721, 613–617.

899 *Ibid*, 613.

900 *Ibid*, 614.

901 *Ibid*, 215.

902 *Ibid*, 616. While Allen (like Harris) is writing primarily about the proper ambit of a *legal right* to privacy, her comments are relevant, nevertheless, to discussion on the proper ambit of the *concept* of privacy (quite apart from its legal manifestations).

The mere fact that the origins of the privacy concept (and privacy rights) lie in the need to protect human sensibilities from outside interference does not mean the concept (and privacy rights) cannot be applied subsequently to legal persons. Legal doctrine, for example, is full of concepts and rules that arose initially to service the needs of individuals but later have come to service also the needs of corporations. An example of such a concept is defamation, which is closely related to privacy. In many countries (eg, Denmark, England, France, Germany and Norway), legal persons have been given a right to sue for defamation, though the exact extent of this right varies.[903] The extension to legal persons of this right is due to recognition that defamation need not always cause only emotional harm; it can also damage other interests that are of value for legal persons.[904]

Whether or not the same can be said for breach of privacy depends on how one categorises the range of interests protected by privacy. For writers like Stevenson and Harris, privacy protection would seem to be concerned only with preventing *emotional* harm. Indeed, much of the literature on the value of privacy is almost exclusively concerned with individuals' emotional needs.[905]

Nevertheless, it is possible to take a more expansive view of the value of privacy.[906] This is pertinently demonstrated in the work of Westin. In the following, Westin's work is analysed in detail as he is one of the first (and few) scholars who have attempted to set out systematically the case in favour of applying the privacy concept to organised collective entities. Moreover, his analysis of the value of privacy for such entities has been applied (often uncritically) by other writers who argue that organisations need privacy and data protection rights.[907] In the following, Westin's analysis of 'organizational privacy' is compared with several theories on

---

903 See generally Mæland, *supra* n 883, 98–105.

904 See further *infra* n 953 and accompanying text. At the same time, the nature of a legal person has meant that, under English and Australian common law, for example, such a person cannot sue for disparagement of 'personal' reputation, only for disparagement of its business operations, including, for instance, allegations that it is in financial difficulties or that its services are a sham: See, eg, *Bargold Pty Ltd v Mirror Newspapers Ltd* [1981] 1 NSWLR 9; *London Computer Operators Training Ltd v British Broadcasting Corporation* [1973] 2 All ER 170. Cf the distinction in Norwegian law between defamation that violates one's 'feeling/sense of honour' ('æresfølelse') and defamation that either damages one's 'good name and reputation' ('gode navn og rykte') or exposes one to 'hate, contempt or loss of confidence, which is necessary for one's position or business' ('hat, ringeakt eller tap av den for hans stilling eller næring fornødne tillit'). Legal persons as such are limited to suing for the latter type of defamation (which is punished in s 247 of the Norwegian *Penal Code*), as the former type (punished in s 246 of the *Penal Code*) only affects emotions: See, eg, Mæland, *supra* n 883, 103 (citing the Norwegian Supreme Court's decision of 15.12.1979 concerning defamation of 'Oslo Bolig og Sparelag' (reported in Rt 1979, 1606, 1615).

905 See the early parts of Chapter 7 (section 7.2.2).

906 See the later parts of Chapter 7 (section 7.2.2).

907 See, eg, R Vandvik, *Individets og bedriftens integritet i data-alderen*, seminar paper (Bergen: Norwegian School of Economics and Business Administration, 1970), 37–38; Rydén, *supra* n 716, 119. Cf Ims, *supra* n 582, 80–82 (building more indirectly upon Westin's analysis).

the nature of legal persons and with the work of Edward Bloustein on the notion of 'group privacy'.

Westin's analysis of value of privacy for organisations
Recall Westin's definition of privacy:

> 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'[908]

According to Westin, privacy serves four main functions: it provides for 'personal autonomy', 'emotional release', 'self-evaluation', and 'limited and protected communication'.[909] Westin convincingly argues these functions are not just of relevance to individuals, they are also important for organisations.

In relation to 'autonomy', Westin makes the obvious point that, as with individuals, organisations need to retain certain secrets or zones of privacy if they are to avoid being manipulated or dominated by others. He claims, for example, that if a business group is to remain commercially viable and independent then its trade secrets and business decisions must be kept confidential.[910] Few would disagree with the substance of this claim although they might have problems accepting that what is at stake here is organisational *privacy* as opposed to, say, secrecy.[911]

On the topic of 'release', Westin advances rather more controversial claims. He argues organisations need to be able to conduct their affairs without having to keep up a 'public face'.[912] He defends the need for a 'gap between public myth and

---

908 Westin, *supra* n 335, 7. Westin offers a second definition of privacy as 'the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve': *id.* It is, however, the first definition that has proven most influential.

909 Westin, *supra* n 335, 32–39. See further Chapter 7 (section 7.2.2).

910 *Ibid*, 43.

911 Westin does not consider the relationship between privacy (as he defines and uses the term) and secrecy. Concomitantly, he does not show why it should be *privacy* that is of value to organisations as opposed to *secrecy*. It could be argued that the latter term, which has always been personality-neutral, is more appropriate (and certainly less controversial) to use in relation to organisations. Yet secrecy is arguably narrower in scope than privacy, even though the two concepts are frequently used synonymously. Bok claims, for example, that secrecy is 'intentional concealment': Bok, *supra* n 63, 6. Privacy, on the other hand, is a condition of limited accessibility, independent of whether or not this is intentional: *ibid*, 10–11. Accordingly, privacy and secrecy will only overlap whenever efforts at controlling access rely on hiding: *ibid*, 11. If one accepts this analysis (as I do), the concept of secrecy ends up being too narrow to be of service to the full range of Westin's claims. At the same time, if one refuses to allow the concept of privacy to be applied to organisations or legal persons (as Bok does: *ibid*, 13–14), but accepts the definitions of secrecy and privacy given by Bok, the English language seems bereft of a term that by itself adequately describes the condition whereby organisations or legal persons (as opposed to individuals) enjoy limited accessibility!

912 Westin, *supra* n 335, 44.

organizational reality',[913] between the idealised view of how organisations are run – rationally, fairly, and orderly – and how they actually often are run. In his view,

> '[p]rivacy affords the relaxation which enables those who are part of a common venture, public or private, to communicate freely with one another and to accomplish their tasks with a minimum of social dissembling for 'outside' purposes. Without such privacy the operations of law firms, businesses, hospitals, welfare agencies, civic groups, and a host of other organizations would be seriously impaired.'[914]

In essence, Westin appears to be arguing that privacy, through the 'release' function, enables organisations to be run efficiently.

As for the functions of 'evaluation' and 'protected communication', Westin basically repeats the points he makes in relation to the 'autonomy' and 'release' functions.[915] It is not entirely clear whether Westin realises this. In my view, the repetition is unavoidable. This is because both the 'evaluation' and 'protected communication' functions are only important in so far as they are necessary elements in the fulfilment of the other two functions, especially that of 'autonomy'.

Westin concludes his analysis by claiming that '[p]rivacy is ... not a luxury for organizational life; it is a vital lubricant of the organizational system in free societies'.[916] He also writes that organisational privacy should be

> 'more than a protection of the collective privacy rights of the members as individuals. Organizational privacy is needed if groups are to play the role of independent and responsible agents that is assigned to them in democratic societies.'[917]

This is an important point that is revisited further below.

Westin canvasses the topic of 'organizational privacy' only in a very generalised way. Just under ten pages are devoted to the topic and the term 'organizations' is intended to cover all public and private bodies, ranging from law firms to political parties to government institutions and agencies.[918] Westin does not specifically consider the rights and needs of organisations in relation to data protection law. Neither does he specifically canvass the extent to which organisational privacy should be protected by other legal rules.

---

913 *Id*.
914 *Ibid*, 45.
915 *Ibid*, 46–51.
916 *Ibid*, 51
917 *Ibid*, 42. See also *ibid*, 368.
918 *Ibid*, 42.

Westin's generalised approach not only results in several of his claims being formulated ambiguously,[919] it blurs some important distinctions that at times should be made between public and private organisations in relation to their respective goals and functions. This is the case when Westin justifies some of his claims about the need for, and desirability of, general organisational privacy by citing examples of public/State organisational needs that should not necessarily have relevance for, say, large private corporations. For example, as support for his claim that organisations *in general* need privacy if their operations are not to be 'seriously impaired', Westin cites the need for secrecy in congressional committee hearings, jury deliberations and judicial private conferences.[920]

Just as his definition of privacy is personality-neutral, so too is his conceptualisation of privacy's value. For Westin, the fundamental value of privacy is that it preserves the *autonomy* of individuals and organisations.[921] Attention is thereby shifted from the microcosm of human feelings to the ability of an individual or organisation to function as a self-determining unit in a wider context, which for Westin is 'democratic society'. Such a perspective on privacy's value can be termed functionalist. In other words, privacy is seen basically in terms of *pattern maintenance* and *tension management*, these two mechanisms being regarded in turn as enabling individuals and organisations to survive as autonomous entities. This is a justifiable view of the value of privacy, though it can have some problematic consequences.[922]

One effect of a functionalist perspective which is particularly relevant to the concerns of this section is that the distinctions between individuals and collective entities tend to diminish. This is best exemplified in the work of recognised functionalists in sociology, such as Talcott Parsons and Philipp Selznick. Both writers adopt what has been termed a 'natural system' theory of organisations.[923] In

---

919 Eg, what does he exactly mean by 'social dissembling' when he discusses the function of 'release'?

920 *Ibid*, 45–46.

921 Reflected in the title of his work, *Privacy and Freedom*.

922 One consequence (which is arguably typical of functionalist analysis generally) is that analysis tends to have a conservative focus. This is exemplified by Westin's examination of privacy's 'release' function. Here Westin appears to defend the organisational *status quo*, without considering the wider social effects of organisations' behaviour. For instance, when Westin refers to the disruptive effects of 'social dissembling' he does not ask whether this might nevertheless be of benefit to wider society. His main concern is that 'social dissembling' detracts from an organisation's efficiency. Yet what sort of efficiency does he mean? The efficiency of the present state of affairs? He does not consider whether or not this 'efficiency' is desirable from the point of view of those whose lives are affected by the action of the organisation. At the same time, though Westin does not have to take into account these sorts of considerations, given the limited focus of his analysis on the privacy *needs* of organisations. However, these sorts of considerations should be canvassed in any discussion of the extent to which such needs should be translated into legal rights. See further Chapter 13.

923 For an overview of this theory, together with other perspectives in sociology on the nature of organisations, see JE Haas & TE Drabek, *Complex Organizations. A Sociological Perspective* (New York: Macmillan, 1973), 24–93.

broad terms, this theory equates (at a functional level) organisations with biological organisms because both have to respond and adapt to their environment in order to survive. The various ways in which each organisation adapts is regarded as giving each a distinct history and personality. While it would be presumptuous to categorise Westin's analysis of 'organizational privacy' as a clear embodiment of 'natural system' theory, there is no apparent conflict between the underlying thrust of Westin's analysis and this theory.

Westin's analysis also appears to be reconcilable with a conceptualisation of legal persons which is found in jurisprudence under a variety of names: 'natural entity theory', 'organic theory', 'group person theory' and 'corporate realism'. Broadly speaking, this conceptualisation treats legal persons as maintaining an existence independent of the individuals who constitute them, independent of the State and independent of the law. The legal person is also seen as constituting some sort of organic whole that is more than the sum of its parts.[924] Again, it would be presumptuous to claim that Westin fully embraces this sort of perspective on corporate entities. Nevertheless, his emphasis on the desirability of organisational autonomy and his claim that organisational privacy should be seen as 'more than a protection of the collective privacy rights of the members as individuals', mesh well with the corporate realist perspective.

The latter perspective can be contrasted with two other major ways of conceptualising the legal person. One of these is the so-called 'fiction' or 'artificial entity' theory, the basic tenets of which are that the corporate entity is a pure fiction and owes its existence to the State (hence, another name for this perspective is 'concession' theory).[925] The other view of the legal person goes under the names of 'aggregate', 'partnership' or 'contractual' theory. This sort of theory treats the corporation as a 'creature of free contract among individual shareholders, no different, in effect, from a partnership'.[926] Like corporate realism, aggregate theory posits the corporate entity as existing independently of the State, but, unlike corporate realism, rejects the notion that the corporate entity is in any way distinct from the individuals who come together and constitute it.

These three perspectives on the legal person underlie the bulk of political, academic and judicial discussion on the appropriate means of regulating and

---

924 For an overview of this perspective and its origins, see, eg, S Bottomley, 'Taking Corporations Seriously' (1990) 19 *Fed L Rev*, 203, 211–213; JC Coates, 'State Takeover Statutes and Corporate Theory: The Revival of an Old Debate' (1989) 64 *NYU L Rev*, 806, 818–825; M Stokes, 'Company Law and Legal Theory', in W Twining (ed), *Legal Theory and Common Law* (Oxford: Basil Blackwell, 1986), 155, 163.

925 See, eg, Bottomley, *supra* n 924, 206–208; Coates, *supra* n 924, 810–815. For an extended critique of fiction theory, see FW Hallis, *Corporate Personality: A Study in Jurisprudence* (London: Oxford University Press, 1978).

926 MJ Horwitz, '*Santa Clara* Revisited: The Development of Corporate Theory', in WJ Samuels & AS Miller (eds), *Corporations and Society: Power and Responsibility* (New York: Greenwood Press, 1987), 13, 22–23. See also, eg, Bottomley, *supra* n 924, 208–211, and Coates, *supra* n 924, 815–818.

protecting corporate activity. The popularity and influence of each perspective has varied from period to period and country to country,[927] as have the purposes for which they have been used.[928]

Of the three perspectives on the legal person set out above, it is corporate realism (ie, natural entity theory) that comes closest to reflecting accurately the present character of corporations (and other organised collective entities) – particularly large ones. Such a perspective better captures than the other two perspectives the fact that an organisation is a body with goals, interests and operational modes which cannot be reduced to the goals, interests and operational modes of the individuals constituting it or of other actors in its environment.[929] At the same time, though, we should not overlook that all organisations are ultimately made up of individuals.[930] We must also remember that the dichotomy between the goals, interests and operational modes of an organisation, on the one hand, and the goals, interests and operational modes of the individuals constituting the organisation, on the other, will vary in strength from organisation to organisation. In many small collective entities (eg, small family enterprises), the dichotomy will be miniscule. In such cases, the perspective embodied in aggregate theory will have considerable empirical relevance.

The perspectives of both natural entity theory and aggregate theory allow for the relatively easy application of human concepts to corporations and, concomitantly, to

---

927 For instance, Coates claims that the natural entity theory has dominated recent legal thinking in the USA: Coates, *supra* n 924, 826. By contrast, Stokes writes that the contractual theory has dominated recent legal doctrine in the UK: Stokes, *supra* n 924, 163.

928 Dewey notes, for example, that 'corporate groups less than the state have had real personality ascribed to them, both in order to make them more amenable to liability ... and to exalt their dignity and vital power, as against external control': .J Dewey, 'The Historic Background of Corporate Legal Personality' (1926) 35 *Yale LJ*, 655, 669.

929 This fact is most vividly conveyed by Christopher Stone: 'the corporation brings together men, machines, and patterns of doing things into an enormous sociotechnical system ... Those who enter into one of these structures become neither individuals, nor even men-in-groups, but fitted parts of elaborate subsystems … each of which is working with (and often at odds with) the other toward the realization of … institutional goals and targets. The whole constellation, moreover, does not ... discharge its human members en masse when their limited task is through. The corporation, itself potentially immortal, continues with an inertia much its own as the individual human or mechanical 'cells' … part and are replaced. In this setting each man's own wants, ideas – even his perceptions and emotions – are swayed and directed by an institutional structure so pervasive that it might be construed as having a set of goals and constraints (if not a mind and purpose) of *its* own'. See C Stone, *Where the Law Ends: The Social Control of Corporate Behavior* (New York: Harper & Row, 1975), 6–7.

930 In some legal systems, though, the creation of a personless corporation might be possible. See further the hypothetical example of such a corporation given by Meir Dan-Cohen with respect to US law: M Dan-Cohen, *Rights, Persons, and Organizations: A Legal Theory for Bureaucratic Society* (Berkeley: University of California Press, 1986), 46–49.

other organised collective entities.[931] Corporate realism treats legal persons as autonomous entities that are functionally analogous to individuals. Accordingly, it provides a conceptual (and, to some extent, normative) foundation for legal persons to assert needs and claims most commonly associated with individuals. Aggregate theory also provides such a foundation, though this foundation derives not from the nature of the legal person as such but from the rights-bearing individuals making up the legal person.[932]

This constitutive status of individuals is emphasised in Bloustein's analysis of 'group privacy'.[933] Bloustein refers to group privacy as being 'an attribute of individuals in association with one another within a group, rather than an attribute of the group itself'.[934] At the same time, Bloustein views the notion of 'group privacy' at least as broadly as Westin views the notion of 'organizational privacy'. For Bloustein, 'group privacy' embraces 'the large, formal organization, as well as the relatively informal relationship, and the whole range of intermediate variations in size, duration and formality'.[935]

Bloustein defends the need for group privacy using justifications similar to those used by Westin in relation to organisational privacy. Bloustein writes of 'confidentiality' as essential to assuring 'the success and ... integrity of the association', and refers to the work of the sociologist, Robert Merton, as illustrating 'the principle that privacy is essential to a properly functioning social structure'.[936] He also emphasises the importance of group privacy for democracy as it preserves 'centers of initiative and power outside the ambit of government'.[937] At the same time, Bloustein points out more obviously than does Westin that privacy for

---

931 The ability of both types of theory to justify the extension of concepts (and, thereafter, legal rights) to corporate entities is illustrated by academic discussion on the rationale underlying the judgement of the US Supreme Court in *Santa Clara Co v Southern Pacific Railroad*, 118 US 394 (1886). In a terse judgment, the court here decided for the first time that corporations are 'persons' and entitled, therefore, to the benefits of the equal protection clause in the US Constitution. What is important for the purposes of the present discussion is not so much the judgment itself as the alleged rationales for it. As Horwitz points out, the judgement has often been viewed as embodying a natural entity theory of corporations. Horwitz convincingly shows, however, that the judgement is quite capable of being viewed as embodying an aggregate or partnership theory of corporations, and that this view of the judgement is the most historically correct. See Horwitz, *supra* n 926, 17ff.

932 See, eg, R Pilon, 'Corporations and Rights: On Treating Corporate People Justly' (1979) 13 *Georgia L Rev*, 1245–1370 (arguing that corporations are basically the individuals who constitute them and that the rights of corporations are grounded in the rights of those individuals).

933 See EJ Bloustein, *Individual and Group Privacy* (New Brunswick: Transaction Books, 1978), 123–186.

934 *Ibid*, 124.

935 *Ibid*, 126.

936 *Ibid*, 181. See also *supra* n 631.

937 *Ibid*, 182; see also 129–130. Bloustein and Westin are not the only persons to emphasise this important point. See also, eg, Schafer, *supra* n 502, 14–15; FD Schoeman, *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992), 156–158, 193–194.

collective entities promotes an independent interest in developing and maintaining inter-personal relationships:

> '[t]he interest protected by group privacy is the desire and need of people to come together, to exchange information, share feelings, make plans and act in concert to attain their objectives. This requires that people reveal themselves to one another – breach their individual privacy – and rely on those with whom they associate to keep within the group what was revealed. Thus, group privacy protects people's outer space rather than their inner space, their gregarious nature rather than their desire for complete seclusion. People fashion individual privacy by regulating whether, and how much of, the self will be shared; group privacy is fashioned by regulating the sharing or association process.'[938]

Like Westin, Bloustein does not canvass whether or not collective entities as such should be given rights as data subjects under data protection statutes. Presumably, Bloustein would argue that any such extension of data protection rights should be justified on the basis of the rights and needs of the individuals forming the groups, not the rights and needs of collective entities as such.

This sort of argument is adopted by Paul Sieghart. He argues for data protection rights for 'associations' because such entities are ultimately groups of individuals.[939] Tuner pursues a similar line of argument in favour of giving data protection rights to legal persons.[940] Giving legal persons such rights would provide, in her view, more complete protection for the rights and needs of the individuals behind such persons, particularly the ability and right of individuals to 'personality development in association' ('Persönlichkeitsentfaltung in Gemeinschaft').[941] In making these claims, both Sieghart and Tuner appear implicitly to build on the aggregate or partnership theory of corporations outlined above.

12.2 Applicability of Other Data Protection Interests to Collective Entities

One of the insights emerging from the previous section is that discussion of the relevance of privacy for collective entities tends to run over into discussion of the equivalent relevance of other interests and values (eg, autonomy) that are closely related to privacy. This broadening of the discussion is both inevitable and desirable, particularly in a data protection context. Data protection laws promote a wide range

938 *Id*.
939 Sieghart, *supra* n 335, 134.
940 Tuner, *supra* n 638, 26.
941 *Id*.

of interests held by data subjects.[942] Hence, to focus merely on the applicability of privacy to collective entities is inadequate for the purposes of resolving the central issue of Part III.

It will be recalled from Chapter 7 (section 7.2.5) that two broad groups of data subject interests are promoted by data protection laws. The first group embraces interests concerning the quality of information and information systems. The overarching interests in this group are summed up in terms of ensuring data validity and information utility together with the manageability, robustness, accessibility, reliability and comprehensibility of information systems. The second interest group comprises interests concerning the condition of persons as data subjects and the quality of society generally. The overarching interests in this group are summed up in terms of ensuring privacy, autonomy, civility, democracy, pluralism, rule of law and balanced control.

All of the first group of interests are obviously capable of being shared by collective entities as such. The same can be said in relation to the second interest group, with the possible exception of the concern for ensuring privacy. However, in light of the discussion in the preceding section, solid grounds exist for maintaining that collective entities can share the latter concern.

The validity of the above statements holds whether one views collective entities in terms of natural entity theory or aggregate theory; ie, one can plausibly view collective entities as having the above interests either in their own right and/or derivatively through their individual members.[943]

Of course, the reasons for which collective entities possess and seek to protect these interests are not always identical with the equivalent reasons applying with respect to individuals. Concomitantly, the importance attached by collective entities to safeguarding these interests is not always the same as that attached by individuals. Moreover, there exist differences between collective entities in terms of how important protection of the interests is for their *modus operandi*. These points are considered in more detail in Chapters 13–14.

12.3 Summing Up

One of the major arguments against giving organised collective entities (primarily legal persons) rights as data subjects under data protection legislation is that (i) the essential rationale for such legislation is the protection of privacy, and (ii) privacy is a concept that can only apply to individuals. Both assumptions are easily assailable.

---

942 See generally Chapter 7.

943 Cf the duality of collective entities as noted in Chapter 9 (section 9.1).

While the protection of privacy is certainly one of the main objectives of data protection legislation, it is not the only objective. Data protection laws seek to promote a broad range of other interests and values as well.

It is obvious that all these interests and values, with the possible exception of privacy, can apply to collective entities. As for the ambit of the privacy concept, this could embrace collective entities on logical grounds, given that most definitions of privacy – and certainly those definitions that best fit with the thrust of data protection laws – are personality-neutral in their essence. Whether or not most people feel it appropriate to apply the privacy concept to collective entities is difficult to ascertain. Numerous persons engaged with privacy and data protection issues have indicated it is not appropriate. Their main reason for taking this stance is that the value of privacy has its origins in the need to protect human sensibilities from external interference. For such persons, the fundamental value of privacy is inextricably located at the level of the individual human psyche.

Yet, as Westin and others show, it is possible to take a more expansive view of privacy's value. Privacy does not simply protect human sensibilities. Its principal function is to help preserve humans' ability to function as autonomous units. At this level of abstraction, it is quite easy to show that privacy can be of value to collective entities by helping them function autonomously and efficiently. It is also quite easy to argue that respecting the privacy of collective entities is not only of value for the entities as such or for the individuals who constitute them. Such respect is also of value to pluralistic, democratic society because it helps maintain relatively independent centres of power.

Westin's analysis of 'organizational privacy' can be viewed as an attempt to tailor the (originally) 'human' concept of privacy to fit organisations by making both the concept and value of privacy personality-neutral. But it is also possible to 'humanise' organisations and thereby give them the possibility of using the privacy concept.

One way of doing this is to build on the aggregate theory of corporations and claim that such bodies, along with other collective entities, are simply individuals in association with each other. This approach, in effect, reduces collective entities to the sum of their human parts. One finds elements of this approach in the work of Bloustein, Sieghart and Tuner.

Another way is to recognise the reality of collective entities as such and argue that these entities are in themselves (ie, independently of their constituents) the functional equivalent of human individuals. This approach builds on a natural entity theory of organisations and corporate bodies. Westin's analysis of organisational privacy can be viewed as in harmony with this approach.

Each of these two types of theory – aggregate and natural entity – addresses an undeniable characteristic of collective entities. However, neither of them offers on its own an entirely satisfactory conceptualisation of collective entities; we can only approach such a conceptualisation by combining both theories. All collective entities

are constellations of individuals. This fact is most obvious in the case of small corporations run by one person or a family. Yet collective entities are also independent of, and more than, the individuals who constitute them. This fact is most obvious in the case of corporate giants, such as General Motors and IBM. Thus, any satisfactory conceptualisation of collective entities and their needs has to balance/adjust between both the aggregate and natural entity perspectives. The same applies when addressing the issue of whether or not collective entities should be given data protection rights.

Finally, even if we accept that the concept and value of privacy and of other data protection interests are sufficiently broad to relate to organised collective entities, this does not necessarily mean that the latter should be afforded the same *legal rights* to data protection as individuals. Other factors need to be taken into account in determining the extent to which it is appropriate to give these entities such rights. These factors are examined in the following chapters.

13. Social, Economic and Political Factors

13.1 Introduction

One of the questions taken up in the previous Chapter concerns whether or not the interests and values safeguarded by data protection laws are broad enough to apply and be of use to (organised) collective entities. As intimated at the close of that Chapter, resolving that issue goes only a short way to determining the extent to which such entities should be afforded data protection rights. Other factors need to be taken into account, and it is with some of these factors that this chapter is concerned. The remainder of these factors are set out and discussed in Chapter 14.

The factors dealt with in this chapter relate largely to the economic, social and political roles collective entities play and are expected to play. These factors can be summed up in terms of the social impact/risk entailed by collective entities' actions; the extent to which collective entities use personal information; collective entities' vulnerability and resources; and their expectations and accountability.

13.2 Social Impact/Risk

Let us make several assumptions. The first assumption is that the impact of the actions of many collective entities on other persons/entities is generally likely to be greater than the impact of individuals' actions. This assumption builds on another assumption, which is that the economic strength and field of operations of many collective entities tend to be more extensive than those of individuals. A third assumption, which follows from the former assumptions, is that a collective entity's potential for engendering widespread social harm is generally likely to be greater than an individual's potential for doing so. The final assumption is that the *risk* of harm can be magnified by any enhancement of collective entities' ability to act in secret.[944]

If we treat the above assumptions as resting on a bedrock of fact, what weight should they be given in determining the extent to which various types of collective entities should have rights as data subjects under data protection laws? They should have at least some weight *if* giving collective entities data protection rights *actually*

944 See, eg, Bok, *supra* n 63, 150-151.

enhances these entities' ability to act in secret. The Lindop Committee set out as one of its arguments against protecting data on legal persons under data protection laws that such protection would reduce access by the general public to information about companies' affairs which is of 'legitimate public interest'.[945]

However, protecting data on legal persons under data protection laws *need* not significantly increase the ability of corporations to act in secret. Indeed, it might very well provide only a minimal increase in that ability. The limitations put by data protection laws on processing information rarely amount to absolute prohibitions.[946] In particular, the limitations on collection and disclosure of information are typically subject to various exemption clauses that, taken together, can render almost nugatory the protection of a data subject's interest in non-transparency. As Korff duly observes,

> '[i]n countries which do extend data protection to legal persons, openness can normally be ensured under relevant open, flexible clauses: when companies do not have a 'protection-worthy' interest in keeping … information secret, restrictive data protection rules can be left aside.'[947]

Further, giving collective entities rights as data subjects under data protection laws does not prevent the enactment of other laws that, directly and/or indirectly, diminish those rights.

Finally, providing collective entities with data protection rights can enhance the general transparency of data-processing operations in a society.[948] It can do so, firstly, by extending the class of data subjects able to exercise access rights; secondly, by extending the class of data to which access rights apply; and, thirdly, by extending the categories of data processing which must be notified either to data subjects or to data protection authorities.

13.3 Information Use

Let us next assume that, as a general rule, many collective entities gather and use personal information to a much larger extent than individuals do. Most people would probably take the veracity of this assumption for granted and, in order to back up

---

945 *Supra* n 505, 156, para 18.38. In a similar vein, Simitis claims that giving data protection rights to legal persons would be at cross-purposes with legislation subjecting such entities to so-called 'sunshine rules'; ie, rules requiring corporations to disclose information on themselves to regulatory agencies and/or members of the public so as to enhance public control of corporate activities. See, eg, Simitis, *supra* n 513, 156–157.

946 See further Chapters 11 (section 11.2.2) and 18 (espec sections 18.4.3 & 18.4.6).

947 Korff, *supra* n 16, 45–46.

948 Refer to the point elaborated by Buttarelli, *supra* n 705.

their view, point to the function and extensive scale of operations undertaken by many corporations. Rule *et al* observe that a central function of organisations is the production of 'authoritative' decisions about people, the most important 'raw material' for this production being personal information.[949]

The fact that corporations are major gatherers and users of personal information makes them an aspect of the problem that data protection legislation aims to remedy.[950] A similar point was made by the Lindop Committee, which stated that data protection legislation aims at redressing the balance of power between individuals and organisations. The Committee felt that to give organisations protection under such legislation would conflict with this aim.[951] The Committee did not elaborate, though, on the extent or level of this conflict. The conflict probably lies more at the level of ideals than of practice. Giving rights to collective entities (or individuals) as data subjects does not necessitate cancelling out their legal duties and obligations as data controllers; neither does it have to prevent individuals from exercising their rights as data subjects.

13.4 Vulnerability and Resources

There are three, inter-related points to be covered here. The first is the trite observation that collective entities have no emotions that can be injured when information on their activities is disclosed. This means that the range of interests that collective entities as such need to have protected is narrower than it is for individuals. It is equally obvious, though, that collective entities are ultimately made up of individuals who have emotions, so the above statement on range of interests in need of protection is not completely true. In many situations where the interests of a collective entity as such are injured (in a non-emotional way), there can be emotional and/or non-emotional injury to the individuals behind the entity. Moreover, these individuals can have been injured simply because of their connection (as employees, directors, etc) with the entity in question. In other words, their connection with the entity can increase *their* vulnerability to injury or harm.

Nevertheless, if one accepts as a fact that collective entities as such have a narrower range of interests in need of protection than is the case for individuals, should this fact constitute a bar to collective entities being given data protection rights? In many jurisdictions, this fact has not prevented legal persons from being given the right to sue for defamation;[952] it has only narrowed the range of contexts in

---

949 Rule *et al*, *supra* n 353, 49.

950 See also Bygrave, *supra* n 5, 140; E Eriksson-Gullquist, *Rätt til insyn i person-register: Den svenska datalagen i internationellt perspektiv*, ADBJ-rapport 1979:15 (Stockholm: Arbetsgruppen för ADB och Juridik, Stockholm University, 1979), 39.

951 *Supra* n 505, 156, para 18.37.

952 See Chapter 12 (section 12.2.2).

which legal persons can employ this right. Allowing legal persons the right to sue for defamation rests upon recognition that such entities have a strong interest in upholding their reputation. Even if they have no feelings that can be injured, damage to their reputation can have a number of other detrimental consequences for them, and these consequences can be both economic and non-economic.[953] It should also be remembered that the principles and rules found in data protection laws are capable of safeguarding not just emotional well-being but a range of other interests as well, concerning, for instance, the quality of data, information and information systems.[954] Moreover, data protection laws do not rank, at least on their face, the importance of protecting the latter sorts of interests lower than the importance of protecting emotional well-being.

The second point builds upon the observation by Stanley Benn that the importance of privacy for a person varies with the degree to which he or she is vulnerable to others' judgements and reliant on his or her own.[955] It could be argued that many collective entities are so large and powerful that they are not as perturbed by bad publicity as individuals might be. This could particularly be the case in a situation where a corporation has a market monopoly; in such a situation, it could well be that bad publicity has the same effect on the corporation as water has on a duck's back. As a general rule, though, many organisations need to maintain a respectable image in the eyes of the general public and governmental agencies in order to sell their products and/or services and/or – particularly if they have a political agenda – their point of view. It is also important for them to maintain such an image in order to make it easier for them to carry out daily operations without undue disturbance (eg, from protest groups or regulatory agencies). Furthermore, a tarnished public image for an organisation could hamper recruitment of persons whom the organisation finds attractive to employ and could have detrimental consequences on working morale within the organisation.[956] Again, the latter

953 In this respect, it is worth noting that, in at least several jurisdictions (eg, those of Norway, England and the USA), legal persons are allowed to claim compensation for *non-economic* damage arising from defamation: see Mæland, *supra* n 883, 290, footnote 46. For Norway, the central judicial authority for allowing legal persons to claim such compensation is the Norwegian Supreme Court's judgement of 18.6.1987 concerning defamation of the construction and engineering company, 'A/S Akers Mek. Verksted' (Rt 1987, 764–780). The Court appears to have had little trouble in holding that the Aker company should be paid compensation for non-economic injury caused by a newspaper that had published defamatory allegations about the reliability of the oil rigs designed and constructed by the company. The Court recognised that defamation of a legal person can injure both the entity itself and the individuals attached to it, in a manner that is difficult to quantify. According to the Court, defamation can damage not only a legal person's reputation to the outside world, it can also create problems for co-operation etc within the entity: Rt 1987, 773. Moreover, the Court held that a legal person should be viewed as 'bearer' of the interests that the individual employees can have as a result of the injury they feel personally: *id*.

954 See further Chapter 7 (section 7.2.5).

955 See Benn, *supra* n 590, 25.

956 Cf the judgement of the Norwegian Supreme Court in the Aker case, *supra* n 953.

observation alerts us to the possibility that ultimately not just the collective entity as such could suffer from bad publicity; the individuals who make up the entity could also suffer.

The third point concerns collective entities' resources and capacity to look after their interests. Let us assume that collective entities generally have greater resources and a greater capacity to take care of their interests than individuals do. As with the assumptions set out above in sections 13.2 and 13.3, the veracity of this assumption is probably taken for granted by most people.[957] Yet the veracity of the assumption should not be taken for granted. On this point, Conard's study of US corporations in the 1970s is noteworthy. Observing a tendency in the USA to view the typical private corporation as a large organisation rich in assets, Conard cites official statistics showing that, as of 1970, approximately 20 percent of US corporations had assets from between zero and $10,000. Just under 60 percent of US corporations had assets under $100,000 and approximately 35 percent had assets from between $100,000 and $1,000,000. Less than 7 percent of US corporations had assets over $1,000,000 and of these, just over 1 percent had assets over $10,000,000.[958] Conard also cites statistical projections showing that, as of 1970, over 90 percent of US corporations had 10 or less shareholders, while less than 1 percent had more than 100 shareholders.[959] Although these statistical distributions would undoubtedly have shifted since 1970, and although they cannot be assumed to be representative for other countries either now or in 1970, they do highlight that care should be taken when making generalisations on the size and wealth of private corporations.

Nevertheless, for the purposes of the following discussion, let us treat the assumption that collective entities generally have greater resources and a greater capacity to take care of their interests than individuals do, as accurately mirroring reality. Let us therefore also assume that collective entities generally have greater resources than individuals do, to deal with or counteract any detriment arising from situations in which data on them are used against their wishes. The important question arising here is: does acceptance of the latter assumption *necessitate* denying data protection rights to collective entities? In my view, it does not. Collective entities generally might not need data protection rights to the same extent as individuals do but this does not mean having such rights would not be of *some* assistance to such entities. The next issue is whether or not the benefits of such assistance outweigh its costs (if any). This particular cost/benefit equation has to take into account not just the costs and benefits of the assistance accruing to collective entities as such but also any possible costs and benefits accruing to:

1) the individuals constituting collective entities;

---

957 Note, eg, the unsupported claim by the Norwegian Ministry of Justice that 'business enterprises generally have greater ability to look after their interests than individuals do': *supra* n 694.

958 See Conard, *supra* n 631, 101 (all figures are in US dollars).

959 *Ibid*, 118.

2) the authorities charged with overseeing the implementation of data protection laws; and
3) society generally.

Examples of the assistance legal persons received upon being given data protection rights in Norway and Denmark are found in Chapter 11 (section 11.3). As pointed out there, this assistance has been modest but not insignificant. Arguably, it has benefitted not just legal persons as such but also the individuals attached to them, the Danish and Norwegian data protection authorities and possibly Danish and Norwegian society in general. Moreover, this assistance *appears* to have resulted in few practical costs for either the legal persons, individuals, data protection authorities or societies concerned.

When considering the benefits of extending data protection rights to collective entities, we must first recall the various types of data existing on such bodies. Let us take, for instance, the situation of corporations. An overview of the various data-types that can be linked to a private corporation is given in Chapter 9 (section 9.1). These data-types can include information on the corporation's management and ownership structure, its scope and site of operations, its assets, profits, losses and capital turnover, its plans, strategies and ideology, its customers and allies, its products (industrial or otherwise), its use of resources, and/or its transgressions of the law.

In the abstract, it is difficult to distinguish between these various data-types in terms of their sensitivity for a given corporation (or attached individuals). Certainly, some of the above types of information could be readily available to the general public (eg, data concerning corporate assets, profits, losses and capital turnover). Other information, however, could be subject to duties of confidentiality limiting its disclosure to certain parties (eg, data concerning corporate plans and strategies). Yet the sensitivity of information does not simply correspond to the degree to which it is public. Ultimately, the sensitivity of information depends largely on how it is used, the context in which it is used, and the result of its use. Data will be sensitive to the extent that their use can lead to action being taken to the detriment of the data subject. Whether or not such use is justifiable in each case is another matter. The important point is that all of the above types of information are capable of being used to the detriment of a corporation.

This detriment could arise in numerous ways: eg, in denying financial assistance to a corporation (in the form of loan, subsidy or insurance); in increasing a corporation's tax rate; in decreasing a corporation's ability to sell its products and/or services (because of, say, a public pressure campaign); in decreasing a corporation's ability to attract staff; or in increasing the tension within a corporate workplace. As pointed out above, these forms of detriment could also have a negative effect on the economic and emotional well-being of individuals who are linked to the corporation (eg, as its managers, directors, employees, shareholders, sponsors or customers).

In many cases, this detriment may be justifiable, legally and/or ethically. Yet this does not eliminate the potential for unjustifiable detriment arising because of, say, the use of inaccurate, incomplete or irrelevant corporate data. Extending the principles of data protection legislation to regulate the processing of data on private corporations could help to minimise this sort of unjustifiable detriment.

Such regulation could also contribute to limiting the ability of organisations and groups to collect and aggregate corporate data. It is clear that by aggregating all (or most) of the above-listed types of information on private corporations, a detailed and multi-faceted picture can emerge of their character (and, in some cases, the character of the individuals attached to them). This picture can depict, for instance, corporations' financial standing and credit-worthiness, internal power structure and working environment, and ethical disposition (including attitude to public norms, legal or otherwise).

There are undoubtedly many organisations and groups interested in gaining access to such an aggregate of corporate data. The corporate registration plans of the two Danish environmentalist organisations referred to in Chapter 11 (section 11.3.1) provide a case in point. In many cases, the motives for aggregating corporate data may be commonly regarded as legitimate. Nevertheless, any person who gains access to such an aggregate of data will have potentially significant power over the data subject(s). This power can be used in a variety of ways, some of which could significantly affect political, economic and/or social relationships. As Westin, Bloustein and others have pointed out, increasing the transparency of groups and organisations increases the potential for undermining their autonomy *vis-à-vis* the State, a development that can then increase society's vulnerability to totalitarianism.[960] Extending the principles of data protection law to regulate the collection and aggregation of information on collective entities could help to limit and steer this potential so that it does not undermine the bases for democratic, pluralistic society. Such regulation would be in the interests of collective entities, individuals, data protection authorities and society generally.

13.5 Expectations and Accountability

Probably few people would disagree that expectations of how much privacy a person should enjoy vary according to context and that one should expect to forfeit some privacy by placing oneself in a public role.[961] Many collective entities are public role-

960 See *supra* nn 916–917, 937 and accompanying text.

961 Thus, in many jurisdictions, the ability of public figures to sue for defamation and/or breach of privacy is not as extensive as for other, more private persons: see, eg, WL Prosser, 'Privacy' (1960) 48 *California L Rev*, 383, 410–419 (discussing US law on breach of privacy); and Mæland, *supra* n 883, 360–369 (discussing Norwegian and, to a lesser extent, US and other countries' laws on defamation).

players to a greater degree than most individuals. They are also required by law to make public a great deal of information concerning their activities. Moreover, many collective entities probably welcome and seek publicity (of the 'right' kind, of course) to a greater extent than most individuals. For business corporations, the 'right' publicity can enhance opportunities for marketing their products and services; for many non-profit organisations, the 'right' publicity can attract new members or sponsors. Accordingly, it seems reasonable to claim that collective entities do not – and should not – expect to be able to enjoy privacy to the same extent as individuals. In turn, it would seem reasonable to expect that collective entities' reduced expectations of privacy should also result in a reduction of their vulnerability to detriment brought about by breaches of their privacy.

Should these entities' reduced expectations of privacy influence whether or not they are given data protection rights? The ICC appears to believe they should. In arguing against giving data protection rights to *business* legal persons, the ICC asserts such persons 'expect that competitors, suppliers, government departments and even individuals will keep computerized files about them'.[962] The major problem with this line of argument is that data protection rights regulate much more than simply the extent to which organisations and individuals can collect and store data on other persons. To claim merely that business legal persons expect others to keep information on them does not indicate of itself what business legal persons expect in terms of, say, the quantity or quality of this information. Neither does it indicate what business entities *desire* in terms of the quantity or quality of such information. Admittedly, the ICC states that '[a]part from a few specific situations, such as credit rating, business legal persons have less interest in the accuracy and relevance of computerized files about them maintained by other *business persons*',[963] but the ICC states nothing about the interest of business legal persons in the quantity, accuracy and relevance of information about them that is kept by, say, *governmental* agencies. The ICC also states nothing about the expectations of legal persons (or other collective entities) not engaged in business. Moreover, the ICC assumes (probably unrealistically) that all business legal persons have the same expectations and interests in being given data protection rights.

It would be surprising, to say the least, if neither business nor non-business entities expect or desire that information collected and stored on them (particularly by governmental agencies, financial and credit-rating institutions) is accurate, complete and not misleading or superfluous in relation to the purposes for which it is processed. It would also be surprising if neither business nor non-business entities were concerned about the amount and nature of the information they are forced to divulge to others.[964] However, this is mere speculation; I have not come across any

962 ICC, *supra* n 748, 425. See also Rutgers, *supra* n 810, 395.

963 *Id* (emphasis added). See also Rutgers, *supra* n 810, 395.

964 Some evidence of this concern can be found, for instance, in Sweden. The Swedish Employers' Association (Svenska Arbetsgivareföreningen) has expressed disquiet over the fact that business

systematic surveys showing what various types of legal persons desire and expect in terms of the quality of the information kept on them by others and in terms of the ways this information is processed, used and stored.

Moving on to the factor of accountability, there is arguably a link between how much privacy one should be accorded and the extent to which one occupies a role in which one is accountable to others. Benn, for example, claims:

> 'for a matter to be private it is not sufficient that it should be kept secret, and so not 'publicised'. It must not be public in the further sense that the person in question is not liable, in principle, to answer for it in terms of principles, procedures, or standards held to promote a wider, 'public' interest.'[965]

Hence, for Benn, if a corporation is to have privacy, it must be 'a player with a free hand in the ordinary game of competitive business'.[966] Benn uses this 'free hand' criterion to distinguish between State enterprises and private businesses:

> 'the directors of a private business, while subject to the ground rules of private business games, can do just as they like with it within those rules, without having to answer for it to anyone outside the business. [...] Any part of the corporation's operations for which it was answerable as an 'official' agency would not be among its 'private affairs'. Public corporations, like British Railways or the Australian Broadcasting Commission do not have private affairs, though some things may be secret or confidential.'[967]

If the above argumentation of Benn is correct, and if it is correct to say that legal persons have as a general rule less room in which they can be non-accountable than individuals have, then legal persons also enjoy less room than individuals do for claiming a right to privacy. It should not be forgotten, though, that Benn's argumentation relates only to the extent to which legal persons can claim a right to keep their affairs 'private'. In terms of data protection rights, his argumentation addresses the extent to which legal persons can claim a right to resist collection and disclosure of certain types of information on them. Such a right is just one aspect of data protection law. Hence, Benn's argumentation is of little relevance for assessing the propriety of legal persons' claims to the *gamut* of data protection rights.

(Cont.)
enterprises in Sweden have been required annually to send in to governmental authorities enormous numbers of forms containing information on their activities. Interestingly, this disquiet is expressed in the preface to a book from 1986 which argues that data on legal persons require better legal protection in Sweden: see Rydén, *supra* n 716.

965 Benn, 'The Protection and Limitation of Privacy', *supra* n 590, 603. DeCew takes a somewhat similar position: DeCew, *supra* n 484, 56.

966 *Ibid*, 604.

967 *Ibid*, 603, 604.

Moreover, data protection legislation tends not to give persons (natural or legal) an absolute right to resist collection or disclosure of information on them.[968] Thus, giving data protection rights to legal persons (or other collective entities) does not preclude subsequent adjustment of the right to non-disclosure, on the basis of, say, the accountability factor defined by Benn.

13.6 Summing Up

None of the factors canvassed above can provide a strong basis for the case against giving data protection rights to collective entities. Any attempt to base this case on the above factors runs the risk of misconceiving the character of data protection law and/or the character of collective entities. With regard to the character of data protection laws, some of the factors tend to underplay the flexibility of such laws and overplay the extent to which they enable data subjects to hide from the public gaze. With regard to the character of collective entities, some of the factors tend to underplay the large variation in types of such entities and the fact they are composed of individuals. Concomitantly, some of the factors tend also to overplay the robustness of collective entities.

More specifically, to justify the case against giving data protection rights to collective entities on the basis of the 'social impact/risk' factor canvassed in section 13.2 and/or the 'accountability' factor canvassed in section 13.5 risks exaggerating the extent to which data subjects may use data protection rights to enhance their ability to maintain secrecy of their operations and internal affairs. To justify the case on the basis of the 'information use' factor outlined in section 13.3 risks overlooking the fact that giving data controllers the data protection rights of data subjects need not hinder the latter in exercising these rights. To ground the case on the basis of the 'vulnerability' and 'resources' factors described in section 13.4 risks underplaying the range of ways in which collective entities, and the individuals who constitute them, can suffer damage of a non-material kind (or a kind that is difficult to quantify financially). Grounding the case on the 'vulnerability' and 'resources' factors also risks underplaying the fact that data protection laws safeguard more than just emotional well-being and can promote a variety of political, economic and social interests that help provide the basis for democratic, pluralistic society. Finally, to justify the case on the basis of the 'expectations' factor set out in section 13.5 runs the risk of misrepresenting collective entities' expectations and wants in terms of the manner in which data on them is handled by data controllers in both the public and private sectors.

Most of the factors are generalisations built upon assumptions. While these assumptions might be held by many people and form part of 'common sense', they

968 See further Chapter 18 (sections 18.4.3 & 18.4.6).

might overly simplify and thereby distort reality. Accordingly, it would be important to test them against empirical evidence before using them in legislative policy-making.

14. Legal Factors

14.1 Introduction

This chapter examines the legal factors that need to be taken into account when resolving the issue of whether or not collective entities should be given data protection rights. Two of these factors are dealt with in section 14.2. Both overlap and are closely related to each other. The first factor concerns the extent to which the data protection interests of collective entities are already adequately protected by branches of the law that are not concerned directly and exclusively with data protection. The second factor concerns the extent to which these branches of the law have the *potential* to safeguard the data protection interests of collective entities in the same way as data protection laws currently protect the interests of individuals.

Section 14.3 sets out a number of alternative legislative regimes under which collective entities could be given data protection rights. It then canvasses the strengths and weaknesses of these regimes. The section also canvasses various legislative means for hindering collective entities (notably private corporations) from abusing any informational access rights they might be given pursuant to data protection legislation.

Finally, there is a summing up (in section 14.4) of the main conclusions to be drawn from the chapter.

14.2 Protection of Collective Entities under other Branches of Law

14.2.1 EXTENT OF PROTECTION

To what extent is the processing of data on collective entities regulated under branches of the law not concerned directly and exclusively with data protection? To what extent does such regulation effectively provide collective entities with the same sorts of rights as they are given (as data subjects) under the data protection laws of, say, Austria and Switzerland? These questions address the degree to which giving data protection rights to collective entities would be redundant at a legal level. It is beyond the scope of this chapter (or book) to provide a detailed and conclusive answer to the questions. To provide such an answer requires careful examination of all branches of the law in order to identify rules relating to:

- collection of data on collective entities;

- use and disclosure of such data;
- quality of such data;
- access to, and correction of, such data; and
- security of such data.

This examination must be done in relation to each country that has enacted, or plans to enact, data protection legislation. If the examination is to impart a full picture of the way in which the handling of data on collective entities is regulated in a given country, it must not only attempt to identify relevant rules found in statutes, regulations, decrees and judicial decisions, but also those found in relatively inaccessible directives, instructions and circulars issued by various agencies for internal use. Once the relevant rules are identified, they must be compared to the rights typically given to data subjects pursuant to data protection laws.

An immense number of rules pertain to the handling of information on collective entities. Only a superficial overview of the main types of these rules and their focus is given in the following. Subsequent research is needed to undertake more detailed examinations of these rules and their relationship with data protection laws.

It is fair to surmise that most if not all countries that have enacted or plan to enact data protection legislation have, in addition to this legislation, well-developed legal doctrines creating, and punishing breaches of, various types of duties of confidence (statutory, contractual, and/or equitable) in relation to corporate trade secrets. Moreover, these countries undoubtedly have legal rules prohibiting certain forms of surveillance/intrusion (eg, unauthorised wire-tapping) that could also affect the confidentiality of corporate information. These rules and others might further punish a variety of actions (eg, computer hacking) that could result in information on corporate and other collective entities being tampered with or altered. In addition, there might be rules punishing the disclosure of false and defamatory information on collective entities. It is also probably fair to surmise that all of the above countries have established rules prohibiting certain forms of unfair competition (eg, deceptive advertising, misuse of intellectual property) between business enterprises.

The sorts of legal rules described above tend to suffer from several weaknesses in terms of their capacity to protect data on collective entities. One weakness is that the remedies they provide are generally *ex post facto*; they focus on the punishment of certain misdemeanours rather than the adoption of fair information practices that could prevent such misdemeanours from taking place. Moreover, the remedies are typically pursued only in the (relatively rare) situation when a data subject becomes aware of the misdemeanour and has the resources to lodge and follow up a complaint.

Another weakness is that many of the rules offer only indirect or incomplete protection of data on collective entities. To take one example, the action for defamation generally does not enable a collective entity to halt the collection and/or dissemination of information that is accurate; nor does it enable a collective entity to control how the information is to be used. To take another example, intellectual

property rights generally focus on regulating the use (more particularly, the commercial exploitation) of information on certain types of *property* of a corporation as opposed to information on the latter's 'person' or identity. In data protection legislation, the opposite is the case; the primary object of protection is information on one's identity or person. Not all information on one's person constitutes information on those parts of one's property that are the subject of intellectual property rights.

A third weakness with the above rules is they tend to focus on safeguarding the confidentiality, as opposed to quality, of information on collective entities. Of course, protecting the confidentiality of information can indirectly assist in protecting its quality. Yet the above rules tend not to underline to the same degree as data protection laws typically do the importance of ensuring that data are relevant, correct, complete and not misleading in relation to the purposes for which they are processed. Few, if any, of the above rules directly or expressly require organisations and individuals to take active measures to check the quality of information they collect or store.

One of the main means of ensuring adequate data quality is to give data subjects legally enforceable rights of access to data concerning them which are held by others. In most jurisdictions, there are probably few such rights found outside data protection law which are enforceable against data controllers in the *private* sector, and there are probably even fewer of these rights that can be exercised by collective entities. While Sweden has provided legal persons with limited rights of access to information on them held by credit-reporting agencies,[969] credit-reporting laws in some other countries benefit individuals only.[970]

Probably the most extensive rights given to organised collective entities as data subjects can be found in legislation concerned with government agencies' handling of information. This legislation can be divided into three main types:

1) laws dealing specifically with the establishment and maintenance of government registers over legal persons;
2) laws on freedom of information (FOI); and
3) laws on government administrative procedure.

The first type of laws can set out the nature of the information to be put in a particular register, the purposes for which this information is to be used, the conditions under which it is to be made available to others (including the data subjects), and rules to ensure its accuracy.[971] In other words, these laws can provide

969 See further Chapter 10 (section 10.2).

970 This is the case, for example, with US federal laws on credit reporting (see the *Fair Credit Reporting Act* of 1970 and *Fair Credit Billing Act* of 1976 (15 USC § 1666)) and with credit-reporting legislation in the UK (see the *Consumer Credit Act* of 1974).

971 See, eg, Denmark's *Central Enterprises Register Act* of 2000 (*lovbekendtgørelse nr 598 af 22 juni 2000 om Det Centrale Erhvervsregister*) and Norway's *Enterprises Register Act* of 1994 (*lov om Enhetsregisteret 3 juni 1994 nr 15*).

considerable protection for data on legal persons but this protection will be primarily only in relation to a particular register kept by a government agency.

As for FOI laws, these often give collective entities (or individuals who can act on their behalf) legally enforceable rights of access to information on themselves (and others) which is held by government agencies. These laws can also provide some protection for business confidentiality by exempting trade secrets and certain other types of confidential business information from mandatory disclosure.[972] However, FOI laws often do not give data subjects an express right to demand rectification or deletion of data that are irrelevant, inaccurate or misleading in relation to the purposes for which they have been collected and stored.[973]

The absence of the latter right can be somewhat compensated for by laws on government administrative procedure. These laws typically embrace several fundamental principles to ensure that fair decision-making procedures are followed by government administrators. Basically, these principles on procedural fairness require that government decision-makers:

1) give an opportunity to be heard to persons (including collective entities) whose interests will be adversely affected by the decisions;
2) be unbiased or disinterested in the matter which is decided;
3) base their decisions on relevant evidence.[974]

Implementation of these principles usually means that parties to a particular case handled by a government agency, should be allowed a right of access to the case documents and a right to seek review of the agency's decision in the case. Implementation of these principles can also require a government agency to ensure a matter is researched to a reasonable extent before making a decision on it.

Neither FOI laws nor administrative procedure laws constitute at present complete data protection statutes. They do not provide collective entities as data subjects the whole range of rights typically provided to individuals under data protection laws although the limited rights they do provide can sometimes go further than the equivalent rights provided under data protection laws.[975] Moreover, FOI and

---

972 See, eg, for Australia, the federal *Freedom of Information Act 1982*, s 43(1); for Canada, the federal *Access to Information Act 1982*, s 20(6); for Norway, the *Act on Openness of Administration*, s 5a (in combination with ss 13(2) & 19(b) of the *Administrative Procedures Act*: see further *supra* n 831 *et seq* and accompanying text).

973 An exception is Australia's federal *Freedom of Information Act* although this only allows for amendment of information relating to the 'personal affairs' of individuals (see s 48) and is thus of little use to collective entities.

974 See, eg, Allars, *supra* n 452, chapt 6 for an overview of these principles as found in Australian administrative law. For an overview of the equivalent principles as found in Norwegian administrative law, see, eg, Eckhoff & Smith, *supra* n 36, chapts 18, 22–24.

975 For instance, in contrast to data protection laws, FOI laws usually allow persons access to both personal and non-personal information kept by government agencies. FOI laws also usually allow persons access to information not just on themselves but on other persons. For a useful overview and discussion of the differences and similarities between FOI and data protection laws, see Burkert, *supra* n 545, 49–69.

administrative procedure laws cover the handling of information by public sector agencies only.

It is somewhat incongruous that the basic principles embodied in FOI and administrative procedure laws are usually allowed to benefit collective entities as well as individuals, while the basic principles of data protection law are usually allowed to benefit only individuals. Significant similarities exist between the principles and aims of the two sets of laws. All of these laws are concerned with regulating the impact of government administration on private citizens. More specifically, all of the laws aim to increase the transparency, accountability and general quality of administrative decision-making processes and thereby protect private citizens from arbitrary and unfair actions that can result from these processes.[976] These similarities go a long way towards justifying the extension of data protection rights to collective entities at least *vis-à-vis* government agencies.

14.2.2 DESIRABILITY OF PROTECTION

Could the data protection interests of collective entities be adequately protected under branches of the law not directly concerned with data protection? This question addresses the issue of whether or not data protection legislation is the appropriate vehicle for regulating the processing of information on collective entities.

Several bodies have opined that data protection law is not the appropriate vehicle for such regulation. The Lindop Committee felt that protection of information on associations 'is more properly the subject of other branches of the law, such as company law, patent law, copyright law, or the law of confidential information in relation to trade secrets'.[977] The ICC has taken a similar view,[978] as did the group of French data protection experts appointed by the EC Commission to examine the desirability of protecting legal person data under data protection law. According to the latter group, data on legal persons should be protected by principles developed within commercial law, particularly legal doctrine relating to unfair competition.[979]

Several difficulties attach to the views of these bodies. First, they overlook that many collective entities (eg, non-profit and charity organisations) are neither set up for commercial purposes nor engaged in business activities. Hence, to base data protection for these types of entities on commercial law principles would be incongruous. Moreover, the problems with which the principles of data protection laws are specifically concerned do not have any *necessary* connection with commercial activities. This point can be illustrated by comparing the rationale for, and scope of, data protection rights with the rationale for, and scope of, intellectual property rights. The latter rights aim at preventing a person exploit for profit assets

---

976 See further Chapters 6 and 7 (sections 6.4.1 and 7.2.5).

977 Lindop Committee, *supra* n 505, 157, para 18.41.

978 ICC, *supra* n 748, 426.

979 Bancilhon *et al*, *supra* n 636, 34–35. See also Chamoux, *supra* n 636, 81.

created by another. They are oriented towards the commercial exploitation of property. Data protection rights, however, are concerned with simply regulating the processing of information (that is not necessarily of commercial value) about one's person. Their orientation is, first and foremost, the establishment of data-handling procedures to assist in securing data subjects a measure of privacy, autonomy, integrity, etc.[980]

Finally, setting into practice the views of the Lindop Committee and ICC could exacerbate a tendency to have rules on the handling of data on collective entities dispersed over a wide spectrum of legal branches with varying foundations and goals. Such a situation can make it difficult for legislators, policy makers, collective entities and individual citizens to get a clear idea of the general contours of the legal protection for such data.[981] This difficulty can hamper in turn the proper and speedy application of this legal protection. It can also hamper the process of legal reform. Such reform is particularly necessary in relation to laws aimed at regulating the handling of information, given the rapid development of various forms of information technology.[982]

Accordingly, significant value inheres in attempting to gather under one set of legislation data protection rights for collective entities. It is doubtful there exists any one branch of law, besides that represented by current data protection legislation, with a rationale and ambit broad enough to encompass all such rights. As intimated in the previous section, the laws most closely related to data protection legislation are those concerned with access to information kept by government agencies (FOI laws) and with government decision-making procedures (administrative procedure laws). For this reason, it would be quite natural to place data protection rights for collective entities within the body of these laws. However, these laws regulate the information

---

980 See further Chapter 7 (section 7.2). See also Poullet, *supra* n 464, 161–181. Poullet convincingly argues that the true rationale for data protection legislation is not to be described in terms of property rights or *ius in rem*, which view personal data as intangible goods similar to other forms of intellectual property. Instead, the true foundation for data protection law is 'the right to self-determination', a right which Poullet sees as relating primarily to one's liberty rather than one's property. Poullet's position builds upon the conceptual work by Rigaux on the nature of personality rights. Rigaux views personality rights as inhering in the freedom of persons to determine for themselves the character of their social identities. As such, personality rights – in contrast to property rights – are unable to be transferred from person to person. See generally F Rigaux, *La protection de la vie privée et des autres biens de la personnalité* (Brussels/Paris: Bruylant/Libraire Générale de Droit et de Jurisprudence, 1990), espec chapt 24.

981 See also Blume's criticism of using sectoral legislation in the field of data protection: P Blume, 'Om den skandinaviske registerlovgivning' (1987) 100 *TfR*, 445, 452–453. Note too Rossnagel, Pfitzmann & Garstka, *supra* n 638, 30 (attacking the legal regime for data protection in Germany for having become 'fragmented and unsurveyable' ('zersplittert und unübersichtlich')).

982 Cf Nordic Council of Ministers, *supra* n 60, espec Appendix 1 ('Legal Aspects of Information Security in the Nordic Countries'), 3, 11–12 (commenting that analysis and reform of legal rules on information security in the Nordic countries is hampered by the fact that such rules are not gathered within a discrete, unified body of legislation).

practices of the public sector only. To revamp these laws with extra data protection rights can be easy to rationalise if these rights are only to be exercised in relation to the public sector; it will not be easy to rationalise if the rights are also to be exercised in relation to the private sector.

14.3 Possible Legislative Regimes for Protecting Collective Entity Data

A large number of alternative legislative regimes exist under which collective entities could be accorded data protection rights. These alternative regimes divide into two broad categories according to the extent to which data on collective entities are protected in the same manner as data on individuals. Hence, we can have:

1) legislation protecting data on collective entities in basically the same manner as data on individuals; and
2) legislation protecting data on individuals to a much greater extent than data on collective entities.

These two categories of legislation can be broken down further into numerous sub-categories. The criterion for this further categorisation is the extent to which data on collective entities are protected under legislation protecting data on individuals. We can envisage, for example, the following alternatives:

- one piece of legislation that protects, in basically the same manner, data on both collective entities and natural persons;
- protection of data on collective entities in just one or two respects – for instance, by providing such entities with the right to gain access to and correct data on them held by certain organisations – albeit pursuant to the same piece of legislation that provides more general protection for data on individuals;
- two data protection laws, one covering data on collective entities only, the other just data on individuals;
- one data protection law to cover data on individuals only, leaving data on collective entities to be protected under various other laws;
- one data protection law to cover data on individuals only, and separate data protection laws to cover different types of collective entities.

Each of these alternatives also can be broken down into further sub-categories according to whether or not they cover data processing in both the private and public sectors. For example, the first-listed alternative can be broken down into the following sub-categories:

- one law that covers processing of data on both individuals and collective entities by *both* the private and public sectors;
- one law that covers processing of both types of data by the *private* sector only;

- and one law that covers processing of both data types by the *public* sector only.

Obviously, how one chooses between the various legislative regimes set out above depends largely on how one resolves the following four issues:

1) should data on collective entities be protected to basically the same extent as data on individuals?
2) should data on collective entities be protected under the same piece of legislation that protects data on individuals?
3) should *all* collective entities be given the same data protection rights?
4) should the data protection rights given to collective entities be observed by data controllers in both the private and public sectors?

An affirmative anwer to each of above four questions is defensible, particularly in light of the discussions in Chapters 11–13 and section 14.2.1 of this chapter. Given the conclusions of these discussions (and taking account of the tentative nature of some of the conclusions), there is much to be said for enacting one piece of data protection legislation that regulates the processing of both data on individuals and on collective entities in basically the same way. In relation to question 4, little sense attaches to providing collective entities with data protection rights that are not enforceable against data controllers from *both* the private and public sectors. This is because the interests of collective entities (and individuals) can be threatened by the processing of data on them by either public or private organisations. Moreover, the boundary lines between the public and private sectors are fading. In many countries, we find a tendency to privatise bureaucratic functions that have traditionally been fulfilled by public agencies, and a tendency towards greater exchange of data (on both individuals and collective entities) between public and private organisations.[983] Hence, any legislative response in the field of data protection will obviously be overly truncated if only the public or private sector is regulated.

Regarding question 2, this is largely a question of legislative format rather than substance. As such, it is perhaps the least important of the four issues. Moreover, its resolution should depend to a great extent on resolution of questions 1 and 3. There are good arguments for and against having one piece of data protection legislation to cover both data on individuals and data on collective entities. On the one hand, having one law can be more advantageous than having two (or more) separate laws as it can avoid unnecessary repetition, dispersal and/or fragmentation of legal provisions. Having one law could also be a sensible option given the fuzzy line that tends to exist between what is to be regarded as data on collective entities and what is to be regarded as data on individuals.[984]

On the other hand, a law can often become very cumbersome and dense if it is called upon to safeguard a large number of interests (eg, commercial and non-

983 See further Chapter 6 (section 6.2).

984 See further Chapter 10 (section 10.3).

commercial, emotional and non-emotional). There is also a risk it will end up with relatively flaccid rules.[985] However, having one piece of legislation to safeguard a mixture of interests will not *necessarily* result in the legislation becoming dense, unwieldy and/or flaccid. The extent of such a result will depend on other factors too; eg, factors concerned with statutory drafting technique and the substance of the principles set out in the legislation. It can be plausibly argued that the basic principles of data protection laws are already of sufficient generality as to be employable in the service of the interests of both collective entities and individuals, regardless of whether these interests are primarily commercial or non-commercial, emotional or non-emotional. This argument is elaborated upon further below.

As for questions 1 and 3, several factors militate against adopting legislation that protects data on all collective entities to basically the same extent as data on individuals. Many collective entities clearly have greater ability to look after their interests than individuals generally do. Further, large variation clearly exists between collective entities in terms of their scale and type of operations, their size, wealth and other resources. These factors could justify adopting a differential legislative approach; ie, an approach that discriminates between various types of collective entities in the extent to which each are given the data protection rights enjoyed by individuals. Such an approach is endorsed by Walden and Savage.[986]

While this approach appears reasonable, it can be realised at a variety of levels. Discrimination between various types of collective entities does not *have* to be realised by simply enacting, for instance, legislation that outright denies some (or all) such entities any opportunity of enjoying the data protection rights given to individuals. Discrimination between various types of collective entities could also be realised by enacting, for instance, legislation expressly benefitting all collective entities and individuals but also allowing for some discrimination to occur in relation to particular areas of application. The manner in which a differential legislative approach should be realised depends on several factors. One important factor concerns the ease or difficulty of determining – in a *fair*, *clear* and *uncontentious* way – the criteria for differentiating between the various types of collective entities. Determining these criteria in such a way is far from simple. Should one have regard to a collective entity's resources? If so, which resources? And how is one to measure these resources?[987] Certainly, it will be easy to differentiate between the situation of a large multinational corporation and that of a small family enterprise but there will be difficult and somewhat arbitrary lines to draw for the mass of private corporations lying between these extremes. The same will apply when attempting to draw lines based on other criteria, such as the goals of collective entities. If such line-drawing exercises do occur, they should be given some built-in flexibility so as to minimise unfair results. Consequently, it could be fairest (for all collective entities and the

985 See further Simitis, *supra* n 513, 158.

986 Walden & Savage, *supra* n 638, 347.

987 On the difficulties of devising such standards, see, ia, Stevenson, *supra* n 893, 73–75, 184–185.

individuals attached to them) to have in place a general framework of data protection rights which can be used for the benefit of *all* (organised) collective entities and individuals, but which also allows for the operation of the various rights to be adjusted on a case-by-case basis.[988] The power to carry out this adjustment could be given to the relevant data protection authority.

A related factor to be considered when determining the manner in which a differential legislative approach should be realised, concerns the basic nature of the principles of data protection law. More specifically, the nature of these principles has to be matched up and compared with the nature of the data protection needs of collective entities. We must ask whether the data protection needs of the various types of collective entities differ sufficiently as to justify different legislative regimes for each entity type. Similarly, we must compare the data protection needs of collective entities generally with the equivalent needs of individuals, and we must ask: do the two sets of needs differ sufficiently as to justify different data protection regimes for each class of data subject?

The core principles and rules of data protection laws are in themselves sufficiently broad and personality-neutral as to be capable of applying to both individuals and collective entities. Their personality-neutral character is due partly to their focus on procedural matters. In the main, they operate by regulating simply the processing, rather than content, of information. The only rules to which it is difficult to attach personality-neutral status are some of those dealing with the processing of certain classes of especially sensitive information,[989] but these rules constitute a small (and dispensable) part of data protection laws. The personality-neutral character of the laws' core principles and rules is also a reflection of the fact that the rights they express are so-called 'compound rights'; ie, rights that can be justified both in terms of a concern to protect individuals as autonomous moral agents, and in terms of a utilitarian concern with promoting overall social welfare.[990]

---

988 Cf Dan-Cohen, *supra* n 930, 113ff (recognising that the issue of whether or not a particular organisation should be given a particular legal right should not be resolved by pre-set categorisations focusing on the entity's legal form but by taking into account the concrete characteristics – complexity, size, permanence, transparency, etc –- of the entity in question).

989 See further Chapters 3 (section 3.9) and 10 (section 10.1.2).

990 See further Chapter 7 (espec sections 7.2.2 and 7.2.5). For discussion of these normative bases of rights as applied to organisations, see Dan-Cohen, *supra* n 930, chapters 4–5. According to Dan-Cohen, rights that can only be justified in terms of protecting individual autonomy and dignity (so-called 'autonomy rights') are difficult to assign to, and be exercised by, organisations in their own right, at least if organisations are viewed as essentially personless machines. However, organisations viewed as such may still be able to exercise autonomy rights derivatively – ie, for the benefit of individuals (*ibid*, 74–77). Further, if organisations and other types of collective entities are not viewed as personless (the better view, in my opinion), it is conceptually and normatively easier to argue that they can enjoy autonomy rights in their own right. As for rights that are best explained in utilitarian terms (so-called 'utility rights'), these can be assigned more easily to organisations than autonomy rights, even if one adopts the machine view of organisations: 'unlike the case of autonomy, there is nothing in the paradigm of utility that would necessarily, as a matter of principle, limit the range of

Most of the interests of data subjects which are promoted by data protection laws are capable of being shared by at least the broad majority of collective entities.[991] Concomitantly, many of the problems addressed by data protection laws are faced potentially, if not actually, by all collective entities (along with all individuals). The handling of data on individuals and collective entities alike in a manner not in conformity with the basic principles of data protection law can bring about unjustifiable detriment to either type of data subject.[992] Of course, the extent and type of this detriment will vary from case to case and this variation will depend in part on the characteristics of the data subject involved. Nevertheless, sight should not be lost of the fact that the principles of data protection laws address problems capable of afflicting any type of collective entity and individual.

In this discussion, we should not just take account of the interests of data subjects; we should adopt a broader perspective taking account of the interests of data controllers and society generally. Observing the principles of data protection laws when handling data on individuals and collective entities alike should have a positive effect on the quality of data controllers' administrative and decision-making processes. Ensuring, for example, that data controllers check the accuracy, completeness and relevance of information before they act on it, makes good administrative and/or business sense, regardless of whether the information is about individuals or collective entities.

Observing the principles of data protection laws when handling either type of information should also have – at least in theory – a positive effect on the quality of the myriad of relationships between data controllers and data subjects. It is reasonable to assume that a greater element of trust, co-operation and transparency would tend to be injected into these relationships were data subjects, be they large multinational corporations, small family enterprises or private individuals, aware that data controllers treat their data in accordance with the basic principles of data protection laws. Moreover, observing the latter principles would also tend to inject a greater element of fairness into these relationships, particularly when the data controller already enjoys a position of power over the data subject. This last point alerts us to the potential of the principles of data protection law to help redress the balance of power between weak and vulnerable persons/entities on the one hand, and

---

(Cont.)
rights given to organizations and prevent the law from assigning to them utility rights that are co-extensive with, or indeed broader than, those given to individuals' (*ibid*, 82). Whether or not organisations should be assigned utility rights depends on an assessment of the effect of such assignment on overall social welfare. As Dan-Cohen points out, most important legal rights can be plausibly explained along both jurisprudential lines – ie, are 'compound rights' (*ibid*, 86). He does not assess whether or not rights to privacy, let alone data protection rights, are compound rights but treats the right to freedom of expression as an instance of such.

991 See further Chapter 12 (section 12.3).

992 See further Chapter 13 (espec section 13.4).

strong and powerful persons/entities on the other, and to help strengthen the bases of democratic, pluralistic society.

It is usually State organs or large, private corporations that are cast in the role of powerful data controllers, while private individuals are usually cast in the role of the threatened data subjects. Actually, though, the latter role is not just occupied by private individuals; it can also be occupied by collective entities. There is a variety of contexts in which such entities (as data subjects) are vulnerable to the actions of data controllers. Such vulnerability is especially manifest in situations where there are tensions or inequalities already built into the relationship between data controller and data subject; eg, when a large corporation processes data on its smaller and/or medium-sized competitors. Yet the same large corporation can be vulnerable as a data subject itself in other contexts; eg, when it seeks financial credit or a government licence, or when data on its activities are collected, processed and disseminated by hostile public interest groups or trade unions.

The basic point emerging from this discussion is that all collective entities and individuals arguably possess as data subjects sufficiently similar interests in data protection as to justify having legislation in place that regulates the processing of data on all private sector persons/entities, both individual and collective. This point is reinforced by the fact that statutes dealing with governmental administrative procedure and FOI are often found to benefit all types of private corporations as well as individuals. As noted in section 14.2.1, the focus and operation of some of the central principles of these statutes are similar to the focus and operation of the basic principles of data protection legislation. At the same time, giving data protection rights to collective entities does not preclude the adjustment or fine-tuning of the operation of these rights so as to take account of various interest conflicts.

Probably the most controversial of these rights is that of information access. A fear has existed that private corporations could use any information access rights they are provided pursuant to data protection laws, in order to find out what information their competitors keep on them and to deduce thereby these competitors' business strategies.[993] It should be remembered that such problems are likely to arise only in the context of data protection legislation governing data processing in the *private* sector; they are unlikely to arise if data protection legislation only regulates processing undertaken by government agencies or if the legislation only allows private corporations access rights in relation to data kept on them by such agencies. Yet these problems can also be hindered through a variety of other control mechanisms, as illustrated in the relevant data protection legislation of Austria, Iceland, Norway, Italy and Switzerland. On the basis of the material presented in this book, it is difficult to determine conclusively how these control mechanisms function in practice. There appear to have been few practical problems in Norway and Austria caused by private corporations' use of information access rights *vis-à-vis*

993 See further Chapter 11 (section 11.1).

competitors.[994] Yet it also seems that, in Norway at least, private corporations were extremely reserved in exploiting these rights. Hence, it is possible that practical problems would arise in Norway (or other jurisdictions) if private corporations were to use these rights more actively and aggressively.

This possibility raises the issue of whether or not it is appropriate to give private corporations and other collective entities *any* right to seek access to data on them kept by other bodies in the private sector. Is, for instance, Denmark's restrictive approach pursuant to the *Private Registers Act* in this respect worth following? In my view, the access rights provided in that Act should represent the absolute minimum. At the same time, Denmark's refusal to provide *any* collective entity with information access rights in relation to private sector bodies other than credit-reporting agencies is problematic. It is problematic for three reasons. First, providing data subjects with a right of access to data relating to them is one of the most important elements of data protection law even if the right has tended to be little used in at least some jurisdictions.[995] This importance is due partly to the inherent, democratic value of the principle embodied by the right and partly to the instrumental value of the right as a means of ensuring satisfactory quality of information and, to some extent, information systems.[996] Loss of the former and latter value of the right can scarcely be fully compensated for by simply instructing data protection authorities, data controllers and/or their agents to carry out information quality checks. Secondly, not all types of private corporations or other collective entities operate for commercial purposes and/or are in direct competition (of a business nature or otherwise) with other bodies. It is doubtful, therefore, that all types of private corporations or other collective entities will be interested in seeking access to data other bodies keep on them, in order to gain some sort of competitive advantage over these bodies. Thirdly, there are a variety of controls that could be imposed to ensure collective bodies do not exploit their information access rights in a manner that damages (or threatens to damage) the interests of their competitors. Of course, some uncertainty exists about how many of these controls might function, particularly in situations where collective bodies aggressively use their information

---

994 See further Chapter 11 (section 11.2.2).

995 On this lack of use, see, ia, *supra* n 821; P Blume, 'How to Control Data Protection Rules' (1992) 6 *Int Computer Law Adviser*, no 6, 17ff; WBHJ van de Donk & H van Duivenboden, 'Privacy as policy: a policy implementation perspective on data protection at shopfloor level in the Netherlands' (1996) 62 *Int Rev of Administrative Sciences*, 513, 522–523. Although I have not seen any systematic surveys of the reasons why data subjects fail to utilise access rights, it would probably be simplistic to attribute such failure largely to data subjects' satisfaction with, or disinterest in, how their data are protected. No doubt many data subjects are unaware of their access rights or of how to use them; still others might refrain from using them out of fear of negative reactions from data controllers. See also Blume, *ibid*, 18.

996 Note, eg, the justification by the CNIL of its decision to grant business enterprises the right to gain access to data held on them by certain municipal councils: see *supra* n 775 *et seq* and accompanying text.

access rights. This notwithstanding, if policy-makers in a given jurisdiction cannot be certain that (i) these controls are incapable of functioning satisfactorily under pressure and (ii) collective entities in that country *will* aggressively use information access rights, it would be premature of the policy-makers to deny such entities *any* chance of using these rights.

Moreover, the access controls found in the relevant data protection laws of Austria, Iceland, Italy, Norway and Switzerland do not constitute the entire range of legislative mechanisms for regulating the use of information access rights by collective bodies. Several legislative strategies could be introduced to supplement the controls found in the above laws. For example, a country's data protection law could stipulate that collective bodies are only allowed access to data on them when:

1) these data do not contain any indication of how the data will be used by the data controller;[997] and/or
2) the data controller is not in the same field of business as the data subject.

A weaker (but arguably fairer) alternative to the latter condition is to allow for access to data when the data controller is in the same field of business as the data subject but only if (i) the controller has made a decision on the basis of these data and (ii) the decision detrimentally affects the legitimate interests or rights of the data subject.

Finally, note should be made of another potential problem with giving access rights to collective entities. In some contexts, such rights could be exploited in a manner threatening the privacy and autonomy of individuals. An example of such a context is when a collective entity demands access to data on it kept by one or more of its employees. The extent to which such use of access rights would be socially acceptable is far from clear and certainly impossible to determine in the abstract. There might well be situations in which such use of access rights is warranted (eg, when an employee threatens to publicise inaccurate or misleading data about his/her firm). In such situations, a variety of other legal remedies (eg, rules on defamation and breach of confidence) might also be available for the entity in question, though these will often apply only after damage is done.

If the data are held for private or household purposes only, they will usually fall outside the scope of data protection legislation.[998] However, determining the parameters of 'private or household purposes' could be difficult especially if the data are kept on a computer system operated by the collective entity concerned.

---

997 Cf the definition of 'personal data' in s 1(3) of the (repealed) UK *Data Protection Act* of 1984 (personal data is 'information which relates to a living individual ... including any expression of opinion about the individual *but not any indication of the intentions of the data user in respect of that individual*': emphasis added). As Walden and Savage point out, company A's ability to gain access to data that company B has stored on A will be of less commercial value to A if the data contain nothing about how company B plans to use it: Walden & Savage, *supra* n 638, 339. Cf also Art 10(1)(b) of Switzerland's federal *Data Protection Act* (permitting media organisations to deny access to data if access would disclose their future publication plans).

998 See further Chapter 2 (section 2.4.3).

In light of the above considerations, it would probably be overly drastic to disallow collective entities any right of access to data kept on them by individuals. At the same time, it would seem necessary to have in place a procedure allowing external assessment of the exercise of access rights in this context. It would also be desirable to require that collective entities inform their employees of their intention to exercise access rights with respect to data stored on their computer systems.[999] This would be in order to prevent exercise of these rights becoming, in effect, surreptitious surveillance of employees.

14.4 Summing Up

The rather superficial treatment in section 14.2 of the way in which collective entity data are currently protected by legal rules lying outside the body of data protection laws, cannot give rise to *firm* conclusions on the extent to which protecting such data under the latter laws is legally redundant or legally appropriate. Nevertheless, the discussion in section 14.2 tends to support the view that current legal safeguards for such data outside the body of data protection legislation are piecemeal and fail to provide all of the safeguards typically found in that legislation. Moreover, there does not appear to be any one branch of law, besides that of data protection, with a rationale and ambit sufficiently broad to encompass all of the basic principles of data protection in relation to both the public and private sectors.

The discussion in section 14.3 shows that a plausible case can be made out for claiming that the basic principles of data protection laws are sufficiently broad and flexible to cater for any differences between the data protection needs of the various types of collective entities and the equivalent needs of individuals. Accordingly, it would seem appropriate to have in place a general framework of data protection rights which can be used for the benefit of all individuals and collective entities. It would also seem appropriate to set this framework of rights in one set of legislation covering data processing in both the private and public sectors. As a point of departure, collective bodies should be given the opportunity of using *all* of the basic rights given to individuals, including the opportunity of seeking access to information held by all private and public sector bodies. At the same time, allowance should be made for the operation of the various rights to be adjusted on a case-by-case basis in accordance with how collective bodies actually exploit the rights and in accordance with how controls over such exploitation actually function.

---

999 Indeed, in some jurisdictions such notice would be mandatory. This is the case with, eg, Norway: see further the case law described in Bygrave & Aarø, *supra* n 554, 341.

15. Protection for Data on Non-organised Collective Entities

15.1 Introduction

This chapter considers the extent to which data on non-organised collective entities (hereinafter also termed 'group data') should be covered by data protection laws. The aim of the chapter is primarily to set out the main parameters of the issue rather than to resolve it. The level of analysis here does not pretend to be nearly as detailed as the analysis in the other chapters of Part III.

While the chapter is an obvious extension of the material covered in the rest of Part III, it also links up to the topic canvassed in Part IV – namely, the regulation of profiling practices. Moreover, its conclusions must be read in the light of the conclusions in Part IV.

15.2 Nature of Non-organised Collective Entities

Non-organised collective entities are constituted primarily on the basis of sets of persons being regarded as sharing certain characteristics. These characteristics can embrace a variety of criteria, such as age, sex, genetic disposition, education, income and/or ethnic background. There exists an almost infinite range of such criteria, which means there is an almost infinite range of group categories for non-organised collective entities and an almost infinite range of information linked to them. Such entities and information types can be defined at numerous levels of abstraction and generality.

What are the chief differences between organised and non-organised collective entities? The most obvious difference, of course, is in terms of level of organisation, but this difference itself gives way to a range of other, more subtle differences. To begin with, the two types of entity differ in terms of how their respective profiles are created. Organised entities tend to generate their own profiles to a greater extent than do non-organised entities. The profiles of the latter are more often determined largely by persons and/or organisations outside the group, though the group's intrinsic characteristics do, of course, play a role. In this sense, we can say (somewhat imprecisely) that organised collective entities tend to be groups constituted from

within, while non-organised collective entities tend to be groups constituted from without.

It follows from this that members of non-organised collective entities will tend to be ignorant of their entity membership more frequently than are members of organised entities. For the former, membership of a particular group will often be latent, activated only by the perceptions and actions of other persons and/or organisations.

Thirdly, membership of non-organised collective entities will tend to be involuntary to a greater extent than membership of organised entities.

Fourthly, there will tend to be greater chance of conflicts of interest arising between the individual members of a non-organised entity (eg, in relation to enforcement of legal rights) than between members of organised entities; concomitantly, the members of non-organised entities will tend to share fewer ties of loyalty.

Fifthly, the duality of non-organised collective entities tends to be less marked than with organised entities; ie, the former are usually less capable of being treated as entities that are greater than the sum of their individual constituents. Thus, arguments about the extent to which non-organised collective entities should enjoy legal protection tend to be rationalised largely, if not exclusively, in terms of what such protection will mean for the individuals attached to them. Additionally, it will usually be more difficult, in practical (and also legal) terms, for non-organised entities than for organised entities to exercise rights in their own right. The opportunity for collective decision making on the part of non-organised entities will tend to be more reduced than with respect to their organised counterparts.

Finally, the range of data on the structure (though not necessarily the profile or behaviour) of non-organised entities will tend to be small relative to organised entities.

These differences notwithstanding, we should not forget that non-organised collective entities can generate organised counterparts. For instance, the attention given to a non-organised group of persons can provoke certain of these persons to get together in organised forms for the purpose of protecting their common interests in the face of such attention. Many consumer protection organisations are results of such a process.

We should also not forget that, as with organised collective entities, some types of non-organised collective entities are so small or so narrowly defined that information on them can be linked to specific individuals and thereby categorised as 'personal data' pursuant to data protection laws. Concomitantly, drawing a hard and fast line between group data and personal data will often be difficult.[1000] Moreover, the processing of group data will frequently generate personal data when it is done

---

1000 See also J Bing, 'Beyond 1984: the Law and Information Technology in Tomorrow's Society' (1986) 8 *Information Age*, 85, 86; Rossnagel, Pfitzmann & Garstka, *supra* n 638, 66.

for the purpose of taking some sort of action in relation to the individual members of the target group.

15.3 Previous Approaches to Issue

To my knowledge, no systematic or extensive analyses have been undertaken of the extent to which group data should be covered by data protection laws. Certainly the issue has been broached but usually only in passing. We find also numerous instances in which the notion of 'group privacy' is canvassed but without examining how the notion could translate into a set of safeguards under data protection laws.

One such instance is presented in Chapter 12 (section 12.2.2) – namely, Bloustein's analysis of group privacy. The notion of group privacy is also canvassed, albeit briefly, by Bing and Flaherty. Like Bloustein, both these writers discuss the notion in terms of protection of individuals in groups, as opposed to protection of groups *per se*. Yet unlike Bloustein, Flaherty and Bing do not analyse the content of the notion in detail. Thus, it remains unclear to what extent the notion is respectively understood by Bing and Flaherty as encompassing both organised and non-organised entities.[1001] Moreover, they only raise the notion in relation to one particular problem. In the words of Flaherty, this problem occurs

> 'when an individual is identified or identifiable as a member of a certain group ... and then receives unwanted attention in the form of solicitations, discrimination, or publicity.'[1002]

Similarly, Bing locates the central problem to which the concept of group privacy (termed 'gruppevern' or 'gruppers personvern' in Norwegian) relates as being that 'membership of a group – which one cannot do anything about – implies that one has certain personal characteristics'.[1003] In other words, the problem identified by both writers concerns the (potentially negative) consequences for an individual which arise when another person or organisation deduces particular characteristics of that individual from the assumed characteristics of a group to which he or she is presumed to belong. Having identified this problem, both writers fail to make clear exactly how it might be resolved. They do not examine, for instance, the extent to which the problem could be alleviated by giving data protection rights to groups *per se*, although Bing does claim that recognition of the problem makes it easier to understand and accept the fact that some countries have extended their data

---

1001 It will be recalled that Bloustein's notion of group privacy encompasses both types of entity.

1002 DH Flaherty, 'Cumulative Data are Not Always Anonymous' (1985) 11 *Privacy Journal*, no 9, 3.

1003 'Et hovedproblem er at medlemskap i gruppen – som man ikke kan noe for – impliserer at man har visse personlige egenskaper': Bing, *supra* n 349, 72.

protection legislation to expressly cover data on legal persons.[1004] At the same time, it should be remembered that such legislation tends not to (have) protect(ed) information on non-organised collective entities (unless the information could be linked to specific individuals).[1005] Hence, protection of legal person data pursuant to this legislation goes only a short way towards addressing the problems identified by Bing and Flaherty in relation to group privacy.

Anton Vedder takes up the same sorts of problems though he links them not to the notion of 'group privacy' but to what he terms 'categorial privacy'. The latter notion is explicated in the following terms:

> 'Categorial privacy can be considered to be relating to information (1) which was originally taken from the personal sphere of individuals, but which, after aggregation and processing according to statistical methods, is no longer accompanied by identifiers indicating individual natural persons, but, instead by identifiers of groups of persons, and (2) which, when attached to identifiers of groups and when disclosed, can cause the same kind of negative consequences to the members of those groups as it would to an individual person if the information were accompanied by identifiers of that individual.'[1006]

Unfortunately, Vedder's notion of 'categorial privacy' is made diffuse by his omission to define what he means by 'privacy'. Nevertheless, he links 'categorial privacy' to the same basic problem identified by Bing and Flaherty above:

> 'the [group] information is often used in judging and treating individuals *as if it were*, strictly speaking, personal information: the individual is judged and treated on the basis of his 'virtual' counterpart, a group to which he accidentally belongs.'[1007]

Moving to expressions of opinion about the extension of data protection rights to non-organised collective entities, we find a relatively small number of persons supporting – at least in principle – some form of safeguards for group data pursuant to data protection law. In some cases, there is a failure to elaborate on what form such safeguards should take.[1008] In other cases, support seems to be expressed for protecting group data in a manner that is largely commensurate with the protections

---

1004 Bing, *supra* n 1000, 87.

1005 Information relating simply to an ethnic group, for example, was not regarded as 'personal information' pursuant to s 1 of Norway's PDRA. See further Chapter 10 (section 10.1.1).

1006 A Vedder, 'Privatization, information technology and privacy: reconsidering the social responsibilities of organizations', in G Moore (ed), *Business Ethics: principles and practice* (Sunderland: Business Education Publishers, 1997), 215, 221.

1007 *Id*.

1008 See, eg, K Anér, *Datamakt* (Falköping: Gummesson, 1975), 145–146.

given to data on individuals.[1009] Quite commonly, though, what is singled out is a need for quality controls of group data in order to minimise the chance of the group members being subjected to unfair discrimination or other harm. Sometimes, it is proposed that such quality controls involve the provision of access and rectification rights for groups.[1010] Sometimes, proposals are made that such quality controls encompass more than just group data but also the information systems used to process these data (and personal data generally).[1011] The latter proposals complement, and can be linked to, arguments for greater recognition and protection of group interests in administrative law generally.[1012]

We seldom find detailed suggestions as to what obligations should be imposed on data controllers or data protection authorities in order to realise the above proposals. One attempt is made by Vedder:

> 'What should be expected from organizations or their executives [who process group data] is at least a willingness to develop a kind of sensitivity to the possible social impact of their activities and policies and a readiness to bring about a maximum transparency of their activities and policies.'[1013]

Not all who address the issue of data protection for non-organised collective entities are in favour of extending the ambit of data protection laws to cover group data. The Skauge Committee in Norway refrained from recommending such an extension for two reasons: first, lack of need; secondly, 'difficult border-delineation problems' ('vanskelige avgrensningsproblemer').[1014] The Committee did not elaborate on the latter reason. With respect to the former reason, the Committee asserted that data on groups will rarely be experienced as 'very personal' in the same way as data on individuals.[1015] These points are revisited in section 15.6.

15.4 Existing Safeguards under Data Protection Laws

Most if not all data protection laws refrain from providing express coverage for data on mere groups. An apparent exception to this pattern is the Finnish legislation: the *Personal Data Act* of 1999 (like its predecessor, the *Personal Data Registers Act* of

---

1009 See, eg, the Bayerl Report, *supra* n 652, 28.

1010 See, eg, S Rodotà, 'Privacy and Data Surveillance: Growing Public Concern', in *Policy Issues in Data Protection and Privacy*, OECD Informatics Studies 10 (Paris: OECD, 1976), 130, 135.

1011 See, eg, Bing, *supra* n 19, 252.

1012 See, ia, E Boe, *Innføring i juss: Statsrett og forvaltningsrett* (Oslo: TANO, 1993), 372 (pointing out that one way of exercising control of administrative systems is to allow rule-of-law principles serve group interests).

1013 Vedder, *supra* n 1006, 224.

1014 NOU 1997:19, 53.

1015 *Id*.

1987) expressly covers data not just on an individual but also 'his [*sic*] family or those living with him in the same household' (s 3(1)).

At the same time, data protection laws generally will offer group data, along with the groups to which the data refer, indirect protection insofar as the data can be linked to a specific individual. Further details on the extent of this possibility can be gleaned from the discussion in Chapter 10 (section 10.3).

Moreover, data protection laws (and/or data protection authorities exercising their powers under these laws) can reduce attention on non-organised (and organised) collective entities by limiting the processing of data on the entities' individual members. A pertinent example is the extra limitations put by most data protection laws on the processing of designated categories of especially sensitive data.[1016] These limitations indirectly restrict the discriminatory treatment of collective entities defined on the basis of these data categories. Other pertinent examples are the limitations put by some laws on the criteria that credit-reporting agencies may use to categorise persons.[1017] Again, such limitations indirectly restrict discriminatory treatment of the collective entities that are defined on the basis of these criteria.[1018]

15.5 Group Actions

Indirect protection of non-organised collective entities can also occur when data protection laws (and/or data protection authorities exercising their powers under these laws) allow for some sort of group action; ie, they have procedural rules in place which facilitate the effective treatment by data protection authorities and/or courts, of complaints that are common for large numbers of people (as data subjects). There are three main kinds of group actions:

1) the *private group action* (also called 'class action' or 'representative action'), whereby an individual member of the affected group institutes an action without being commissioned to do so by the other group members, but where the outcome of the action may be binding on the whole group;
2) the *public group action* which is instituted by a public authority on behalf of the affected group; and
3) the *organisational action* which is brought by a private organisation on behalf of the affected group.[1019]

1016 See further Chapters 3 (section 3.9) and 18 (section 18.4.3).

1017 See, eg, ss 20(1) and 23(4) of the Danish *Personal Data Act*.

1018 For further instances of indirect protection of groups, see Chapter 18 (sections 18.3–18.4) dealing with the ways in which data protection laws regulate the generation and use of profiles.

1019 For further detail on the characteristics of the various kinds of group action (with particular focus on the modern American 'class action' pursuant to Rule 23 of the US *Federal Rules of Civil Procedure*), see PH Lindblom, *Grupptalan. Det anglo-amerikanska class actioninstitutet ur svenskt perspektivt*

The primary form for group action embraced by data protection laws is a form for public group action, with data protection authorities representing and advancing the interests or claims of groups of data subjects, though typically outside the setting of court litigation and only when the data subjects are individuals. Examples of data protection laws that make express provision for either of the other two types of group actions (class actions and organisational actions) are relatively scarce.

A lonely example of express provision in a data protection law for class actions is s 36(2), in conjunction with ss 38–39, of Australia's federal *Privacy Act*. This allows the Privacy Commissioner to entertain so-called 'representative complaints' if certain conditions are met. So far only one such complaint has been made.[1020] It should be emphasised that the provisions in the Act dealing with representative complaints protect a collective entity in the sense of a group of individuals who have been similarly affected by a similar breach of law. There is no prerequisite for this group to be organised in order for a representative complaint to be mounted. The protection afforded by the action is not primarily of the collective entity as such but of the individuals making up the entity.

With respect to organisational actions, the Netherland's *Data Protection Act* of 1988 (repealed) made specific provision (in s 10(2)) for such actions up until 1994. Thereafter, this provision was removed on account of more general provision for organisational actions being introduced into the Dutch *Civil Code*.[1021]

While there is no equivalent provision for organisational actions in the Norwegian PDA or its predecessor (the PDRA), both the Data Inspectorate and the Ministry of Justice have heard complaints (under the PDRA) brought by organisations on behalf of non-organised groups of persons.[1022] The willingness of the Inspectorate and Ministry to hear such complaints would seem to reflect the readiness on the part of Norwegian courts to allow for organisational actions even when the outcome of the matter at dispute does not have 'direct significance' ('direkte betydning') for the organisation itself or its members.[1023]

(Cont.)
(Stockholm: Norstedts, 1989); and PH Lindblom, 'Group Actions in Civil Procedure in Sweden', in S Strömholm & C Hemström (eds), *Swedish National Reports to the XIIIth International Congress of Comparative Law* (Uppsala: Almqvist & Wiksell International, 1990), 59–100.

1020 Case C2776, opened 3.7.1995, closed 6.12.1996. The complaint was mounted by a group of women employees at a social club who complained that video surveillance cameras had been covertly installed to film their work change-room. The complaint was withdrawn after being resolved pursuant to the federal *Sex Discrimination Act 1984*.

1021 See Arts 305a & 305b in Chapt 3 of the Code (*Burgerlijk Wetboek*).

1022 See, eg, case 85/1367 concerning a complaint brought by a citizen initiative group called 'Folkeaksjonen mot bompenger i Bergen'. The case facts are summarised in Bygrave, *supra* n 37, 59–61.

1023 See espec the judgments of the Norwegian Supreme Court in the so-called 'Alta' and 'Saugbrugsforeningen' cases (reported in Rt 1980, 569 and Rt 1992, 1618 respectively). More generally, see Eckhoff & Smith, *supra* n 36, espec 510ff; J Hov, *Rettergang i sivile saker* (Oslo:

The apparent paucity of data protection laws making express provision for class actions and/or organisational actions is somewhat surprising. Indeed, my impression is that the bulk of data protection discourse has shown little if any interest in these sorts of group actions, even in recent years. For instance, neither the EC Directive nor its *travaux préparatoires* make one mention of the possibility or desirability of class and/or organisational actions. This lack of interest is incongruous with the evidence of increasing readiness in many Western legal systems to allow for class and/or organisational actions in other areas, such as environmental and consumer protection, with some similarities to that of data protection.[1024]

15.6 Extending Protection Levels?

When canvassing whether and how current safeguards for data on non-organised collective entities should be extended pursuant to data protection laws, regard must be had to the factors listed in Chapter 9 (section 9.1). It will be recalled that the primary factor is the *need* for extending such protection. This factor breaks down into several other factors the most relevant of which for present purposes can be summed up as:

1) the extent to which non-organised collective entities have interests that could be safeguarded by data protection laws;
2) the extent to which these interests are already safeguarded by data protection laws; and
3) the extent to which these interests are protected under other types of laws.

Regarding the first-listed factor, we must remember that the duality of non-organised collective entities is less pronounced than with organised bodies. Thus, analysis of the factor must take as its point of departure the data protection interests of the individuals who form or are otherwise linked to the groups. At the same time, the analysis must be primarily related to the processing of data on the groups as such, not data that can be linked to specific individuals (though, as pointed out above, the distinction between the two data types will often be blurred). Moreover, the interests in question will have a collective dimension, such that the analysis must also encompass an appraisal of the relevant interests of the groups constituted by the individuals and, ultimately, the relevant interests of the wider society.

It is obvious that non-organised collective entities and the individuals attached to them have interests related to the processing of data on the entities as such and that these interests are logically capable of coverage by data protection laws. Also obvious is that the interests encompass all those described in Chapter 7 (section

---

(Cont.)
Papinian, 1994), chapt 7; IL Backer, *Rettslig interesse for søksmål, skjønn og klage – særlig ved naturinngrep* (Oslo: Universitetsforlaget, 1984), espec 146ff.

1024 See, eg, *Grupprättegång*, SOU 1994:151, Part A, chapt 8 for an overview.

7.2.5); ie, interests in data validity and information utility, together with interests in the quality of information systems, and interests in privacy, autonomy, civility, democracy, pluralism, rule of law and balanced control.

It will be recalled from section 15.3 that the Skauge Committee expressed scepticism towards protecting group data, partly for the reason that such protection is unnecessary. Elaborating on this reason, the Committee held that group data would rarely be experienced as 'very personal'.

This focus on the 'very personal' seems overly narrow given that law and policy on data protection have broader concerns. Additionally, at least some group data will often be experienced as 'very personal' – eg, data on families, households, groups with diseases. As a general rule, group data are increasingly likely to be experienced as personal the smaller the group is or the more sensitive the data are. We must also not forget that the sensitivity of group data can vary from culture to culture. For example, data relating to certain tribal customs can be extremely sensitive (and/or 'personal') for members of the tribe concerned though not for others.[1025]

More generally, the Committee's assertion that there is no need for protecting group data is difficult to square with the fact that the processing of such data can be harmful to the individuals who are linked to the group. There are numerous examples of this detrimental potential of aggregate/group data. An oft-cited example is the US Army's use, during World War II, of aggregate data from the US Census Bureau to aid in locating and incarcerating persons of Japanese descent living in the USA.[1026] Yet aggregate/group data do not cease to be innocuous simply in wartime or military contexts. A large variety of other situations exist in which such data can serve to stigmatise or otherwise harm individuals. These situations span the fields of research, marketing, insurance, immigration control and employment – to name but a few.[1027] Furthermore, these situations are increasing in tact with the developments in surveillance and control set out in Chapter 6 (section 6.2) and related developments in the use of profiling as depicted in Chapter 17 (section 17.2).

In most, if not all, of these situations, three main sets of problems can arise for the individual members of the group concerned:

1) the individual can be given an identity that is not of his/her choosing or that is objectively invalid (thus violating his/her integrity, interfering with various of his/her autonomy-related interests – particularly the interest in identificational self-determination – and/or sowing the seeds for the other problems listed below);

1025 See further *Minding our own business. Privacy protocol for Commonwealth agencies in the Northern Territory handling personal information of Aboriginal and Torres Strait Islander people* (Sydney: Privacy Commissioner, 1998).

1026 See further D Burnham, *The Rise of the Computer State* (London: Weidenfeld & Nicholson, 1981), 22–25.

1027 For examples, see Flaherty, *supra* n 1002, 3, 6; Bing, *supra* n 1000, 87–88. See also Chapter 17 (section 17.3).

2) he/she can be subjected to unwanted attention (thus incurring interference with a range of his/her privacy- and autonomy-related interests – particularly the interests in non-interference, non-information, in-flow control and attentional self-determination);
3) he/she can be subjected to unwanted or unjustified discrimination (thus violating his/her integrity and otherwise interfering with various of his/her autonomy-related interests).

Of course, the actual extent of harm incurred will depend partly on the quality (more specifically, the validity) of the group data – including the links attributed to these data with the individual concerned – and partly on the ways in which these data are acted upon in relation to the individual. It will further depend partly on the extent to which the individual is made aware of these uses. At the same time, the harm incurred might have an impact on more than just the individuals linked to the data. The quality of society generally (eg, in terms of the level of civility and pluralism it offers) might also be affected.

As for the extent to which the data protection interests of non-organised collective entities are safeguarded under current data protection laws, the analysis in sections 15.4–15.5 reveals that most such safeguards are of an indirect nature only. Of arguably greatest concern is the apparent lack of direct controls on the quality of group data. This point is revisited in Chapters 18–19.

Regarding the extent to which the data protection interests of non-organised collective entities are safeguarded by legal rules other than those found in data protection legislation, analysis of this requires examining all branches of the law in a given jurisdiction to identify rules on the collection, use, disclosure, quality and security of group data, along with rules on accessing and rectifying such data. It would seem most natural to analyse firstly the scope of rules aimed at combatting defamation and various forms of discrimination as these often provide some protection of group integrity in relation to the processing of group data. Other sets of rules, such as those found in legislation and/or agreements on workers' rights, could also be relevant. Consideration will also need to be given not just to legal rules but also other normative codes, such as guidelines for scientific research. No attempt shall be made here to analyse the reach of these sorts of rules in detail. I venture to suggest, however, that it is doubtful they provide, alone or together, the gamut of safeguards provided by data protection laws. For example, anti-discrimination legislation usually only limits certain uses of group data defined on the basis of sexual, racial or religious criteria.

Turning to the issue of *how* protection should be given to group data, discussion of this needs to be divided along three levels of analysis:

1) what sort of obligations should data controllers have with respect to group data?
2) what sort of rights should the group members have with respect to such data?

3) what sort of powers should data protection authorities have with respect to such data?

Question 1 is essentially concerned with the extent to which data controllers should process group data in accordance with the basic principles of data protection law. In approaching this question, it should first be noted that all of these principles are logically capable of applying to group data.

At the same time, care will need to be taken that any requirements that the data be processed in accordance with these principles do not constitute an unjustified interference with rules on freedom of expression. There is a real risk that subjecting the processing of group data to stringent data protection norms will involve such interference. I refrain here from analysing in detail where and how the balance between data protection and freedom of expression should be struck – such an analysis goes well beyond the tasks of this book. It suffices to say that the above risk will escalate in proportion to increases in both the generality of the group data subjected to regulation and the stringency of this regulation – particularly in terms of the ability to communicate/disseminate group data. Some allowance must probably be made for data controllers to communicate/disseminate (ie, express) opinions about groups of persons – especially relatively broad groups – even if the opinions are of dubious validity or promote social prejudice (eg, 'housewives are fat'; 'Nazis are good'; 'Australians are lazy'). Yet again, exactly how much allowance must be given is difficult to determine – particularly in a non-private/-domestic context. No doubt, some people would argue that respect for the right to freedom of expression requires that all group data be omitted from coverage under data protection laws. Others would argue that such data be covered only when the data are intended to be used in a manner that seriously infringes the privacy and related interests of the individuals attached to the groups concerned. I tend towards support of the latter position. Concomitantly, I believe that the degree to which we permit the interest in freedom of expression to restrict data protection safeguards for group data should vary according to whether or not the data controller is utilising the data in a decision-making process that could have considerable detrimental effects for the group members.

One possible way of tackling the above tension would be to apply only the principle of fair and lawful processing to group data and permit data protection authorities to chisel out more detailed rules pursuant to this principle on a casuistic or sector-specific basis. This approach would provide flexibility at the same time as it would reduce the risk of regulatory overreaching. Part and parcel of this approach could be the insertion of provisions requiring data controllers to take account of the social impact of their processing operations with respect to group/aggregate data, and to notify data protection authorities of basic facts regarding these processing operations.

Arriving at a satisfactory answer to question 2 is a great deal more difficult on account of some of the features of non-organised collective entities noted in section

15.2. For instance, much uncertainty attaches to how the exercise of access and rectification rights could practicably work in relation to group data. What would happen if, for example, one group member wants to rectify data on the group, yet another group member does not because he/she believes the data to be correct? This potential conflict might be able to be solved by way of an objective (third party) assessment of the validity of the data concerned. Further, a record could be made of the group members' respective assertions and kept with the data.

Larger problems arise with respect to the exercise of consent requirements. What if one or more group members consent to the processing of data on the group, but other group members do not? Should one only take account of what the majority of group members decide (as is sometimes the case in labour agreements)?

A possible solution here would be to cut back on group consent requirements in relation to the processing of group data. This reduction could be off-set by the exercise of paternalistic consent mechanisms on the part of data protection authorities; ie, the latter could be given competence to set conditions for the processing of group data. The extent and character of this competence (eg, licensing or notification) – together with the stringency of the conditions set – could vary in accordance with the extent to which the planned processing would interfere with the legitimate interests of the group members. It is probably also desirable that these conditions attempt to regulate the basic architecture of the information *systems* used.[1028]

As for question 3, I refer to what is written above in relation to the other two questions.

15.7 Summing Up

Although there exist a multiplicity of differences between organised and non-organised collective entities, to deprive the latter of any data protection rights purely because they are non-organised is scarcely defensible. Any appeal to organisational criteria as a basis for discriminating between the two types of entities in this context needs to be analysed carefully. Of paramount importance is not so much an entity's degree of organisation but the extent to which it and its constituent members have interests that are capable and deserving of protection pursuant to data protection law.[1029]

Nevertheless, to legally operationalise data protection rights for non-organised collective entities is difficult precisely because of the lack of organisation. This difficulty notwithstanding, extending express protection to group data would probably not be legally impracticable, especially if the protection were

1028 See further Chapter 19 with respect to control of profiling practices.

1029 Mæland takes a similar view when considering the extent to which collective entities should be protected pursuant to defamation law: see Mæland, *supra* n 883, 108–109.

operationalised primarily as a set of requirements for data controllers or a type of control competence for data protection authorities. Further, extending such protection would probably not be legally redundant, at least with respect to control of the quality of group data.

Thus, consideration should be given to requiring data controllers to process group data in accordance with at least some of the core principles of data protection laws – notably, the principles of fair and lawful processing, purpose specification, minimality, information quality, disclosure limitation and information security. Further, consideration should be given to requiring data controllers to notify data protection authorities of the processing of group data when the processing is carried out in order to control or manipulate the members of the group. And consideration should be given to permitting data protection authorities to set conditions for the processing of group data when this processing carries significant risks for the interests of the group members.

Finally, consideration should be given to allowing for group and organisational actions along the lines provided for by Australian and Dutch legislation.

16. Concluding Observations for Part III

Support for the idea that collective entities should be given data protection rights has never been widespread. Strongest opposition to the idea, at least in terms of rights for legal persons, appears to have come from large business bodies. Nevertheless, there was a fairly strong trend during the 1970s to propose and/or enact data protection laws expressly covering data on legal persons (as well as individuals). In some instances, protection has also been extended to data on other types of organised collective entities but it has seldom been extended to data on mere groups.

These laws have been proposed and/or enacted for a variety of reasons some of which are connected not just with a concern to provide more complete data protection for individuals but also to protect the interests of collective entities as such. There is little solid evidence to support the claim that these laws have also been introduced for reasons of economic protectionism.

While the data protection Acts expressly safeguarding data on organised collective entities are broadly similar, they are neither completely uniform in their ambit, the level of detail of their provisions nor in the stringency of their control regimes. Nevertheless, they all protect data on collective entities to a much larger degree than those laws expressly safeguarding data on individuals only. While the former Acts recognise and safeguard the data protection rights of collective entities *qua* such entities, the latter laws do not.

However, the fact that a country's data protection law expressly protects data on individuals only, does not necessarily mean that organised collective entities operating in that country have been left without any data protection. There are at least five ways in which these entities can be protected. First, the country's data protection authority could have used its powers to give such entities some data protection rights without this extension of protection being reflected in actual legislation. This is, for example, the situation in France. Secondly, collective entities could have been given some rights as data subjects in relation to a specific type or sector of data processing, these rights being set down expressly in sectoral legislation. This is, for instance, the case in Sweden in relation to the credit-reporting and debt-recovery industries. Thirdly, collective entities are given some measure of indirect protection through limitations being set on the processing of certain data on their individual members. Fourthly, they could be afforded indirect protection through flexible rules on standing.

Fifthly, data on collective entities could be protected if they fall within the definition of 'personal data' (or 'personal information') pursuant to the country's

main data protection law. Yet such protection may occur only in order to make the protection of data on individuals more complete. Concomitantly, data on collective entities will only be protected by the data protection law to the extent they can be linked to specific individuals. The extent to which such data can be linked to individuals depends on the way in which the term 'personal data' (or 'personal information') is defined in the relevant law. The vague manner in which this term tends to be defined makes it difficult to determine what data on collective entities will qualify as personal information pursuant to the relevant law.

The central conclusion of this Part is that the case in favour of giving at least some data protection rights to collective entities (primarily those that are organised; secondarily those that are non-organised) appears to be stronger than the case against giving these entities such rights. This conclusion builds on a range of factors the most important of which are the following. First, the basic principles, rules and rationale of data protection laws are conceptually capable of servicing the interests of collective entities. Secondly, giving collective entities data protection rights can be of practical assistance to them and to the individuals who constitute them. Concomitantly, in many situations where the data protection interests of a collective entity are injured, there can also be injury to the individuals behind the entity. Thirdly, extending coverage of data protection laws to data on collective entities can enhance, in sum, the general transparency of data processing operations, thus promoting a diffusion of knowledge for the benefit of wider society. Fourthly, and closely related to the previous point, giving data protection rights to collective entities can expand the possibility of hindering development of control mechanisms facilitating the misuse of power and undermining the bases of pluralistic, democratic society. Finally, giving data protection rights to collective entities (at least those that are organised) does not *necessarily*:

1) increase such entities' ability to maintain operational secrecy to the detriment of the general public interest;
2) weaken the ability of individuals to exercise their own data protection rights;
3) force collective entities to disclose sensitive business information to their competitors;
4) overburden data protection authorities or collective entities (as data controllers); or
5) significantly hinder transborder flows of collective entity data.

At the same time, any extension of data protection rights to collective entities will need to be carefully balanced with other, partly opposing rights. In particular, legislating safeguards for the protection of data on non-organised collective entities will need to make adequate provision for the right to freedom of expression. Achieving the appropriate balance here will be a major challenge.

We should also remember that the empirical basis for some of the above claims about the practical consequences of data protection for organised collective entities

(particularly claims 4–5) is rather thin. The claims primarily reflect Norwegian (and, to a lesser extent, Austrian and Danish) experiences in giving data protection rights to legal persons. It cannot be said with any certainty that other countries have had or will have the same experiences. The extent to which claims 1–5 will be true for a given country will largely depend on the interplay of several variables, including the policies and actions of the country's data protection authority and the nature of the country's corporate culture. Thus, it would be foolish to assert that on the basis of the experiences and material presented in this Part, each and every country should extend data protection rights to collective entities. One can safely assert, though, that on the basis of the material presented here, there are good reasons for all countries to seriously consider allowing collective entities the benefits of data protection rights.

PART IV
PROFILING – REGULATION BY DATA PROTECTION LAWS

'What has happened … is that we have come to mistake our reach for our grasp. With the modernization of consciousness has come belief that information is a reasonable substitute for knowledge, and that knowledge, rationally accumulated, is a reasonable substitute for wisdom.'

– L Thayer, cited in R-J Ravault, 'The Ideology of the Information Age in a Senseless World', in JD Slack & F Fejes (eds), *The Ideology of the Information Age* (Norwood, New Jersey: Ablex Publishing Corp, 1987), 187.

17. Profiling as Practice and Problem

17.1 Introduction

The central theme of Part IV concerns the ways in which profiling practices challenge the regulatory capabilities of data protection laws. The theme is taken up mainly in Chapter 18. The present chapter presents necessary background material for the theme by describing the ways in which profiling practices threaten data protection interests. More specifically, this chapter describes, firstly, what profiling is and how it is practised (see section 17.2). It then describes the ways in which profiling may impact upon data protection interests (see section 17.3).

Much of the analysis in this chapter and the next builds upon and extends the material presented elsewhere in the book. Of particular relevance for this chapter is the material presented in Part II, while some of the material in Part III is especially relevant for Chapter 18.

17.2 Profiling as Practice

As a definitional point of departure, profiling is the inference of a set of characteristics (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics. The set of characteristics will typically relate to the behaviour (actual or expected) of a person/entity. Thus defined, profiling is neither a new nor extraordinary phenomenon. All people engage in some form of profiling as an integral part of relating to other persons and organisations, though they often do so only in an informal or non-systematic way. What is new – and which deserves the attention of this book – is the increasingly extensive, systematic use by organisations of relatively formalised and sophisticated profiling practices for a variety of control purposes. This is not to suggest that such practices are only of recent origin; instances of them have existed through the ages and, in some cases, with potentially dire consequences for those profiled (witness, eg, the outcomes of judicial sentencing). Yet the expansion and intensification of such practices in recent years can scarcely be denied. Details of this development are elaborated upon further below. First, though, it is necessary to describe the profiling process in more detail.

The profiling process has two main components: (i) the process of inferring a profile; (ii) the process of treating persons/entities in light of this profile. The former component can also be formulated in terms of profile generation, the latter component in terms of profile application. As pointed out below, the line between the two components can blur in practice.

The inference process typically consists of processing and analysis of data in search of patterns, sequences, relationships, etc. The resultant profile is essentially a set of assumptions based on probabilistic reasoning. As for the treatment process, this involves making a decision about a person/entity based on the profile generated. The decision will often, though need not, result in the taking of concrete measures with respect to the person/entity profiled or other persons/entities. In cases when the decision is made only about the person/entity profiled and does not result in concrete measures, the treatment process will be difficult to distinguish in practice from the inference process. Furthermore, the application of a profile related to one person/entity can lead to the generation of a new profile for another person/entity.

It will be obvious from the above that profiling – particularly the treatment process – is closely tied up with discrimination in the sense that it involves taking (or not taking) action (often exclusionary) on the basis of perceived differences between persons (or classes of persons).

Profiling is to be distinguised from the matching or cross-checking of various sets of data. However, as demonstrated in the next chapter, profiles can be generated, reinforced or modified on the basis of data matching, and matching operations can be designed and initiated on the basis of profiling. Hence, legal controls of data matching will tend to affect the ability to carry out profiling and *vice versa*.

The tasks involved in profiling can be carried out by a single person or organisation. Alternatively, they can be divided or shared between a multiplicity of persons/organisations. For instance, the generation of a profile can be undertaken by one organisation (or group of organisations), and application of the profile by another.

In the following, a person/organisation who/which engages in the generation and/or application of a profile is termed ‘profiler’. At the same time, a profiler will usually be a data controller, data processor and data user. As for those persons/ entities that are profiled, these are termed ‘data subjects’.

Some studies confine the concept of profiling to particular ways of generating and applying profiles. For instance, a study by the former Office of Technology Assessment (OTA) that was attached to the US Congress appears to view profile generation as necessarily involving a process by which the profile of a particular person is built up mainly from data or assumptions about *other* persons (with whom the first person is linked).[1030] Analyses by Roger Clarke and the Australian Privacy

1030 See US Congress, OTA, *Federal Information Technology: Electronic Record Systems and Individual Privacy* (Washington, DC: US Government Printing Office, 1986), 87–88.

Commission seem to take the same point of departure.[1031] They also appear to view profile application as necessarily involving a database search to identify other persons who fit the profile concerned. Moreover, all of these studies apparently consider profiling as a process ultimately targeted at individuals (as opposed to collective entities).

The definitional point of departure for this book does not delimit the concept of profiling along such lines. Thus, profiling can target an individual, an organised collective entity or a non-organised collective entity. Concomitantly, a profile can relate to any one of these three categories. Further, the generation of a profile can be based exclusively upon data relating to the person/entity who/which is profiled, or it can be based, partly or wholly, on data relating to other persons/entities. Finally, the application of a profile does not have to involve a database search for other profile targets; such targets might be clearly apparent already at the stage of profile generation.

Despite (and because of) this broad point of departure, it is heuristically useful to single out two basic forms of profiling which can serve as reference points in the course of Part IV analysis. One form involves the inference of a set of characteristics about a relatively abstract category of persons or collective entities (eg, male university students; large multinational corporations). These characteristics are then employed to assess persons or entities who/which are seen to belong to the category. Following Clarke, this form of profiling is termed 'abstract profiling'.[1032] The other form of profiling involves the inference of a set of characteristics about a specific individual or organised collective entity on the basis of collection and analysis of data related to *that* person/entity, as opposed to data related to other persons/entities or an abstract category of person/entity. This form of profiling is sometimes called 'personal profiling'.[1033] Here, however, it is termed 'specific profiling' so as not to give the impression that it targets individuals only. The two forms of profiling can be treated to some extent as ideal types in terms of how they relate to each other. In practice, they often overlap: abstract profiles are frequently generated partly on the basis of specific profiling and *vice versa*.

The data from which profiles are generated can come from a variety of sources: they can be collected by the profiler directly from the data subject (eg, pursuant to a sales transaction) or from databases maintained by third parties. Some of the latter types of data can be generally available to the public (eg, data from land title registers) or they can be relatively confidential (eg, customer lists). Further, the data

---

1031 See Australian Privacy Commissioner, *Profiling and Privacy*, Information Paper 2 (Sydney: HREOC, 1995), 1; RA Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' (1993) 4 *J of Law and Information Science*, 403, 404; RA Clarke, 'Profiling and its privacy applications' (1994) 1 *PLPR*, 128.

1032 See RA Clarke, 'Customer profiling and Privacy Implications for the Finance Industry', May 1997, <http://www.anu.edu.au/people/Roger.Clarke/DV/CustProfFin.html>.

1033 *Id.*

used to generate a profile can come exclusively from the data holdings of the profiler; alternatively, they can come from the holdings of a multiplicity of organisations. The data can represent a mixture of (relatively objective) facts and (relatively subjective) opinions.

For the purposes of *abstract* profiling, none of the data used to build up the profile need be capable of revealing the identity of a specific individual person or organised collective entity; they can be, from the viewpoint of data protection laws, completely non-personal (as will often be the case with census data). *Specific* profiling can also build to some extent on such data, but will tend to require the existence of some data that are capable of being connected, directly or indirectly, to a particular person/collective entity. It cannot be taken for granted, though, that all of the latter data are personal from the viewpoint of data protection laws. The extent to which these data may be personal is an issue taken up in the next chapter (section 18.2). The issue is especially pertinent in an Internet context, given that profiles of Internet users can be built up merely on the basis of net-browsing patterns (registered as so-called 'clickstream' data and often stored, in part, as 'cookies')[1034] that are directly linked to the user's hardware and software as opposed to, say, the user's own name or PIN.

Profiling (both abstract and specific) can be used for a multitude of ends. Amongst the most common ends are the targeted marketing of goods and services. Profiling enables the identification (or localisation) of potential customers/clients for an organisation, and/or the identification of existing customers/clients who may be interested in other products from that organisation (or linked organisations).[1035] Profiling also enables development of more individualised/personalised marketing strategies.

Other common ends are the cost-effective provision of health care and insurance. For instance, profiling can enhance identification of persons who are likely to develop particular health disorders and/or of ways in which to cut health-care and insurance costs (eg, through application of a profile of the 'ideal cost-saving

---

1034 Typical constituents of clickstream data will include: the IP (Internet protocol) address and type of computer used; the type of operative system and browser program used; the type of language utilised by the browser program; a list (not necessarily complete) of other URLs visited; and a list (not necessarily complete) of the keywords typed into search-programs. See further, eg, G Greenleaf, 'Privacy and cyberspace – an ambiguous relationship' (1996) 3 *PLPR*, 88, 91–92; J Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50 *Stanford L Rev*, 1193, 1225ff. In essence, cookies are transactional data about a browser's Internet activity which are automatically stored by an Internet server on the browser's computer. The primary aim of cookies is to allow for the customising of an Internet service for the browser's subsequent use of the service or linked services. For description of the way cookies are generated and of the issues they raise for data protection laws, see, eg, V Mayer-Schönberger, 'The Internet and Privacy Legislation: Cookies for a Treat?' (1998) 14 *CLSR*, 166–174.

1035 For concrete examples, see Novek *et al*, *supra* n 363, espec 527–533; Australian Privacy Commissioner, *supra* n 1031, 8.

patient').[1036] Still other common ends are credit assessment, law enforcement and crime control. For instance, profiling can enhance identification of persons who are likely to default on their loan repayments,[1037] or persons who are likely to engage in criminal activity.[1038] Profiling can also be employed to detect and root out delinquent behaviour falling short of the latter activity.[1039]

Profiling need not be used only for ends that have a direct effect on data subject behaviour; it can be utilised for general planning purposes that affect data subjects only indirectly (as is frequently the case, eg, with a national census). Moreover, profilers will not always be interested in learning the names or other identifying characteristics of data subjects (as is often the case, eg, in epidemiological research). This might even be the case with respect to marketing: what a marketing company might want (and need) is not the name of the person/collective entity who/which is the object of the marketing (and the subject of the profile) but simply some reliable point (eg, a computer's IP address or an e-mail address) through which to make contact with that person/entity.[1040]

The purpose(s) served by a particular profiling operation will often differ from the purpose(s) for which the data forming the basis of the profile have originally been collected and/or further processed. In other words, profiling will often involve re-purposing of data.

As pointed out at the beginning of this section, profiling – both abstract and specific – is not a new phenomenon but an integral part of many inter-human relationships. What is new is the increasingly extensive, systematic use by organisations of relatively formalised and sophisticated profiling practices for a variety of control purposes. At the same time, caution must be exercised when attempting to delineate the extent of this development. There is a paucity of reliable empirical data providing a comprehensive overview of organisational profiling practices on national or sectoral bases.[1041] Consequently, analyses of the extent of such practices are often (to use the words of Clarke) 'developed predominantly by

---

1036 See further Simitis, *supra* n 19, 710–712, and examples cited therein. See also Vedder, *supra* n 1006, 216–219 (with respect to health insurance schemes).

1037 See further the cases referred to *infra* nn 1205–1206.

1038 For concrete examples, see GT Marx & N Reichman, 'Routinizing the Discovery of Secrets: Computers as Informants' (1985) 1 *Software LJ*, 95, 103–105; Madsen, *supra* n 46, 134–135.

1039 For examples involving the monitoring and shaping of children's behaviour, see J Bing, 'Data Protection and Social Policy', in *Beyond 1984: The Law and Information Technology in Tomorrow's Society*, Proceedings of the Fourteenth Colloquy on European Law held in Lisbon, 26–28 September 1984 (Strasbourg: CoE, 1985), 82, 91; Simitis, *supra* n 19, 713.

1040 See further Chapter 18 (section 18.2).

1041 This appears to be partly due to practical problems in collecting such data. One such problem is that organisations are frequently coy about their data-processing practices. See further the research experiences described by Clarke ('Profiling: A Hidden Challenge to the Regulation of Data Surveillance', *supra* n 1031, 404) and Gandy (*supra* n 381, 108ff).

reflection on technological capabilities, anecdotes and unofficial information, and through use of the limited secondary sources'.[1042]

With these cautionary remarks in mind, evidence exists, nevertheless, to indicate growth in the frequency and intensity of organisational profiling practices (both abstract and specific) in at least some fields, particularly marketing, crime control and insurance.[1043] Concomitantly, there appears to be growth in the scale of ambition of these practices as measured in the comprehensiveness of the profiles they aim to generate and apply.

A corollary of this growth is the development of profiling as an industry in itself. Enterprises are springing up which specialise in generating profiles to be traded on the burgeoning market in information services.[1044] This industry is making itself felt not just in the 'off-line' world but also in relation to the Internet.[1045] Complementing the industry is the tendency for organisations to diversify their operations, thereby expanding both their customer/client base and their interface with this base. Thus, we see an increasing degree of 'totalising' relationships between organisations and their customers/clients.[1046] Such relationships enhance customer/client transparency and the generation of more detailed customer/client profiles. Also important is the increased interest by organisations in tracking the preferences, desires, etc of their customers/clients and/or of potential customers/clients (eg, through the use of survey questionnaires and loyalty card schemes).

Further, the techniques for generating profiles are evermore sophisticated. Two inter-related techniques of note have emerged in recent years: data warehousing and data mining. Data warehousing is the process by which an organisation gathers data from disparate sources and loads these data into a central, integrated database for subsequent analysis and (re)use. Data mining is the process by which data (eg, those in the 'warehouse') are examined through the use of various algorithms in order to uncover latent data patterns, connections, sequences, etc that may be useful for the organisation.[1047] The efficacy of the latter process is now being enhanced through the

---

1042 Clarke, *ibid*.

1043 See, eg, the findings of the OTA study with respect to (abstract) profiling by US federal government agencies: OTA, *supra* n 1030, 89. More generally, see Gandy, *supra* n 381, espec 71–74.

1044 For examples, see *Der Spiegel*, 5.7.1999, 112ff; Madsen, *supra* n 46, 135–136; Novek *et al*, *supra* n 363, 526ff; Froomkin, *supra* n 373, Part IV.

1045 See, eg, R Runett, 'Hungry for Better Response Rates? Dial the Data Munchers', *The Digital Edge*, 1999, <http://www.digitaledge.org/monthly/1999_05/profiler.html> (describing several US-based companies that specialise in creating and supplying consumer profiles based on persons' behaviour on the Internet).

1046 Novek *et al* point to Sears, Roebuck & Company as 'a particularly important example of the multi-product firm which is beginning to combine data from its various lines of business into a massive marketing database': Novek *et al*, *supra* n 363, 527. There are numerous other examples of such firms.

1047 See generally the collection of articles in U Fayyad & R Uthurusamy (eds), 'Data Mining and Knowledge Discovery in Databases' (1996) 39 *Communications of the ACM*, no 11, 24–68. See also A Schweizer, *Data Mining, Data Warehousing: Datenschutzrechtliche Orientierungshilfen für*

use of artificial neural networks[1048] and intelligent agents.[1049] Part and parcel of the increasing sophistication of profiling techniques is their increasing automatisation. We see evidence of this particularly in cybermarketing practices. The advertising banners on Internet sites, for example, are frequently programmed to automatically adjust their content and/or format according to the net-browsing data about the site visitor which are stored as 'cookies' on the visitor's computer.[1050]

The catalysts for the above developments are to be found in the constellation of factors (technological-organisational, economic and ideological) accounting for the keenness of organisations' informational appetite generally and the pervasiveness of systems of mass surveillance and control – as outlined in Chapter 6 (sections 6.2.1–6.2.2). The very same constellation of factors makes it unlikely these developments will stop up, at least in the short term; if anything, they will probably intensify.

17.3 Profiling as Problem

This section examines problematic sides of the profiling practices of organisations in light of the developments outlined above. The basic aim here is to identify those aspects of profiling which justify current regulation of the practice pursuant to data protection laws and possibly a sharpening of such regulation.

A point of departure for this analysis is the catalogue of data protection interests set out in Chapter 7 (section 7.2.5). It will be recalled that this catalogue consists of two groups of interests. The first group embraces interests relating to the quality of (personal) information and information systems. The overarching interests in this

---

(Cont.)
Privatunternehmen (Zürich: Orell Füssli Verlag, 1999), chapts 1–2; Ontario, Information and Privacy Commissioner, *Data Mining: Staking a Claim on Your Privacy*, January 1998, <http://www.ipc.on.ca/english/pubpres/ sum_pap/papers/datamine.htm>. For a concrete example of the use of data mining to monitor employee behaviour, see *Computerworld Norge*, 28.4.1999, 5.

1048 In short, artificial neural networks are computer algorithms that attempt to simulate the analytical operations of the human brain. For further description, see, eg, JP Bigus, *Data Mining with Neural Networks: Solving Business Problems from Application Development to Decision Support* (New York: McGraw-Hill, 1996), espec chapts 2 and 4; KT Hubick, *Artificial Neural Networks in Australia* (Canberra: Department of Industry Technology and Commerce, 1992), espec 18ff.

1049 Intelligent agents are software applications that execute specific tasks – eg, data searches and filtering – for a computer user or computer system. For an introductory overview of the various kinds of such agents, see Bigus, *supra* n 1048, chapt 8. For analysis of the privacy risks posed by agent technologies, see JJ Borking, BMA van Eck & P Siepel, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector* (Registratiekamer: The Hague, 1999), chapter 4; LA Bygrave, 'Electronic Agents and Privacy: A Cyberspace Odyssey 2001' (2001) 9 *Int J of Law and Information Technology*, 275–294.

1050 See further US Federal Trade Commission, *Online Profiling: A Report to Congress*, June 2000, <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>, 3ff; Mayer-Schönberger, *supra* n 1034, 168–169.

group are summed up in terms of ensuring data validity and information utility together with the manageability, robustness, accessibility, reliability and comprehensibility of information systems. The second group comprises interests concerning the condition of persons (and collective entities) as data subjects and the quality of society generally. The overarching interests in this category are summed up in terms of ensuring privacy, autonomy, civility, democracy, pluralism, rule of law and balanced control.

Although the focus of this section is mainly on the problematic consequences of profiling for *data subjects*, care must be taken not to overlook the position of profilers and society generally nor to cast the interests of profilers as always in conflict with the interests of data subjects. Profilers, data subjects and society generally can suffer mutual detriment from the same profiling operation (eg, when the latter leads to mistaken suspicion of criminal or delinquent behaviour on the part of the data subject(s)). Conversely, profilers, data subjects and society generally can benefit mutually from the same profiling operation (as will sometimes be the case with targeted marketing), though the nature and extent of the mutual detriment or benefit will not necessarily be the same for each party. It is also possible for the one profiling operation to detract from some of the interests of all parties involved yet benefit other of their interests (as will usually be the case with targeted marketing). These points are revisited at the end of this section.

The nature of the pros and cons of profiling for data subjects (and for profilers and society generally) depends on a combination of factors:

1) the quality of the data and processes (technological-organisational, analytical-cognitive) from which profiles are generated;
2) the comprehensiveness of the profiles;
3) the degree of data subject awareness of the profiling practice; and
4) how and to what ends the profiles are applied.

The first-listed set of factors raises issues pertaining directly to the first group of data protection interests described in section 7.2.5 of Chapter 7; the remaining sets of factors raise issues pertaining directly to the second group of those interests.

Elaborating on the first-listed set of factors, it is clear the quality of a profile depends upon the validity of the data upon which the profile is based. Bigus underlines this point in his presentation of neural networks for data-mining purposes:

> 'If ever there was a system where GIGO was the rule (garbage in, garbage out), neural networks is it. They are highly forgiving of noisy and incomplete data, but they are only as good as the data they are trained with.'[1051]

1051 Bigus, *supra* n 1048, 58. At the same time, it should not be forgotten that profiling operations will have differing degrees of error tolerance, depending on the purposes for which they are used. It

The quality of a profile will be detrimentally affected not only by invalid data but also by valid data that are incomplete or irrelevant in relation to what the profile is intended to represent or the purposes it is supposed to serve. For instance, Marx and Reichman note:

> 'The data base used for constructing a profile may be reasonably accurate as far as it goes, but may not be representative of the larger universe of events. Important data may never enter the system. Thus it is sometimes argued that our knowledge of criminals is distorted because it is based primarily on those who get caught and they may be less competent than those who manage to avoid apprehension.'[1052]

As stated in the previous section, profiles are essentially assumptions based on probability equations. The mere fact they are the outcomes of probability equations means they tend to contain some margin of error.[1053] The extent of such error and, concomitantly, the extent to which the error might have detrimental consequences for the data subject will be influenced to a large degree by the cognitive qualities of the profiler. Are, for instance, the assumptions of the profiler based largely on intuitive hunches? How tainted are the assumptions by cultural, racial and/or gender bias? How high is the profiler's degree of inferential ambition? Generally speaking, the more inferentially ambitious the profile (ie, the higher the ratio between detail or scope of assumption and detail or scope of data from which the assumption is made), the greater is the chance of error entering into the profile. For example, assuming the ethnicity of a person merely on the basis of his/her surname is an instance of profiling with a relatively high degree of inferential ambition.

Abstract profiling arguably tends to involve a higher degree of such ambition than specific profiling. The former arguably will tend also to be more vulnerable than the latter to error brought about by cultural, racial and/or gender bias. Yet instances of specific profiling can be envisaged which are just as, if not more, problematic in these respects.

The extent of error in a profile will also be determined by a range of technological-organisational factors. These include all of the elements (set out in Chapter 7 (section 7.2.5)) making up the quality of the information system used to process the data concerned. Of particular importance will be the extent to which the profiler actively checks the various stages of the profiling operation for faults that could have detrimental consequences for the data subject.

(Cont.)
should also be remembered that the profiler's level of error tolerance could be different to the data subject's tolerance level. See further Chapter 7 (section 7.3).

1052 Marx & Reichman, *supra* n 1038, 112.

1053 Eg, as noted by the OTA, (abstract) profiles will tend to accentuate the similarities among a given population, and play down the differences: OTA, *supra* n 1030, 93.

In light of the above observations, together with the inadequacies with data/information quality and cognitive quality alluded to in Chapter 6 (section 6.2.3), a real danger exists of profiling operations resulting in unfair or unwarranted assessments of data subjects. This danger is accentuated by some of the technological-organisational tendencies identified in Chapter 6 (section 6.2.1) – notably, the increasing automatisation of organisational decision-making processes and, concomitantly, the diminishing role played by data subjects in influencing such processes.

To elaborate a little on the consequences of automatisation: following Bing, it seems reasonable to surmise that as profiling operations become increasingly automated, they will rely more and more on pre-collected, structured data held either by the profiler or a third party.[1054] Moreover, these data will tend to express relatively 'strict', easily quantifiable criteria that are *apparently* less ambiguous and less context-sensitive than their 'soft' counterparts.[1055] At the same time, use of such data for profiling might well generate a multiplicity of quality-related problems.[1056] Some of these problems could stem from the very nature of the data as described above; they might, for instance, omit or distort important aspects of 'the larger universe of events' (in the words of Marx and Reichman). Some of the problems could alternatively stem from the fact that, pursuant to the profiling process, the data will tend to be employed for new purposes to which they are not really suited; their coupling might, for example, lead to misrepresentations of fact because they have different underlying referents.

Moving to the factor of profile comprehensiveness, this determines the extent to which a data subject's privacy – more specifically, realisation of his/her/its interests in non-transparency and anonymity – will be diminished by a profiling operation. The amount of privacy a person/organisation enjoys *vis-à-vis* another person/organisation is partly a function of the degree to which the latter is able to draw together data on disparate aspects of the former's activities.[1057] The more such data are able to be drawn together, the more comprehensive is the profile that can be validly inferred from the data and the less privacy is enjoyed by the data subject (at least *vis-à-vis* the profiler). This diminishment of privacy can have detrimental effects on the realisation of additional interests of the data subject, such as the interest in identificational self-determination.[1058] Other autonomy-related interests might be

---

1054 See espec J Bing, 'Three Generations of Computerized Systems for Public Administration and Some Implications for Legal Decision-Making' (1990) 3 *Ratio Juris*, 219, 233. Bing's analysis focuses on the decision-making processes of government agencies but, for present purposes, it is also pertinent to organisational decision making more generally.

1055 *Ibid*, 227ff.

1056 As Bing himself indicates: *ibid*, 232.

1057 Thus, Paul Müller defines 'Privatsphäre' as 'Aufrechterhaltung der unterschiedlichen Bilder, die über [einen Person] … bei anderen Personen und bei Institutionen existieren': PJ Müller, 'Funktion des Datenschutzes aus soziologischer Sicht' (1974) 5 *DVR*, 107.

1058 See also *Botschaft*, *supra* n 680, 35.

detrimentally affected as well.[1059] There might also be negative consequences at a macro-level for realising the interests in pluralism and democracy.

The problems identified above with respect to profile comprehensiveness arise most directly in relation to specific profiling. Yet these problems can also arise as a result of abstract profiling – depending on the validity of the assumption(s) made about the group in focus, the extent to which these assumptions are communicated to the group members and the ways in which the assumptions are otherwise acted upon.[1060]

As for the factors concerning data subject awareness of profiling practices, these impact directly upon the interests in predictability and insight (as described in Chapter 7 (section 7.2.5)). Deficits in insight and predictability can detract in turn from realisation of other data protection interests, such as autonomy, civility, pluralism and democracy. The most important point to note is that profiling techniques tend not to be intrinsically visible processes *vis-à-vis* data subjects. Even if some of these processes occur with the knowledge of the data subjects, other aspects might not. For example, while the collection of data and their application for profiling purposes might occur overtly, data subjects might not be aware of the logic or reasoning that steers the profiling operation.

> 'In short: when they [data subjects] are affected by the use of group profiles, they will experience the consequences, but they will often not be aware of what exactly causes these phenomena.'[1061]

Contributing to this deficit in awareness is the fact that a great deal of profiling tends to involve substantial re-purposing of data.

The final set of factors concerns the use made of the results of profiling. These factors have the obvious potential to impinge upon the bulk of the second group of data protection interests set out in section 7.2.5 of Chapter 7. Profiling can be used to extend and tighten control over data subjects, directly or indirectly, thereby undermining realisation of their interests in autonomy and privacy. More specifically, profiling can increase the possibility that data subjects are subjected to unwanted contact or attempts at contact by others, thus undermining realisation of their interests in non-interference, non-information, inflow control, attentional self-determination and, in some cases, civility. When utilised as an instrument for mass surveillance and control, profiling can also undermine realisation of the interests in

---

1059 Refer, for instance, to the effects of panopticism, as outlined in Chapter 6 (section 6.3.1).

1060 See also Chapter 15 (section 15.3).

1061 Vedder, *supra* n 1006, 223. See also Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance', *supra* n 1031, 411 ('Profiling appears to be being conducted … by many … agencies and corporations outside the purview, and largely without the knowledge, of the public, its Parliamentary representatives or any statutory watchdog').

plurality, democracy, civility and/or balanced control.[1062] Realisation of other interests that do not figure explicitly in the interest catalogue set out in Chapter 7 can be detrimentally affected as well.[1063]

The above possibilities manifest themselves not just in the context of investigation and prevention of crime or other delinquent behaviour, but also in a commercial/marketing context. Novek *et al*, for instance, highlight the way in which profiling opens up for various types of consumer discrimination: 'profiles ... allow companies to pre-judge the future behavior of consumers, leading some of these firms to ignore certain types of people, and thereby limiting such persons' access to information about goods and services'.[1064] Such discrimination need not always be illegitimate or unfair but it can be.[1065]

Profiling can also reinforce a tendency to regard persons as mere objects, thereby violating their integrity and dignity.[1066] Indeed, a profile can be used in such a way that it effectively usurps the constitutive authority of the data subject; ie, the profile becomes more 'real' than the latter. In crime investigation, this possibility can manifest itself in presumptions of data subject guilt and corresponding alterations in the burden of proving innocence. As the Australian Privacy Commissioner points out,

> '[w]here profiles are used to identify individuals engaging in fraudulent or other illegal activity there is a risk that the mere fact an individual fits a profile may be seen as evidence of guilt.'[1067]

This presumption of guilt can influence the way in which follow-up investigations are undertaken of individuals who appear to fit the profile in question.[1068] Yet even in

---

1062 See further Clarke, *ibid*, 409ff; and, more generally, RA Clarke, 'Information Technology and Dataveillance', in D Dunlop & R Kling (eds), *Computerization and Controversy: Value Conflicts and Social Choices* (San Diego: Academic Press, 1991), 496–522 (originally published in (1989) 31 *Communications of the ACM*, 498–512).

1063 Eg, profiling directed at employees of a country's defence force can create problems for national security: increased transparency of the financial and/or other affairs of such persons makes for increased vulnerability of those persons to threats from foreign forces. See, eg, interview with staff at the Norwegian Defence Force Headquarters, reported in *Computerworld Norge*, 24.4.1998, no 16, 2.

1064 Novek *et al*, *supra* n 363, 533.

1065 For example, Novek *et al* point to the dangers of 'electronic redlining', a situation 'where calls from low-income neighbourhoods identified by their telephone exchange, can be routed to a busy signal, a long queue, or a recorded message suggesting that the desired information service is not presently available': *ibid*, 535. Note too the online practice of 'weblining': see *infra* n 1096 and accompanying text.

1066 See generally Bråten, *supra* n 349, 54, 60.

1067 Australian Privacy Commissioner, *supra* n 1031, 11.

1068 On this point, see the evidence cited by the Australian Privacy Commissioner from a 1993 study on the auditing practices of the Australian Taxation Office (ATO). The study found that the procedures used by ATO auditors to select particular taxpayers for closer investigation 'were contributing to the

the context of other administrative procedures, profiling (especially abstract profiling) can create a biased approach to case handling which breaks with basic assumptions and requirements of impartiality – the ideal that a case handler should approach the facts of a case with an open mind.

The focus of this section notwithstanding, profiling can be used in ways that *enhance* some of the data protection interests set out in Chapter 7 and/or mitigate some of the above-mentioned problems. For example, targeted marketing carried out on the basis of profiling can have a positive impact on consumer privacy and autonomy – more specifically, the interests in non-interference, non-information, inflow control and attentional self-determination – inasmuch as it narrows the number of consumers who receive advertising. Similarly, the use of profiling techniques for the purposes of fraud control will not be as intrusive as control methods based on random selection, insofar as it cuts back on the possibility of innocent persons being subject to investigation. Additionally, profiling need not result in feelings of disrespect or alienation on the part of data subjects. Profiling can lead to more insight into a person's character. This insight can make it more difficult for the profiler to treat that person as a mere object. Concomitantly, profiling can be used to develop a personalised, 'soft-touch' approach to data subjects which is experienced by the latter as non-alienating. Moreover, profiling can have beneficial effects for other interests of data subjects (eg, when used to identify persons who are not receiving benefits or utilising rights to which they are entitled).

Of course, the extent to which such advantages are realised will hinge on the validity of the particular profile developed. This highlights again the importance of controlling the quality of profile generation and use.

At the same time, in assessing the extent to which profiling should be legally regulated, the beneficial potential of profiling for data subjects must be balanced against the problematic aspects of profiling identified above. Another factor to be weighed in this assessment is the beneficial potential of profiling for profilers (eg, in terms of more cost-effective operations) and for society generally (eg, in terms of reducing crime, disease, etc).

(Cont.)
development of a belief amongst auditors that cases chosen by case selection staff should automatically return revenue to the Commonwealth': *ibid*, 12.

18. Regulation of Profiling

18.1 Introduction

This chapter analyses the central ways in which data protection laws are able to regulate certain kinds of profiling, more specifically the relatively formalised and systematic profiling practices initiated by organisations for a variety of control purposes. The fundamental issue at point is the extent to which this regulatory capability can mitigate the problems identified in the previous chapter (section 17.3) which these practices might have for data subjects. The analysis focuses upon the applicability of the core principles of data protection laws to such practices and upon the logical/conceptual efficacy of these principles in regulating the practices. It is also hoped that such analysis will go a significant way to elaborating the general content of what are often vaguely formulated principles and rules.

The first question considered is the degree to which the above types of profiling (hereinafter termed simply 'profiling' or 'profiling practices') fall within the ambit of data protection laws (see section 18.2). This question boils down to whether or not a given profiling practice involves the processing of *personal* data. Therafter, an examination is made of rules in data protection laws which *expressly* regulate profiling practices (see section 18.3). This is followed by analysis of the main rules that regulate such practices *indirectly* (see section 18.4).

The primary legal point of departure for discussion in the chapter is the EC Directive. This is due to the Directive's relatively high degree of normative influence.[1069] Some account is taken also of the relevant regulatory capabilities of older data protection laws (particularly Norway's PDRA) together with more recent laws that explicitly address profiling practices.

It is important to keep in mind that profiling will be constrained by a variety of laws and rules other than data protection legislation. For example, rules on duty of confidence will tend to restrict the ability to generate profiles. As for profile application, this will tend to be limited by, ia, natural justice doctrines in administrative law and by legislation prohibiting racial, sexual or religious discrimination. Constitutional protections of citizen privacy and autonomy can also play an important role.[1070] Additionally, there exist a wide range of non-legal

---

1069 See especially Chapter 2 (section 2.2).

1070 See, eg, the extensive case law developed by the US Supreme Court (pursuant to the Fourth Amendment in the US Constitution) on the constitutionality of police detainment of persons on the

constraints on profiling practices.[1071] However, analysis of such constraints and of laws and rules outside data protection legislation is not undertaken in this chapter.

The chapter also passes over several problem areas that impinge on the ability of data protection laws to regulate profiling practices. These problem areas concern the regulation of transborder data flows, issues of jurisdiction and choice of laws, and issues concerning the availability and nature of legal sanctions. In other words, the chapter does not attempt to undertake an exhaustive analysis of the regulatory capabilities of data protection laws with respect to profiling. Rather, it seeks to delineate the strengths and weaknesses of the laws' core principles in the light of the material presented in Chapter 17.

18.2 The Concept of Personal Data Revisited – Particularly in Light of Internet Profiling

The creation and use of profiles may be regulated by data protection laws usually only insofar as *personal* data are processed. Thus, consideration of the applicability of these laws to profiling practices requires a closer analysis of what the laws mean by 'personal data'. In the following, discussion of this issue focuses upon Internet-based profiling practices as it is in such a context that the issue is likely to have a great deal of practical significance. Nevertheless, much of the logic of the discussion will be applicable to profiling practices in non-Internet contexts.

As indicated in the previous chapter (section 17.2), profiling can be based on a variety of data that are difficult if not impossible to classify as personal pursuant to these laws. Such data will typically be data linked to large collective entities (especially non-organised ones). Such data will also be data linked to machines and other non-human objects. Profiling processes employing only these sorts of data are able to elude regulation pursuant to most data protection laws unless the data can be linked to a specific individual. The possibility of such linkage with respect to data on collective entities is analysed in Chapter 10 (section 10.3). In the following, therefore, focus is directed at the possibility of such linkage with respect to what are *prima facie* machine data. More specifically, focus is directed at linkage possibilities with respect to clickstream data connected *prima facie* to a computer address.[1072] As noted in the previous chapter, a great deal of profiling of Internet users is able to occur purely on the basis of registration and analysis of such data.

(Cont.)
basis of their fitting a drug courier profile. Leading cases include *United States v Mendenhall*, 446 US 544 (1980); *Florida v Royer*, 460 US 491 (1983); *United States v Sokolov*, 490 US 1 (1989).

1071 For an overview, see Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance', *supra* n 1031, 412ff.

1072 For a short explanation of what is meant by 'clickstream data', see *supra* n 1034.

Chapter 2 (section 2.4.1) shows that the concept of personal data is usually defined by data protection laws in a broad and flexible manner. The focus of the definitions tends to be on the potential of data to enable identification, directly or indirectly, of a single natural/physical person (or sometimes a single organisation). The allowance for *indirect* identification means that data may be personal even if they permit a person to be identified only in combination with other (auxiliary) data. The definition of 'personal data' in Art 2(a) of the EC Directive bears repeating here:

> 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'

The reference to 'identification number' in the above definition is potentially broad. Nothing in the Directive or its *travaux préparatoires* expressly indicates that such a number must refer directly to a natural person. Hence, a computer's IP number could qualify as such a number. Moreover, it is arguable that at least some other types of clickstream data (eg, domain names, URLs visited, keywords used in search programs) have the potential to qualify as 'factors specific to … [the Internet user's] mental, economic, cultural or social identity'. Yet the mere fact that clickstream data may be encompassed by elements of the above definition does not mean that such data are 'personal' for the purposes of the Directive (or other data protection laws).[1073]

Recital 26 in the Directive's preamble indicates that data will only be personal if they can facilitate identification of a single person by means that are reasonably capable of being utilised by another person.[1074] However, the Directive refrains from elaborating on further criteria for determining whether such facilitation is possible. Nevertheless, little doubt exists that one criterion is the probability of identification.

1073 Cf the Data Protection Working Party which appears to take for granted that most if not all clickstream data are personal for the purposes of the Directive: see 'Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware', Recomendation 1/99 adopted 23.2.1999, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm>. By contrast, Reidenberg and Schwartz correctly observe that '[f]or on-line services, the determination of whether particular information relates to an 'identifiable person' is unlikely to be straightforward': JR Reidenberg & PM Schwartz, *Data Protection Law and On-Line Services: Regulatory Responses*, study conducted for Directorate General XV of the EC Commission, December 1998, <http://europa.eu.int/comm/ internal_market/en/dataprot/studies/regul.htm>, 23. The latter study reveals considerable uncertainty, contradiction and diversity in Belgian, French, German and UK approaches (prior to national transposition of the EC Directive) to the issue of what constitutes 'personal data' for the purposes of applying data protection laws to the on-line environment.

1074 See further Chapter 2 (section 2.4.1).

Related criteria are the degree of technical ease with which identification can occur, together with the amount of time and effort demanded by the identification process.

Accordingly, the extent to which clickstream data may amount to personal data under the Directive is a question of fact that is impossible to answer conclusively in the abstract. Further, any answer will have to be continually revised in light of technological-organisational developments; data which presently could only be linked to an individual with great difficulty might be linked relatively easily in the near future.

In the event of there existing a readily accessible directory listing one particular person against one particular IP address, there will be a relatively high chance of that address (and the other clickstream data registered against that address) constituting personal data.[1075] The chance will be lessened in cases where the Internet service provider issues a temporary address and fails to keep a record of which user name has been registered against that address.[1076]

The possibility of a multiplicity of persons sharing a machine with an address registered in the name of only one person is unlikely to disqualify that machine address from being treated as personal data. Many numbers (eg, car registration and telephone numbers) which are formally registered against the name of one specific person tend to be treated as personal data even if the objects to which they directly attach are occasionally or regularly used by other persons.[1077] In Sweden, though, it was held on two occasions that telephone numbers did not constitute personal data pursuant to the *Data Act* of 1973 (repealed),[1078] precisely because of the possibility of the telephones being used by a multiplicity of persons.[1079] However, these decisions

---

1075 See also Greenleaf, *supra* n 1034, 114–115; Bygrave & Koelman, *supra* n 316, 73.

1076 A temporary address (often also called a 'dynamic' address) will usually last only for the length of the period in which the machine of the Internet user is connected to the net. New/different addresses will be issued for each subsequent period of Internet connection.

1077 See, eg, the study by Reidenberg & Schwartz, *supra* n 1073.

1078 The concept of 'personal data' ('personuppgift') was defined in s 1 of that Act as 'information concerning an individual' ('upplysning som avser enskild person').

1079 See the decision of 29.5.1975 by the government in case 3029-74, and the decision of 27.11.1997 by the Stockholm City Court (Länsrätten) in case Ö 14897-97. The first case concerned use of a telephone-debiting register for distributing telephone charges within the Volvo corporation. Approximately half of the telephone lines in question were each at the official disposal of single employees; the other half were each at the disposal of two or more employees. The Data Inspection Board held that at least the debiting data linked to those lines at the disposal of single employees constituted personal data. On appeal, the government determined that even these data were not personal as no guarantee existed that the telephone lines in question would only be used by the same single employees. The second case dealt with plans by a Stockholm taxi company to establish a register containing telephone numbers and street addresses for the Stockholm area but no other data types (such as names of persons). The Stockholm City Court held that the planned register did not contain personal data for the same reasons cited by the government in the former case.

appear out of line with the bulk of opinion in data protection discourse and have little relevance for construing the provisions of the EC Directive.[1080]

At the same time, the chance of an IP address (and other clickstream data registered against that address) constituting personal data will be diminished if a multiplicity of persons are *registered* against the address. This outcome might change, though, in cases where only a very small number of persons are registered. The question then is: how small? For the purposes of the Directive, setting down a fixed number is neither possible nor desirable. This notwithstanding, there can be little doubt that the registration of just two persons against an address will be insufficient to deprive the data of the possibility of being classified as personal.[1081] The same might also apply with respect to registration of a family, household or small business.

It is instructive to ponder over a situation in which an IP address is registered against the name of an institution (eg, a university or university department) and is capable of being (legally) used by a fairly large number of persons. It is extremely unlikely the address (and other clickstream data linked to it) could be judged as 'personal'. However, a different conclusion could (and should) be reached if use of the machine (to which the address is attached) is preconditioned by use of a password for each individual member of the institution *and* there are readily available means of linking the clickstream data to a period in which one password is active. A different conclusion could (and should) also be reached if the machine is located in an area (eg, office) to which only one or two persons have authorised access.

Finally, it will be recalled that the definition of 'personal data' in the EC Directive is in terms of the *capability* of identification: this means that even if a data controller does not exploit such a capability (eg, by stating he/she/it will refrain from trying to link an IP address to the name of the person registered against that address), the IP address data could still be 'personal' and the processing of these data thereby subject to the rules of the Directive. This point is particularly relevant to a situation in

---

1080 See, eg, COM(92) 422 final – SYN 287, 15.10.1992, 9: 'A person may be identified directly by name or indirectly by a *telephone number*, a *car registration number*, a *social security number*, a *passport number* or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc)' (emphasis added). See also para 19 of the Explanatory Memorandum to CoE *Recommendation R (95) 4 on the Protection of Personal Data in the Area of Telecommunications Services, with Particular Reference to Telephone Services* (adopted 7.2.1995) which stipulates that a telephone number is personal data for the purposes of the Recommendation. Note too the *travaux préparatoires* to Sweden's *Personal Data Act* of 1998 which at least entertain the possibility of IP addresses ('nätnodsadresser och liknande 'elektroniska identiteter'') being personal data: see SOU 1997:39, 338. The *Personal Data Act* defines 'personal data' in much the same way as the Directive does; ie, as 'all types of information that directly or indirectly can be linked to a live, physical person' ('all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet': s 3). Cf the possibly narrower definition of 'personal data' in the *Data Act* of 1973, *supra* n 1078.

1081 In some jurisdictions, such as France, a considerably higher number of persons could well be judged as insufficient too: see Reidenberg & Schwartz, *supra* n 1073, espec 32–33.

which a cybermarketing company sends advertisements to an IP address only (in the light of a profile based on the Internet-browsing patterns registered against that address), but the company expressly refrains from attempting to find out who is behind the address.

18.3 Express Regulation of Profiling

This section canvasses rules in data protection laws which expressly regulate profiling practices. The rules presented here are not the only such rules,[1082] but constitute those that are most likely to exercise a considerable influence on future regulatory initiatives.

18.3.1 EC DIRECTIVE

The EC Directive contains one provision (Art 15) dealing directly with profiling practices. Article 15(1) reads as follows:

> 'Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'

This provision restricts a particular *application* of a particular type of profiling process. It does not directly restrict the *creation* of profiles.

The operation of the right contained in Art 15(1) is closely connected with several other provisions in the Directive – primarily, Arts 15(2), 14 and 12(a). The latter two of these provisions are canvassed in section 18.4.5 while the former is dealt with at the end of this section.

Currently, provisions along the lines of Art 15(1) are fairly new amongst data protection instruments at both national and international levels. While their roots in data protection law go back to the late 1970s – more specifically to s 2 of the French data protection legislation enacted in 1978[1083] – less than a handful of countries had

---

1082 For instance, rules dealing specifically with credit-reporting activities can also be said to regulate profiling in a fairly direct manner. Several instances of these rules and their application are presented in section 18.4.7.

1083 Section 2 stipulates: 'No judicial decision involving an appraisal of human conduct may be based on any automatic processing of data which describes the profile or personality of the citizen concerned. No governmental or private decision involving an appraisal of human conduct may be based solely on

incorporated such provisions in their data protection laws *prior* to the EC Directive being adopted.[1084] This situation, of course, will soon change, mainly – though not exclusively[1085] – as a result of the Directive.

The fact that the Directive does not contain provisions specifically addressing the *creation* of profiles is far from unique.[1086] The vast majority of data protection laws also lack such provisions. Two exceptions to this pattern are Germany's federal *Teleservices Data Protection Act* and Switzerland's federal *Data Protection Act*. The relevant provisions of these Acts are described in the following sections.

For the right contained in Art 15(1) to apply, four cumulative conditions must be satisfied:

1) a decision must be made;
2) the decision concerned must have legal or otherwise significant effects on the person whom the decision targets;
3) the decision must be based solely on automated data processing;
4) the data processed must be intended to evaluate certain personal aspects of the person who is targeted by the decision.

A considerable amount of ambiguity inheres in these conditions. This ambiguity is scarcely mitigated by the Directive's recitals or *travaux préparatoires*.

(Cont.)
any automatic processing of data which describes the profile or personality of the citizen concerned'. See also s 3 set out below in section 18.4.5.

1084 In addition to s 2 of the French Act, see Art 12 of the first Spanish data protection law (*Organic Law 5/1992 of 29.10.1992 on the Regulation of the Automatic Processing of Personal Data* (*Ley organica 5/1992 de 29 de octubre 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*; replaced and repealed by Organic Law 15/1999 of 13.12.1999) and Art 16 of the first Portuguese data protection law (*Act no 10/91 of 12.4.1991 for the Protection of Personal Data with Regard to Automatic Processing* (*Lei no 10/91 de 12 de Abril 1991, da Proteccão de Dados Pessoais face à Informática*); replaced and repealed by Act no 67/98 of 26.10.1998).

1085 Other (also non-legal) instruments could play a role here too. For instance, the ILO Code of Practice on Protection of Workers' Data (ILO, *supra* n 74) contains several principles restricting the use of fully automated decision making in the assessment of worker conduct. See here principles 5.5 ('Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data'), 5.6 ('Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance'), 6.10 ('Polygraphs, truth-verification equipment or any other similar testing procedure should not be used') and 6.11 ('Personality tests or similar testing procedures should be consistent with the provisions of this code, provided that the worker may object to the processing').

1086 Note that the original proposal for the EC Directive on telecommunications privacy contained a provision (Art 4(2)) dealing specifically with the creation of electronic subscriber profiles but the provision was deleted from later drafts 'in order to take account of the principle of subsidiarity': see COM(94) 128 final-COD 288, 13.6.1994, 8. The provision read as follows: 'The telecommunications organization shall not use such data [ie, personal data on subscribers] to set up electronic profiles of the subscribers or classifications of individual subscribers by category'.

Regarding condition 1, neither the Directive nor its *travaux préparatoires* specifically address what is required for a decision to be made. Nevertheless, it is fairly obvious that making a decision about an individual person ordinarily involves the adoption of a particular attitude, opinion or stance towards that person. Such an attitude/stance can be of numerous kinds. For example, it can require the person to act or refrain from acting in a certain way. Or it can involve acceding to or denying a particular request from the person. Alternatively, it can result in action being taken to influence the person with or without his/her knowledge.

Difficulties could sometimes arise in distinguishing decisions from other processes (eg, plans, suggestions, advice, mapping of options) that can prepare the way for, or head off, formal decision making.[1087] At the same time, Art 15(1) does not operate with any *prima facie* requirement that a decision be of a certain form. Further, the notion of decision in Art 15(1) is undoubtedly to be construed broadly and somewhat loosely in light of the provision's rationale and its otherwise detailed qualification of the type of decision it embraces. Thus, the mere fact that a process is formally labelled or perceived as a plan or an advice would not be sufficient in itself to bring the process outside the ambit of Art 15(1). Nevertheless, if a decision is to be caught by Art 15(1), it must have some degree of binding effect on its maker (such that the latter is likely to act upon it). This follows partly from the very concept of a decision and partly from the requirement that the decision must have legal or otherwise significant effects on the person whom the decision targets (see condition 2 below).

Some uncertainty as to whether a decision is made could pertain to situations in which a human decision maker is apparently absent; ie, when the process at hand consists of a response on the part of computer software (eg, an intelligent agent) to particular constellations of data and data input. This issue is actualised by certain profiling practices in the context of cybermarketing. For instance, when advertising banners on Internet websites are programmed to adjust automatically their content and/or format according to net-browsing data about the site visitor[1088], does such adjustment involve a decision being made?

In support of a negative answer, it could be argued that the term 'decision' ordinarily connotes a *mental* action (the adoption of a particular *opinion* or *belief*). An affirmative answer, though, has stronger foundations. On the one hand, it can be plausibly argued that the term 'decision' should be construed broadly for the reasons set out above. In light of this, the logical processes of computer software would seem to parallel sufficiently the processes of the human mind to justify treating the former as analogous to the latter for the purposes of Art 15(1). On the other hand, it can be

---

1087 For elaborations of these difficulties in the field of Norwegian public administrative law, see, eg, Eckhoff & Smith, *supra* n 36, 403–404; G Woxholth, *Forvaltningsloven med kommentarer* (Oslo: Juridisk Forlag, 1993, 2nd ed), 31; A Frihagen, *Forvaltningsrett* (Oslo: Frihagen, 1991), vol 1, espec 282ff.

1088 See, eg, US Federal Trade Commission, *supra* n 1050.

plausibly argued that a human decision maker will still exist even if he/she is not directly involved in the process concerned. That decision maker will be the person who is responsible for programming the software.[1089]

Regarding condition 2, it is relatively clear what 'legal effects' involve. These are effects that are able to alter or determine (in part or in full) a person's legal rights or duties. Ambiguity with respect to condition 2 inheres mainly in the notion of 'significantly'. Does the notion refer only to effects that are significant for the data subject in an objective sense (ie, relatively independent of the data subject's own perceptions)? Does it refer only to effects of a material (eg, economic) nature? Does it require the decision concerned to be *adverse* to the interests of the data subject?

Given the thrust of recitals 9 and 10,[1090] together with an apparent intention on the part of the drafters of the Directive to allow recovery for both material and immaterial losses pursuant to Art 23,[1091] it is doubtful that 'significantly' refers exclusively to material effects. Arguably, therefore, a significant effect might lie merely in the insult to a data subject's dignity which is occasioned by the simple fact of being judged by a machine, at least in certain circumstances (eg, when there is no reasonable expectation of, or reasonable justification for, the sort of decision making described in Art 15(1)).

Moreover, if we accept that an important part of the rationale for the right in Art 15(1) is protection of human integrity and dignity in the face of an increasingly automated and inhuman(e) world,[1092] some consideration must be given to how the data subject perceives the effect(s) of the decision concerned. Nevertheless, the criterion of 'significantly' also has objective (inter-subjective) connotations. Thus, a data subject's perception of what constitutes a significant effect on him/her is very unlikely to be wholly determinative of the issue; the legal weight of the perception will depend on the extent to which it is regarded by a considerable number of other persons as having a reasonable basis.

Safeguarding the interests of the data subject requires that assessment of what is a significant effect is not based solely on the data subject's own reactions. Consider, for example, a situation in which a person who is considering whether to apply for a bank loan interacts with a fully automated loans assessment service offered by a bank. As a result of this interaction, the person is informed that he/she qualifies for a loan of a certain sum under certain conditions. The terms of this assessment could be viewed by the person as favourable yet fail to give an objectively accurate depiction of how much and under what conditions the person would be able to loan because,

---

1089 While this argument is highly plausible for computer software processes today, we should not overlook the future possibility of intelligent agents becoming so autonomous in their actions and learning capabilities that it is *logically* difficult to link their behaviour with any particular human(s). Even in such a situation, though, we could probably still find humans to whom the decisions could *legally* be linked.

1090 Set out *supra* n 135.

1091 See Chapter 4 (section 4.2).

1092 A line argued in Bygrave & Berg, *supra* n 576, 25 & 32.

for instance, the programme steering the assessment does not take into account certain details about the person's life situation. Indeed, were the latter details taken into account, the person would qualify for a higher loan with more favourable repayment conditions (for him/her). In such a situation, the data subject might well experience the assessment decision as unproblematic despite its objective faults. Paradoxically, however, this sort of situation could fall outside the scope of Art 15(1) on account of the provisions in Art 15(2), which are described further below.

As for the issue of whether the criterion of 'significant(ly)' requires the decision concerned to be *adverse* to the interests of the data subject, an earlier draft of the Directive expressly limited the right in Art 15(1) to such decisions.[1093] However, this fact alone does not mean we should read the same limitation into the final version of Art 15(1). Indeed, the very fact that the term 'adversely' has been dropped from Art 15(1) might suggest an intention not to limit the scope of the right in such a way. Still, it is extremely doubtful that Art 15(1) may apply when a decision has purely beneficial effects for the data subject. This follows partly from Art 15(2), described further below. At the same time, there exists a large amount of conceptual (and practical) overlap between the notions of 'significantly' and 'adversely'. This overlap notwithstanding, the criteria cannot be read as fully commensurate with each other. Some adverse effects can be too trivial to be 'significant'. In other words, the fact that a decision has adverse effects is merely a necessary but not sufficient condition for finding that the decision has significant effects. Thus, what is required is a decision that is *significantly adverse* in its consequences.

On the latter point, the EC Commission seems to have been of the opinion that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect the persons for the purposes of Art 15(1).[1094] Also other commentators view advertising (or at least certain forms of advertising) as too trivial to be significant.[1095] Nevertheless, some forms of advertising have at least a potential to significantly affect their targets. For instance, a cybermarketing process could

---

1093 The version of the right as set down in the 1992 Amended Proposal for the Directive read: 'Member States shall grant the right to every person not to be subjected to an administrative or private decision *adversely* affecting him which is based solely on automatic processing defining a personality profile' (Art 16(1); emphasis added). See also the commentary on this provision in COM(92) 422 final – SYN 287, 15.10.1992, 26–27: 'The person must be subject to an adverse decision. The decision must be one which can be invoked against him, one which has consequences for him; thus the simple fact of sending a commercial brochure to a list of persons selected by computer is not a decision adversely affecting them for these purposes. […] Thus the use of scoring techniques with a view to the lending of money to an individual is possible, if positive decisions to lend are based solely on an automatic assessment of risks; but where the score is negative the legitimate interests of the data subject must be safeguarded, for example by deferring a final answer until the organisation has been able to carry out a 'flesh and blood' study of the case.'

1094 *Ibid*. It should not be forgotten, though, that the Commission's opinion relates to a draft provision expressly requiring an *adverse* effect.

1095 See, eg, U Damman & S Simitis, *EG-Datenschutzrichtlinie: Kommentar* (Baden-Baden: Nomos, 1997), 220.

plausibly be said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of 'weblining' (eg, the person visiting the website is offered products or services at a higher price than other, assumedly more valuable consumers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others).[1096]

There can be little doubt that a decision may have a significant effect on the data subject even if it does not result in a manifest/positive alteration of his/her situation *vis-à-vis* other persons. In other words, Art 15(1) may apply even if the decision concerned is used to *refrain* from changing the *status quo* (eg, psychometric testing of job applicants results in none of them being offered jobs).

Moving to condition 3 (ie, the decision is based solely on automated data processing), the main problem here is to determine the proper meaning of the criterion 'solely'. If the criterion is read very strictly, one could argue that few, if any, decisions are or can be wholly the result of automated processes because the programmes steering these processes are initially created by human beings.[1097] Yet such an argument deprives Art 15(1) of any practical effect. Thus, it is necessary to operate with a relative notion of 'solely'. What the notion seems intended to denote is a situation in which a person fails to *actively* exercise any *real* influence on the outcome of a particular decision-making process. Such a situation would exist if a decision, though formally ascribed to a person, originates from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalised as a decision.[1098]

At the same time, it is important to note that if a data subject successfully exercises his/her right to object pursuant to Art 15(1), the data controller is simply required to review critically the criteria or factors forming the basis for the fully automated decision. The controller is not required to change these criteria or factors, nor to supplement them with other criteria/factors. Nevertheless, the review process might well involve these sorts of amendments being made.

Such a review process will be partly facilitated by the data subject's right under Art 12(a) to knowledge of the logic behind decisions of the kind embraced by

---

1096 Further on weblining, see M Stepanek, 'Weblining: Companies are using your personal data to limit your choices – and force you to pay more for products', *Business Week Online*, 3.4.2000, <http://www.businessweek.com/2000/00_14/b3675027.htm>; US Federal Trade Commission, *supra* n 1050, 13.

1097 An argument also broached in D Korff, 'The Effects of the EC Draft Directive on Business', in J Dumortier (ed), *Recent Developments in Data Privacy Law* (Leuven: Leuven University Press, 1992), 43, 50.

1098 See also COM(92) 422 final – SYN 287, 15.10.1992, 26: 'what is prohibited is the strict application by the user [data controller] of the results produced by the system. Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgement must have its place. It would be contrary to this principle, for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality'.

Art 15(1). The existence of this right means, in effect, that decision makers themselves must be able to comprehend the logic of the automated steps involved. This further means, in effect, that the logic be documented and that the documentation be kept readily available for consultation and communication (both inside and outside the decision maker's organisation).[1099] The documentation must set out, at the very least, the data categories which are applied, together with information about the role these categories play in the decision(s) concerned.

As for condition 4 (ie, the data processed are intended to evaluate 'certain personal aspects' of the data subject), this does not necessitate, on its face, the construction of a formalised profile of the data subject.[1100] In practice, however, the use of profiling techniques and the creation of some sort of personality profile will be required, though the profile need not be formalised as such. It would seem that Art 15(1) indirectly covers some use of abstract profiles, as the term 'data' is not directly qualified by the adjective 'personal'. Ultimately, though, the decision to which a person may object must be based on a profile of that person (ie, a specific profile). At the same time, there is no requirement that the profile casts the person in a particular (positive or negative) light.

The chief point of uncertainty with condition 4 is the scope of the phrase 'certain personal aspects'. There is little doubt that the phrase 'personal aspects' refers to aspects of the data subject's person or personality.[1101] There is also little doubt that inclusion of the word 'certain' means that not all 'personal aspects' are legally relevant for the application of Art 15(1). The question arises as to where and how the line is to be drawn between legally relevant 'personal aspects' and those aspects that are not legally relevant. Some aid is provided by the non-exhaustive exemplification in Art 15(1) itself ('work performance', 'creditworthiness', 'reliability' and 'conduct'). It indicates that legally relevant 'personal aspects' must relate to a person's abilities, behaviour, preferences or needs; ie, they must concern a person's *character*. They must concomitantly have a degree of complexity.[1102] Thus, quantitative data on purely physiological traits (eg, a person's physical speed of

---

1099 Recital 41 of the Directive, however, places some limits on such communication to data subjects (and to other persons external to the organisation of the data controller or decision maker). The recital states, *inter alia*, that the right to knowledge of the logic behind automated decision making 'must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software'. Yet the recital also states that 'these considerations must not … result in the data subject being refused all information'. It remains to be seen just how difficult achieving the right balance here will be.

1100 Cf Art 16(1) of the 1992 Amended Proposal for the Directive which specifically referred to 'personality profiles': see *supra* n 1093. By contrast, Art 14(2) of the 1990 Directive Proposal (COM(90) 314 final –- SYN 287, 13.9.1990) referred to 'data defining his [the data subject's] profile or personality'.

1101 See also the French version of the Directive which refers to 'certain aspects of his [the data subject's] personality' ('certains aspects de sa personnalité'), while the German version refers to 'certain aspects of [the data subject's] person' ('einzelner Aspekte ihrer Person').

1102 A point emphasised particularly in Dammann & Simitis, *supra* n 1095, 219.

reaction or blood type) are unlikely in themselves to constitute 'personal aspects' unless they are combined with other data that connect them more directly to a person's character (eg, the data are applied to evaluate a person's degree of diligence/negligence in a particular context).[1103]

The exemplification further indicates that 'personal aspects' need not relate primarily to the private (non-public) or domestic (non-professional) sides of a person's character. There would also appear to be no necessity that these aspects are unique to the person. It is otherwise exceedingly difficult at this stage to make reasonably determinative statements about the reach of the phrase 'certain personal aspects'.

Nevertheless, there can be little doubt that a fully automated decision by a bank to refuse a person cash simply because the person lacks the necessary credit in his/her bank account, will fall outside the ambit of Art 15(1).[1104] A different result might well arise, however, if the decision concerned were grounded on a fully automated analysis of the person's payment history. To take a related example, may Art 15(1) apply to a fully automated decision about a person's eligibility for a retirement pension, when the decision is grounded simply on the level of the person's income and financial assets? There is no obvious answer to the question.[1105] At first glance, these data types appear relatively neutral in terms of what they indicate about a person's character. Yet they are sufficient to constitute a rudimentary personality profile when linked together and it might well be possible to derive latent aspects of a person's character from their linkage. Moreover, they are sufficient to give a reasonable indication of a person's creditworthiness (one of the categories of 'personal aspects' listed in Art 15(1)). Thus, solid grounds exist for arguing that Art 15(1) embraces the above type of decision on pension eligibility.

The right in Art 15(1) is not absolute. According to Art 15(2), a person may be subjected to a decision referred to in Art 15(1) in two sets of situations:

1) where the decision is taken in the course of entering into or executing a contract, *and* either the data subject's request for the entering into or execution of the

---

1103 See also *ibid*, 219–220; E Ehmann & M Helfrich, *EG Datenschutzrichtlinie: Kurzkommentar* (Cologne: O Schmidt, 1999), 230.

1104 The same line is taken in, ia, *Behandling af personoplysninger*, Bet nr 1345 (Copenhagen: Statens Information, 1997), 494. See also COM(92) 422 final – SYN 287, 15.10.1992, 26: 'The processing must apply variables which determine a standard profile (considered good or bad) to the data concerning the data subject; this excludes all cases where the system does not define a personality profile: for example, the fact that a person is unable to obtain the sum of money he wants from an automatic cash dispenser because he has exceeded his credit limit would not fall inside this definition'.

1105 Cf the Skauge Committee which appears to have had little trouble in answering this question in the negative: see NOU 1997:19, 69. The Committee's report subsequently notes, though, that '[a]vgrensningen av hva som skal regnes som 'bestemte personlige forhold' må generelt sies å være relativt uklar': *id*.

contract has been fulfilled *or* provision is made for 'suitable measures' to safeguard the person's 'legitimate interests' (Art 15(2)(a)); or

2) where the decision 'is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests' (Art 15(2)(b)).

Article 15(2) stipulates that both its sets of derogations must be incorporated into the legal regimes of EU Member States, though 'subject to the other Articles of this Directive'. How problematic this is from a data protection perspective will depend partly on the nature of the "suitable measures" for safeguarding the interests of data subjects.

An example of a 'suitable measure' in the first situation delineated by Art 15(2) is described as 'arrangements allowing [the data subject] … to put his point of view' (Art 15(2)(a)). Given the rationale for Art 15, it is to be presumed that these arrangements must not only allow for the data subject to put his/her point of view but also ensure that this point of view is received and taken into account by those who are formally responsible for the decision concerned.[1106] It is further to be presumed that the arrangements must allow for the data subject's viewpoint to be expressed *before* any final decision is made.[1107]

This example of a 'suitable measure' is undoubtedly pertinent for Art 15(2)(b) as well. At the same time, the example is not intended to delineate the entire range of 'suitable measures' in both situations.

Independent of the issue of suitable measures, there is a significant problem from a data protection perspective in one of the assumptions apparently underlying Art 15(2)(a): this assumption is that fulfilment of a person's request to enter into or execute a contract will always be unproblematic for that person. Such an assumption, however, is fallacious – as indicated by the bank loan example set out above. To take another example, Art 15(2)(a) would seem to allow a person's application for employment to be decided solely on the basis of psychometric testing if he/she is given the job (ie, his/her request to enter into a contract is met). Yet such testing can have detrimental consequences for the person concerned (and for the quality of employment application processes generally): eg, the person could well regard such testing as demeaning, or the testing could fail to reveal that the person is qualified for another, more favourable position. These sorts of problems might be able to be mitigated if the above phrase 'subject to the other Articles of this Directive' is read as requiring the application of Art 15(2)(a) to conform with the general requirements of Art 6(1) – most notably, the fairness criterion in Art 6(1)(a). This criterion is analysed in section 18.4.1.

Finally, it should be noted that, in the interests of freedom of expression, certain derogations from Art 15(1) – and from other provisions in Chapters III, IV and VI of

1106 See also Dammann & Simitis, *supra* n 1095, 221–222.

1107 See also Ehmann & Helfrich, *supra* n 1103, 233.

the Directive – are permitted pursuant to Art 9. These derogations are dealt with in section 18.4.6.

18.3.2 GERMANY'S TELESERVICES DATA PROTECTION ACT

Unlike the EC Directive, the *Teleservices Data Protection Act* expressly restricts the *generation* of certain types of profiles – more specifically, profiles of teleservice users.[1108] The creation (by teleservice providers) of such profiles is allowed if four cumulative conditions are met: (i) the profiles are linked to pseudonyms; (ii) the profiles are only used for purposes of 'advertising, market research and structuring the teleservices to comply with demand'; (iii) the user does not object to the profiling; and (iv) the profile is not combined with data relating to the bearer of the pseudonym' (s 6(3)).[1109] This regulation serves to reduce the transparency of teleservice users *vis-à-vis* teleservice providers (and others) at the same time as it allows providers some ability to trace and analyse patterns of teleservice consumption at an individual user level.[1110] Of course, the reduction of transparency does not amount to full user anonymity, just 'quasi-anonymity',[1111] or, more specifically, a form for *legally conditioned* anonymity. No definition of the term 'profile' is given by the Act or its *travaux préparatoires*. Concomitantly, the term is not qualified in a manner that cuts back on its potential scope – unlike the situation with Art 15(1) of the Directive.[1112] It is apparent, though, that s 4(4) directly addresses the generation of *specific* profiles only, as opposed to purely abstract profiles. Whether or not the restrictions in s 4(4) may be waived by the consent of the data subject is unclear.

The restrictions in s 6(3) are directly supplemented by ss 4(4)(4) and 6(5). Section 4(4)(4) requires that teleservice providers 'take technical and organisational measures' to ensure that 'personal data relating to the use of several teleservices by one user may be processed separately', while s 6(5) restricts the transfer (by a

---

1108 For details on the Act's background and scope, see Chapter 10 (section 10.2).

1109 The same restriction applies with respect to use of mass media services: see s 19(4) of the *Interstate Agreement over Media Services*. The data protection rules in this Agreement largely mirror the rules of the *Teleservices Data Protection Act*.

1110 In the words of the *travaux préparatoires* to the Act, '[d]ie Regelung ermöglicht einen Kompromiß zwischen dem Interesse des Nutzers an weitgehender Anonymität seines Konsumentenverhaltens und dem berechtigten wirtschaftlichen Interesse des Dienstanbieters, die Inanspruchnahme der Teledienste auszuwerten': *Gesetzentwurf der Bundesregierung; Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste* (Deutscher Bundestag, 13 Wahlperiode, Drucksache 13/7385, 9.4.1997), 24.

1111 'Pseudonymes Handeln ermöglicht nicht anonymes, sondern quasi-anonymes Handeln. Ein Pseudonym kann ein Name oder eine Kurzbezeichnung sein, die aus sich heraus die Identität des Nutzers nicht preisgeben, aber über eine Referenzliste beim Diensteanbieter mit der Identität des Nutzers zusammengeführt werden können': *ibid*, 23.

1112 Note too the Swiss legislation dealt with in section 18.3.3.

teleservice provider) of usage and accounting data to third parties, including other teleservice providers.[1113] A range of other provisions in the Act also contribute, albeit more indirectly, to restricting both the generation and application of user profiles.[1114]

18.3.3 THE SWISS FEDERAL DATA PROTECTION ACT

The Swiss federal *Data Protection Act* has provisions dealing specifically with 'personality profiles' ('Persönlichkeitsprofile'). A 'personality profile' is defined as a 'combination of data allowing assessment of essential aspects of a natural person's personality' (Art 3(d)).[1115] A personality profile as so defined does not embrace a purely abstract profile. Neither does it embrace a profile of a legal person or collective entity unless the profile allows assessment of a particular individual's personality. There is no necessity for a personality profile to provide a *complete* picture of the personality concerned, only 'essential' aspects of the latter. It would also seem unnecessary that the data collection concerned provides a 'final and objective' assessment of personality.[1116]

At the same time, the exact meaning of 'essential' is far from clear. Does the criterion signify that the data collection concerned must, in effect, reveal information about those sensitive aspects of personality which are specifically addressed in Art 3(c) of the Act (under the heading 'data especially worthy of protection' ('besonders schützenswerte Personendaten'))?[1117] Support for an affirmative answer to this question could be derived from the fact that the regulation of 'personality profiles' is the same as for the data categories listed in Art 3(c). Yet an affirmative answer would render Art 3(d) superfluous – unless the provision is merely intended to signify that the sensitivity of a data-processing operation does not derive solely from the initial sensitivity levels of each of the various data elements. Some manifestation of such an intention can be found in the commentary to the government Bill for the legislation,[1118] but this is only weak. Earlier elaborations in

---

1113 Usage data may be transmitted to other providers if (i) this is for the purposes of market research; and (ii) the data are anonymised. Accounting data may be transmitted to a third party if (i) the latter is contracted by the provider to render accounting services; (ii) the transferred data are necessary to carry out this task, and (iii) the third party observes confidentiality requirements. These restrictions do not apply to transfer of data to law enforcement agencies for the purpose of criminal prosecution (s 6(5)).

1114 See further sections 18.4.3 and 18.4.5.

1115 'Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt'.

1116 Belser, *supra* n 700, 80.

1117 The latter data types are elaborated upon in Chapter 10 (section 10.1.2).

1118 See *Botschaft*, *supra* n 680, 35 ('Entscheidend ist, dass auch durch die systematische Zusammenstellung von an sich nicht besonders schützenswerten Daten (z.B. über Lesegewohnheiten, Reise- und Freizeitaktivitäten) sensitive Bereiche einer Person, z.B. ihre Weltanschauung, erschlossen werden können').

the same commentary over 'personality profiles' make no attempt to limit the scope of such profiles to the areas covered by Art 3(c).[1119] Other commentaries I have read on the legislation fail to provide guidance on the issue. Noteworthy, though, is the opinion of the Swiss Federal Data Protection Commissioner that a personality profile is not constituted by a register containing a debtor's name and address together with data about the debt-recovery and bankruptcy proceedings initiated against that person.[1120] This seems to indicate that the Commissioner does not view data that allow assessment only of a person's payment capabilities and, possibly, credit worthiness as pertaining to 'essential' aspects of personality. Yet the opinion tells us little else about what is meant by 'personality profile'. Indeed, there is very little elaboration of the concept in the annual reports and other public guides issued by the Commissioner.[1121]

As noted above, personality profiles are subjected to the same special regulations as govern the categories of sensitive data listed in Art 3(c). On many points, this regulatory regime is similar in effect to that of the EC Directive. However, some major points of difference exist. One such point is that, unlike the Directive, the rules of the Swiss Act clearly discriminate between data controllers in the private sector and data controllers in the public sector, with regulation of the latter generally more stringent than for the former. Indeed, regulation of data controllers in the private sector sometimes falls short of the requirements in the Directive – as is made clear further below. Another major point of difference is that the Swiss Act lacks the explicit rights to object as found in Arts 14(2) and 15(1) of the Directive, though a

---

1119 *Ibid*, 34–35 ('Ein Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeit und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der betreffenden Person ergibt'). The same general description of 'personality profiles' is embraced by the Swiss Federal Data Protection Commissioner (Eidgenössischer Datenschutzbeauftragter) in, ia, his second annual report: see *2. Tätigkeitsbericht 1994/95* (available via <http://www.edsb.ch/>), Part II, section 6.

1120 See *5. Tätigkeitsbericht 1997/98* (available via <http://www.edsb.ch/>), Part I, section 7.2.

1121 My impression here is based solely on a search (undertaken 12.5.2002) of the Commissioner's Internet homepage (<http://www.edsb.ch/>). The search revealed little more than a handful of instances in which the Commissioner has specifically addressed the concept of 'personality profile'. For the most part, the Commissioner merely indicates that such a profile *could* result from a particular data collection or data-processing operation. See espec *2. Tätigkeitsbericht 1994/95*, Part I, section 3.8 (data on television-viewing preferences can result in personality profiles); *3. Tätigkeitsbericht 1995/96*, Part I, section 3.1 (data on Internet-surfing patterns can result in personality profiles); *4. Tätigkeitsbericht 1996/97*, Part I, section 3.3 (personality profiles can be generated from financial transaction data registered in postal accounts). Cf *1. Tätigkeitsbericht 1993/94*, Part I, section 9.1 ('graphologischer Gutachten' about job applicants will 'usually' ('in der Regel') constitute personality profiles). See also *2. Tätigkeitsbericht 1994/95*, Part II, section 6 (on publication of book 'Die 350 Reichsten und Einflussreichsten in der Schweiz'); *5. Tätigkeitsbericht 1997/98*, Part I, section 4.2 (on disclosure of data about unemployed persons over the Internet); *5. Tätigkeitsbericht 1997/98*, Part I, section 5.4 (on the 'AHV-Spiegelregister'); *5. Tätigkeitsbericht 1997/98*, Part II, section 1.1 (on use of customer cards).

general right to object can be derived from Art 15(1) in the Act. This right is set to be strengthened under proposed amendments.[1122]

There are two main provisions specifically regulating the creation and further processing of personality profiles by federal government agencies. First, Art 17(2) prohibits such processing unless it is either:

- expressly permitted by a formal law ('formelles Gesetz'); or
- indispensable for accomplishing a task that is clearly defined in a formal law; or
- authorised by the Federal Council (Bundesrat – federal government) on the grounds that the rights of the data subject are not endangered; or
- the data subject has consented to the processing or made the data concerned publicly accessible.[1123]

Secondly, Art 18(2) stipulates that such processing must always be brought to the notice of the data subject.[1124]

As for the creation and further processing of personality profiles by persons and organisations in the private sector, the main rule specifically regulating such activity is found in Art 11(3).[1125] This provision requires the data controller to notify the Federal Data Protection Commissioner of the data collection concerned if:

- the controller 'regularly' ('regelmässig') processes such a profile; and
- the processing is not mandated by statute; and
- the data subjects have no knowledge of the processing.

Notification must occur before the data collections are utilised (Art 11(4)).[1126] The information notified to the Commissioner shall be entered into a publicly available register pursuant to Art 11(1). There is, however, no requirement for data controllers to provide direct notification to data subjects, though such a requirement will pertain under proposed amendments to the Act.[1127]

Several other provisions specifically regulate the *disclosure* to third parties of personality profiles by data controllers in the private sector. Article 12 stipulates that

---

1122 These provisions are formulated in terms of the 'processing' ('bearbeiten') of such profiles, but the term 'processing' is defined broadly to include the 'acquisition' ('beschaffen') of data (Art 3(e)). It goes without saying that the generation and use of personality profiles must also conform to all of the rules in the Act for government processing of personal data generally. See the proposed new Arts 15a and 17(2)(c) as summarily described in RJ Schweizer & P Sutter, 'Die Revision des Datenschutzgesetzes in der Schweiz' (2002) *DuD*, no 3, 156ff. It is unclear when these amendments will take effect.

1123 For detailed commentary on Art 17, see J-P Walter, 'Art. 17', in Maurer & Vogt, *supra* n 700, 228ff.

1124 For detailed commentary on Art 18, see J-P Walter, 'Art. 18', in Maurer & Vogt, *supra* n 700, 240ff.

1125 Again, it goes without saying that such activity must also conform to all of the rules in the Act for private sector processing of personal data generally.

1126 For detailed commentary on Art 11, see U Belser, 'Art. 11', in Maurer & Vogt, *supra* n 700, 170ff.

1127 See new Arts 7a & 7b, set out in Schweizer & Sutter, *supra* n 1122, 159. It seems that Art 7a will apply only with respect to especially sensitive data and personality profiles. Cf Arts 10–11 of the EC Directive (described in section 18.4.5). The new Art 7b will apply in relation to the decision making embraced by Art 15 of the Directive.

such disclosure is not permitted without 'justification' ('Rechtfertigungsgrund').[1128] Justification is deemed to exist when disclosure is consented to by the data subject, or is required by law or by some 'overriding' ('überwiegendes') private or public interest (Art 13(1)). A lengthy though non-exhaustive list of alternative conditions for when such an interest can exist is set out in Art 13(2).[1129] Of especial importance is that these conditions do not apply when the disclosure or other processing of a personality profile is undertaken for the purposes of assessing a person's credit-worthiness (Art 13(2)(c)).

18.3.4 NORWEGIAN PDA

Norway's *Personal Data Act* of 2000 contains an innovative provision to promote data subject awareness of certain profiling practices. Section 21 of the Act places data controllers under a duty of information when, on the basis of 'personal profiles' ('personprofiler'), either the data subject is approached/contacted or a decision, directed at the data subject, is made. In such cases, the data subject must be automatically informed of the data controller's identity, the data constituting the profile(s) and the source(s) of these data.[1130] This duty of information complements

---

1128 For detailed commentary, see M Hünig, 'Art. 12', in Maurer & Vogt, *supra* n 700, 186ff.

1129 These conditions are, in summary: (a) the processing in question is 'closely connected with' ('in unmittelbarem Zusammenheng mit') the conclusion or execution of a contract with the data subject; (b) the processing is pursuant to, and for the purposes of, economic competition, but does not involve disclosure of the data to third parties; (c) the processing is for the purposes of credit assessment (subject to exceptions for personality profiles: see *infra*) but does not involve disclosure of the data to other parties than those who require the data for concluding or executing a contract with the data subject; (d) the processing is undertaken on a professional basis for the sole purpose of a publication in an edited periodical medium ('im redaktionellen Teil eines periodisch erscheinenden Mediums'); (e) the processing is undertaken for non-personal ends, particularly those related to research, planning and statistics, and any published results are in a format not permitting identification of the data subject(s); or (f) the processed data relate to a 'public person' ('eine Person des öffentlichen Lebens') and concern his/her public life. For detailed commentary on these conditions, see M Hünig, 'Art. 13', in Maurer & Vogt, *supra* n 700, 197ff.

1130 The provision reads as follows: 'Når noen henvender seg til eller treffer avgjørelser som retter seg mot den registrerte på grunnlag av personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, f eks som ledd i markedsføringsvirksomhet, skal den behandlingsansvarlige informere den registrerte om (a) hvem som er behandlingsansvarlig, (b) hvilke opplysningstyper som er anvendt, og (c) hvor opplysningene er hentet fra'. The provision is similar to s 23 of the draft Bill proposed by the Skauge Committee except that the information duty pursuant to the latter provision also arises when, on the basis of a personal profile, a decision ('enkeltavgjørelse') is made determining a person's legal rights/duties: see NOU 1997:19, 167. The Ministry of Justice decided to leave this decisional criterion out of s 21 of the Act because of difficulties in defining the concept of 'enkeltavgjørelse' (which is a product of administrative law), particularly in the context of private sector activity: see Ot prp 92 (1998–99), 120, 60.

and extends the duties of information set out in Arts 10–11 of the EC Directive (and which are incorporated in ss 19–20 of the Act).[1131]

Unfortunately, the concept of 'personal profiles' is not properly defined in the Act or the *travaux préparatoires*. Thus, it is not entirely clear if the concept covers both abstract and specific profiles. The structure of the concept would seem to suggest that it covers only profiles based on 'personal' data. However, the Skauge Committee in its draft Bill intended the concept to cover both abstract and specific profiles; ie, the profiles would not have to be composed of 'personal' data but could be made up entirely of statistical/aggregate data.[1132] The Ministry of Justice did not specifically address this possibility at all in relation to s 21 of its Bill. It stated, though, that s 21 'largely equates' ('[i] hovedsak tilsvarer') with s 23 of the draft Bill proposed by the Skauge Committee. This statement could be read to imply that the concept of 'personal profiles' is to be construed in the same way as it was construed by that Committee. However, when illustrating how such profiles are generated, the Ministry tended to refer to the processing of 'personal' information.[1133] From a data protection perspective, it would be advantageous for the concept of 'personal profiles' to embrace both personal and non-personal data. This notwithstanding, it would also be remarkable if the concept does in fact embrace both data types, given that the ambit of the Act (along with many other data protection laws) is otherwise limited to the processing of personal data only.

The duty of information in s 21 seems to arise *after* application of a personal profile, not before. This aspect of the duty is not specifically addressed in the *travaux préparatoires*. Thus, the time frame in which the information has to be given remains unspecified. Presumably, the information would have to be given as soon as is reasonably practicable. In any case, the *ex post facto* operationality of the duty reduces the latter's value as a means of controlling the quality of profile generation, especially if the profiles are based only on non-personal data (to which the duty of information in s 21 might not attach, and to which rights of access and rectification will certainly not attach). Concomitantly, it diminishes the duty's value as a proactive means of ensuring fairness for data subjects. At the same time, though, it would probably be impracticable to make such a duty operate *ex ante*.

The provision does not require notification of the actual assumptions lying behind each profile. This omission is noted in the *travaux préparatoires* but not explained:[1134] is it because of a belief that the provision of such information would be overly burdensome for data controllers and of relatively little benefit for data subjects, or is it

---

1131 See section 18.4.4 below.

1132 NOU 1997:19, 148.

1133 Ot prp 92 (1998–99), 120 ('Bestemmelsen gir rett til informasjon ved bruk av personprofiler, og får bl a betydning for bruken av elektroniske spor, dvs *personopplysninger* som rutinemessig innsamles i systemer for betalingsformidling, elektroniske informasjonstjenester og annet. […] Personprofiler kan også baseres på *personopplysninger* som er samlet inn på annen måte, f eks på opplysninger om inntektskategori, boligstrøk og alder …': emphasis added).

1134 Ot prp 92 (1998–99), 120; NOU 1997:19, 148.

due to a belief that such assumptions would be plain to discern for data subjects? The latter belief and, to a lesser extent, the former belief seem naive in light of the increasing sophistication and complexity of profiles.[1135] However, the omission will be *partly* mitigated by the right of data subjects (as set down in s 22 of the Act and Art 12(a) of the EC Directive) to gain access to information about the logic behind automated decisions. This right is canvassed in section 18.4.5.

18.4 Indirect Regulation of Profiling

This section explores central ways in which data protection laws – primarily the rules of the EC Directive – may indirectly regulate profiling practices. Focus is directed first at the reach of the main rules expressing the principles of fair and lawful processing, purpose specification and minimality. Then comes an analysis of rules dealing specifically with information quality, and, thereafter, rules dealing specifically with rights and duties on information access, notification and consent. A description of the main categories of derogations to these rules is then given. Finally, there is a presentation of the way in which profiling practices may be regulated pursuant to a licensing system such as that established under Norwegian legislation.

18.4.1 PRINCIPLE OF FAIR AND LAWFUL PROCESSING

How and to what extent may profiling practices be restricted by the principle – enshrined in, ia, Art 6(1)(a) of the EC Directive – that personal data be 'processed fairly and lawfully'? Obviously, both the generation and application of profiles will have to comply with this principle insofar as they involve the processing of personal data, but what exactly does the principle require of such processing?

The criterion of lawfulness is relatively self-explanatory. Less obvious but potentially broader is the criterion of fairness. This criterion is not directly defined in the EC Directive or its *travaux préparatoires*. It is rarely defined directly in other data protection instruments or their *travaux préparatoires*. However, the phrasing of Art 6(1)(a) – which links the criterion of fairness to the *processing* of personal data – indicates that the other provisions in the Directive which attach rights and obligations to various aspects of processing are an elaboration of the criterion of fairness (along with that of lawfulness). Indeed, two of these provisions expressly state that certain of their rules are elaborations of a fairness requirement.[1136]

Two questions then arise: does the fairness criterion in Art 6(1)(a) have a content beyond what is elaborated in the other provisions of the Directive? If it does, what is

---

1135 See generally Chapter 17 (section 17.2).

1136 See Arts 10–11 presented in section 18.4.5.

that content? The first question is relatively easy to answer in the affirmative, for a negative answer would effectively render the criterion redundant. The second question is much more difficult to answer conclusively.

Preliminary comments on the content of the fairness criterion are given in Chapter 3 (section 3.2). It will be recalled from there that, while the criterion cannot be exhaustively defined in the abstract, certain requirements may be read into it: notably, a requirement that data controllers do not ride roughshod over the interests and reasonable expectations of data subjects; concomitantly, that persons are not unduly pressured into supplying data on themselves to a data controller or accepting that the data are used by the latter for particular purposes, such as profiling; and that the processing of personal data be transparent and non-misleading for the data subject(s). Further, the fairness criterion may necessitate that data controllers provide data subjects with more details about their processing operations than are expressly listed in Arts 10 and 11 of the Directive (set out in section 18.4.4). Such details may concern, for example, the nature of particular profiling practices (including the reasoning upon which they are based), at least when these practices involve the processing of personal data and significantly impinge on the data protection interests of the data subjects.[1137] Arguably, another requirement flowing from the link between fairness and transparency is that, as a point of departure, personal data shall be collected directly from the data subject, not from third parties. This requirement is expressly laid down in some data protection instruments,[1138] though not the Directive. Nevertheless, it arguably inheres in the Directive's Art 6(1)(a). Such a requirement would appear to have little direct effect on profiling practices but may help to mitigate some of the information quality problems which these practices raise and sometimes magnify.

The requirement that data controllers must take some account of the reasonable expectations of data subjects has direct consequences for the purposes for which data may be processed. It helps to ground rules embracing the purpose specification principle (dealt with more fully in the next section) and sets limits on the secondary purposes to which personal data may be put. More specifically, it arguably means that when personal data obtained for one purpose are subsequently used for another purpose, which the data subject would not reasonably anticipate, then the data controller may have to obtain the data subject's positive consent to the new use. This line has been taken by the UK Data Protection Tribunal (now 'Information Tribunal') in a decision touching upon the marketing of goods and services on the basis of customer profiles.[1139] While the Tribunal's decision is not directly relevant for interpretation of Art 6(1)(a) of the Directive, it does illustrate that:

1137 Cf s 21 of Norway's *Personal Data Act* as described in section 18.3.4. See further section 8.4.5 below.

1138 See *supra* n 211.

1139 *British Gas Trading Limited v Data Protection Registrar* (1998) – decision of 24.3.1998 (case reference unspecified) set out in *Fourteenth Report of the Data Protection Registrar, June 1998*

- the reasonable expectations of data subjects may play an important role in the elaboration and application of the fairness criterion in situations where data are used for secondary purposes that involve profiling; and
- taking account of such expectations potentially impinges on the ability to apply and, usually more indirectly, generate profiles (primarily, specific profiles and, secondarily, abstract profiles).[1140]

Finally, consideration must be given to whether assessment of what is fair pursuant to Art 6(1)(a) is intended to be carried out by reference to the interests of data subjects only. The notion of fairness on its own can connote that the interests of both data subjects and data controllers be taken into account.[1141] However, in the context of Art 6(1)(a), and in light of recitals 9–11,[1142] it is most natural to interpret 'fairly' as primarily, if not exclusively, denoting concern for the interests of data subjects.[1143] Nevertheless, any obligations on data controllers implied by the fairness criterion in Art 6(1)(a) and not expressly laid down in other provisions must probably be qualified by reference to what is reasonably practicable for data controllers to accomplish in the circumstances of the case. The application of this sort of standard follows from the latent nature of the obligations together with the fact that some of

---

(Cont.)

(London: The Stationery Office, 1998), Appendix 6. The case concerned the ability of a utility company to process personal data that the company collected pursuant to a contract for the supply of gas to the data subject, the contract being entered into at a time when the supplier held a monopoly over such gas supply. The main point of contention was whether the company could use these data to market, *vis-à-vis* the data subject, other types of goods or services without the data subject's prior and positive consent. The Tribunal, like the then Data Protection Registrar, held that use of the data in such a way would breach the fairness criterion in DPP 1 in Part I of Schedule 1 to the *Data Protection Act* of 1984 (stating that 'the information to be contained in personal data shall be obtained ... fairly and lawfully'), unless the use accorded with what the data subject would reasonably anticipate. According to the Tribunal, the marketing of gas-related goods or services ('including the promotion of energy conservation') could be reasonably anticipated but not the marketing of goods or services related to 'banking, mortgages, or health, household or endowment insurance'. It is pertinent to note that the issue of profiling received explicit attention in the case, with the Tribunal observing that the customer information 'when processed, particularly when combined with personal data from other sources, enables a 'profile' of an individual to be built up of use in marketing'. See too *Innovations (Mail Order) Limited v Data Protection Registrar* (1993) Case DA/92 31/49/1. The case concerned a mail-order company that, upon collecting personal data from its customers, sold these data to third parties without first informing the customers of its 'list-broking' practice. The Tribunal found the practice to violate the fairness criterion partly because the practice involved what was for the customers a non-obvious use of their data.

1140 Compare also NPP 2.1(a)–(b) in Schedule 3 to Australia's federal *Privacy Act*.

1141 See further Chapters 5 and 8.

1142 Set out *supra* n 135.

1143 The UK Data Protection Tribunal adopted a similar line when interpreting the fairness criterion in the UK *Data Protection Act* of 1984: see *CCN Systems Limited and CCN Credit Systems Limited v The Data Protection Registrar* (1991) Case DA/90 25/49/9, paras 48–52 (holding that, as the basic purpose of the Act is to protect the rights of data subjects, the fairness criterion must be applied paramountly in consideration of data subjects' interests).

the other provisions of the Directive which implicitly express the fairness criterion also seem to operate with such a standard.[1144]

At the same time, the Directive specifically permits derogations from the requirements in Art 6(1)(a) pursuant to both Arts 9 and 13(1). The general thrust of the latter provisions is described in section 18.4.6.

18.4.2 PRINCIPLE OF PURPOSE SPECIFICATION

The principle of purpose specification is expressed in Art 6(1)(b) of the EC Directive as follows:

> '[Member States shall provide that personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that the Member States provide appropriate safeguards.'

Application of the purpose specification principle is a central, albeit challenging, element of all data protection regimes. As the Data Protection Working Party appropriately observes, '[a]ssessing the compatibility of any given operation with the purpose for which the data were originally collected … is one of the most difficult and important tasks in supervising compliance with data protection legislation'.[1145] More specifically, application of rules embodying the purpose specification principle has obvious repercussions for the ability to generate and use profiles insofar as the latter processes involve a re-purposing of personal data. As noted in Chapter 17, profiling techniques will often involve such re-purposing.

The principle in Art 6(1)(b) is grounded partly in concern for ensuring foreseeability in data-processing outcomes. Concomitantly, the principle aims to ensure that both the way in which personal data are processed and the results of such processing conform with the reasonable expectations of data subjects. Expressed more abstractly, we can say that the principle aims to reduce deficits in the cognitive sovereignty of data subjects. The principle is additionally grounded in concern for ensuring that personal data are used for purposes to which they are suited. In other words, the principle is concerned with ensuring adequate information quality,[1146] and, more indirectly, adequate cognitive quality. In this regard, we can see the principle as also serving to ensure that data-processing outcomes conform with the expectations of data controllers. The principle is grounded in several other concerns too – most notably, a concern to dissuade data controllers from accumulating extensive amounts

---

1144 See espec Arts 6(d), 11(2) and 12(c).

1145 See Data Protection Working Party, 'Notification', Working Document adopted 3.12.1997, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp8en.htm>, chapt 4.

1146 Hence, the title given to Art 6 is 'Principles Relating to Data Quality'.

of personal data in the belief that the data might sometime prove useful,[1147] and a concern to increase the privacy and autonomy of data subjects and, concomitantly, decrease the overall surveillance levels of society.[1148]

Given its above-described rationale, the purpose specification principle and rules giving effect to it would appear to have considerable potential to tackle many of the problems with profiling identified in Chapter 17 (section 17.3). The extent to which this potential can be realised, though, will partly depend on how the terminology of the principle and its rules is construed.

The principle, as manifested in Art 6(1)(b), consists of three conditions:

1. the purposes for which data are collected shall be 'specified' and 'explicit';
2. these purposes shall be 'legitimate';
3. the purposes for which the data are further processed shall not be 'incompatible' with the purposes for which the data are first collected.

The first of these conditions is relatively free of ambiguity. From the wording of Art 6(1)(b), it is apparent that the purposes for which a data controller collects personal data must be defined and documented in advance of collection.[1149] Further, the purposes must be delineated in a relatively concrete, precise way.[1150]

The second condition is more problematic: what is the meaning of 'legitimate'? Does it simply mean 'lawful'? Or does it denote a broader criterion of social acceptability? Certain comments in the *travaux préparatoires* can be read as indicating that 'legitimate' is essentially synonymous with 'lawful' but they are far from conclusive on this point.[1151] Some of the national legislation enacted to implement the Directive also define the purposes for which personal data may be collected and further processed simply in terms of that which is 'lawful',[1152] but, again, this is hardly conclusive of the issue.

1147 See also P Blume, 'Formålsbestemthedsprinsippet i databeskyttelsesretten' (1995) 9 *UfR*, 110.

1148 See further C Lenth, *Adgangen til å benytte personopplysninger med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor*, CompLex 2/2000 (Oslo: Universitetsforlaget, 2000), 18–19, 20–21.

1149 Note too COM(92) 422 final – SYN 287, 15.10.1992, 15. The purpose(s) must also be notified to the data subject pursuant to Arts 10–11 of the Directive: see further section 18.4.5.

1150 See also COM(92) 422 final – SYN 287, 15.10.1992, 15.

1151 *Id* ('Personal data can be stored and used only for a 'legitimate' purpose, so that the potential purposes of processing are limited. A processing operation may be designed and performed only for a purpose permitted by the Directive and by the domestic legislation in the Member States'). The German version of Art 6(1)(b) uses the term 'rechtmässige', which connotes 'lawful' and which is also the same term used in Art 6(1)(a). However, the French version uses the term 'légitime' as opposed to 'licitement', which is used in Art 6(1)(a). Similarly, the Swedish version employs the term 'berättigade', which connotes 'justified' and which seems broader than the term 'laglig' ('lawful') employed in Art 6(1)(a).

1152 See, eg, DPP 2 in Part I of Schedule 1 to the UK *Data Protection Act* of 1998. The equivalent provision in the 1984 UK legislation operated with the same lawfulness criterion.

A problem with construing 'legitimate' as 'lawful' is that it creates some overlap with the rule on 'fair and lawful' processing in Art 6(1)(a). Moreover, it overlooks the fact that 'legitimate' can carry connotations not fully captured by 'lawful'. Thus, fairly solid grounds exist for arguing that 'legitimate' embraces a potentially broader criterion of social acceptability, such that personal data should only be processed for purposes that do not run counter to predominant social mores.[1153] But, if so, how are these mores to be defined? Are they to be defined essentially in terms of procedural norms (eg, that the purposes for which personal data are processed should be compatible with, or fall naturally within, the ordinary (and lawful) ambit of the particular data controller's activities)? Or do they also have substantive elements (eg, that the data controller's activities are socially desirable in the sense that they promote or do not detract from some generally valued state of affairs constituted by, say, a particular balance between privacy-related interests and economic interests)?

The general conditions for data processing laid down in Art 7 of the Directive provide some guidance on the ambit of the legitimacy criterion,[1154] at least for the purposes of the Directive, but this guidance is scarcely exhaustive. These conditions are, in summary, as follows: (a) the data subject consents to the processing; (b) the processing is necessary for concluding a contract with the data subject; (c) the data controller is legally required to carry out the processing; (d) the processing is necessary for protecting the 'vital interests' of the data subject; (e) the processing is necessary for performing a task executed in the 'public interest' or in exercise of official authority; or (f) the processing is carried out in pursuance of 'legitimate interests' that override the conflicting interests of the data subject. From these conditions, it would seem that the reference to 'legitimate' in Art 6(1)(b) is to be understood mainly in procedural terms, but that substantive elements might also come into consideration, depending on how one interprets the undefined phrases 'vital interests', 'public interest' and 'legitimate interests'.

The most important point to take from this discussion is that the potential regulatory impact of Art 6(1)(b) – and of other rules enshrining the purpose specification principle – on profiling operations will be more stringent when a social acceptability criterion is applied which embraces both procedural and substantive elements as exemplified above, than when a mere lawfulness criterion is applied. This will also be so even when a social acceptability criterion is applied which only requires that the data processing in question falls within the data controller's normal

---

1153 In other words, the purpose specification principle, insofar as it uses such a criterion, can arguably be said to harbour a 'social justification principle' similar to that proposed by the New South Wales (NSW) Privacy Committee in its *Guidelines for the Operation of Personal Data Systems*, Background Paper 31 (Sydney: NSW Privacy Committee, 1977), 3. According to the latter principle, 'a personal data system should exist only if it has a general purpose and specific uses which are socially acceptable'. A similar principle has been championed by Michael Kirby: see MD Kirby, 'Transborder Data Flows and the 'Basic Rules' of Data Privacy' (1981) 16 *Stanford J of Int Law*, 27, 46.

1154 A point also made by the EC Commission in its commentary on the equivalent provisions in its 1992 Directive proposal: see COM(92) 422 final – SYN 287, 15.10.1992, 4.

or natural field of operation. While data processing not forming part of a controller's normal or natural field of operation will often be unlawful (and *vice versa*) – particularly when the controller is a statutory body – this will not always be the case.

Of greatest significance, though, in regulating the ability to generate and apply profiles (primarily, specific profiles and, secondarily, abstract profiles) is the third condition. The crucial issue is how to define the phrase 'not … incompatible'. The *travaux préparatoires* provide no help on this question. To begin with, the phrase should probably be read as meaning simply 'compatible', though use of the double negative perhaps denotes a slightly less stringent standard than that of straight compatibility. It might be feasible to read the phrase as simply requiring that the secondary purposes for which data are processed must not reduce the possibility of realising the primary purposes for which the data were collected. This interpretation, however, reduces the rationale for the criterion of compatibility/non-incompatibility to a concern with promoting efficiency of data processing primarily, if not exclusively, for the benefit of the data controller. As such, it fails to do justice to the broader rationale for the purpose specification principle as described towards the beginning of this section, and it can scarcely be supported in light of the fairness criterion in Art 6(1)(a). Accordingly, the phrase 'not incompatible' most likely connotes additional criteria to that just canvassed.

One such criterion is undoubtedly that the secondary purposes are, from an objective point of view, similar to, or at least not fundamentally different from, the primary purposes. This criterion is unlikely to be met when, for instance, data that have been registered for government administrative purposes are sought to be subsequently used for private commercial purposes (on the basis, say, of a profile derived from the data).[1155] Further, if we accept that one of the underlying concerns of the purpose specification principle is to ensure that data are processed in conformity with the reasonable expectations of data subjects, any secondary purposes will not pass the test of compatibility/non-incompatibility unless the data subject is objectively able to read those purposes into the primary purposes, or the secondary purposes are otherwise objectively within the ambit of the data subject's reasonable expectations. It is doubtful, for example, that the purpose of customer profiling, or of

1155 On this point, note, eg, the decision of the Norwegian Data Inspectorate in case 92/2884 (described in Bygrave, *supra* n 37, 141–143) concerning a private company's request to use data from the agricultural property register (Landbruksregisteret) maintained by the State, in order to publish a book on Norwegian farms. The Inspectorate (and Ministry of Justice on appeal) turned down the request because the register is maintained for purely administrative purposes. See also a 1995 Belgian court decision concerning use by the Mercedes company of State-held data on motor vehicle registrations for marketing purposes. The court held this use to be in breach of rules embodying the purpose specification principle and accordingly prohibited it. For further details on the case, see Reidenberg & Schwartz, *supra* n 1073, 85 and references cited therein.

marketing based on customer profiling, would satisfy this test if the primary purpose for the data processing were specified only in terms of billing or accounting.[1156]

Finally, the Directive provides for derogation from the principle of purpose specification in Art 6(1)(b) with respect to data processing for 'historical, statistical or scientific purposes'. This derogation is only permitted, though, when Member States provide 'appropriate safeguards'. Recital 29 states that such safeguards 'must in particular rule out the use of the data in support of measures or decisions regarding any particular individual'. Further derogation from the purpose specification principle in Art 6(1)(b) is permitted pursuant to Arts 9 and 13.[1157]

18.4.3 PRINCIPLE OF MINIMALITY

The principle of minimality requires that the amount of personal data collected is limited to what is *necessary* to achieve the purpose(s) for which the data are gathered and further processed.[1158] Rules giving effect to this principle will have an impact upon profiling practices by restricting the amount of personal data upon which profiles can be generated. Such restriction will primarily affect the creation of specific profiles, though the building of abstract profiles could thereby be indirectly affected as well. It is important to realise that such restriction will not always stop profile generation. Rather, such restriction might only result in the generation of relatively coarse-grained profiles. As a general rule, the less data made available for generating profiles, the less fine-grained and comprehensive will be the profiles generated from those data. The result can discourage any attempts at applying such profiles or narrow the range of purposes for which the profiles are sought to be used.

The minimality principle is manifested in a broad range of rules. In the context of the EC Directive, the most direct manifestation of the principle is the requirement in Art 6(1)(c) that personal data be 'not excessive' in relation to the purposes for

---

1156 See also the decision of 15.9.1997 by the Norwegian Data Inspectorate in case 97/790 (unreported). The case concerned whether or not a bank, Postbanken, could legally use the account data it ordinarily kept on its customers' transactions, in order to market certain financial services *vis-à-vis* these customers on an individualised/customised basis. The DI decided that such use would breach s 2-4 of the main regulations to the PDRA (which permitted use of bank customer data for the purposes of carrying out, ia, 'ordinary bank and financial services' ('ordinære bank- og finanstjenester')). In reaching this decision, the DI held that the ambit of the latter phrase must be interpreted in light of what bank customers would expect such services to involve. In the Inspectorate's view, the above use of customer data did not accord with such expectations: see letter of 15.9.1997 to Postbanken. Note too the Belgian court decisions described *supra* n 613, together with the decision of the UK Data Protection Tribunal in the British Gas Trading case described *supra* n 1140. For analysis and criticism of the Inspectorate's decision in the Postbanken case, see Lenth, *supra* n 1149, 32ff.

1157 See *infra* section 18.4.6.

1158 See also Chapter 3 (section 3.3).

which they are processed. The criterion 'not excessive' connotes utilisation of only those data that are necessary to achieve the purpose(s) for which they are applied.

The minimality principle is also manifested in Arts 7 and 8 of the Directive both of which permit the processing of personal data only if one or more alternative conditions are met. As noted elsewhere, Art 7 addresses the processing of personal data generally. Basically, such processing is permitted only if: (a) the data subject 'unambiguously' consents to the processing; or (b) the processing is 'necessary' for concluding a contract with the data subject; or (c) the processing is 'necessary' for compliance with a 'legal obligation' on the data controller; or (d) the processing is 'necessary' for protecting the 'vital interests' of the data subject; or (e) the processing is 'necessary' for performing a task executed in the 'public interest' or in exercise of official authority; or (f) the processing is 'necessary' for the pursuance of 'legitimate interests' that override the conflicting interests of the data subject.

As for Art 8(1), this prohibits the processing of certain kinds of especially sensitive data; ie, data on a person's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … health or sex life'. Exemptions to this prohibition are laid down in Art 8(2). In summary, these exemptions are as follows: (a) the data subject gives 'explicit' consent to the processing (except where national laws override this condition); or (b) the processing is 'necessary' for the data controller to meet obligations and rights pursuant to 'employment law' and is authorised by 'national law providing for adequate safeguards'; or (c) the processing is 'necessary' for protecting the 'vital interests' of the data subject (or another person where the data subject is incapable of consenting); or (d) the processing is undertaken by a non-profit organisation with a 'political, philosophical, religious or trade-union aim' and only concerns the organisation's members or regular contacts, and the data are not disclosed to third parties without the data subject's consent; or (e) the data are 'manifestly made public' by the data subject, or their processing is 'necessary' for pursuit of 'legal claims'. These exemptions may be supplemented by others that are laid down by national law or a decision of the national data protection authority (Art 8(4)). Further conditions are laid down in Arts 8(3) and 8(5) with respect to medical treatment and the processing of data on criminal convictions and the like.[1159]

By casting the conditions for processing personal data as exceptions to a rule, the drafters of the Directive underline that such processing can have significant

1159 According to Art 8(3), the prohibition in Art 8(1) shall not apply if the processing is required for medical purposes and carried out by a 'health professional' or other person subject to an 'obligation of professional secrecy'. As for data on criminal convictions, this sort of data, along with data on 'offences', 'security measures', 'administrative sanctions' and 'civil trials', may be processed 'only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable safeguards' (Art 8(5)). At the same time, 'a complete register of criminal convictions may be kept only under the control of official authority'; such a requirement may also be laid down for 'data relating to administrative sanctions or civil trials' (Art 8(5)).

ramifications for data subjects and, accordingly, that the legitimacy of such processing cannot be assumed but must be proven in each case. Nevertheless, the broad and open-ended way in which many of these conditions are formulated could render the practical impact of the initial restrictions on processing almost nugatory, at least with respect to Art 7. An especially slippery condition in this regard, and one of potentially great significance for profiling, is Art 7(f). Yet it is difficult at this stage to reach any firm conclusions on these conditions' likely consequences for data processing generally and profiling practices particularly.[1160] This difficulty is exacerbated by the failure of the Directive and its *travaux préparatoires* to provide useful guidance on how to interpret the conditions. Thus, EU Member States (and, indirectly, other countries) are left with considerable flexibility to elaborate criteria for the processing of personal data, including the data types listed in Art 8.

Of crucial importance for the extent to which data processing (and, thereby, profiling practices based on such processing) may occur, is interpretation of the criterion 'necessary' in paras (b) – (f) of Art 7 and paras (b), (c) and (e) of Art 8(2). Is the criterion to be read as merely denoting usefulness and relevance, or is to be read as denoting indispensability? Neither the Directive nor its *travaux préparatoires* specifically address this issue. The necessity criterion should probably be construed as embracing two overlapping requirements: (a) that the processing corresponds to a pressing (and legitimate) social, political or commercial need; (b) that the processing is proportionate to the aim(s) involved. This interpretation is inspired by, and partly builds upon, the way in which the ECtHR has construed the term 'necessary' in Art 8(2) of the ECHR.[1161] Requirement (b) also follows from the criterion 'not excessive' in Art 6(1)(c) of the Directive. The stringency of the above two requirements will undoubtedly vary from case to case depending, ia, on the sensitivity of the data involved and the context in which the processing occurs.[1162] Thus, as a point of departure, the necessity criterion in Art 8(2) should be interpreted strictly; ie, as denoting a relatively stringent standard of indispensability.

1160 For a relatively penetrating attempt to analyse how these conditions will affect the operation of digital rights management systems, see Bygrave & Koelman, *supra* n 316, 75 ff.

1161 See, eg, Bygrave, *supra* n 102, 273. If called upon to construe the necessity criterion in Arts 7 and 8 of the Directive, the ECJ would be unlikely to depart substantially from this line taken by the ECtHR, particularly as the Directive has as one of its objects the protection of the right to privacy in Art 8 of the ECHR: see espec recital 10. Nevertheless, it must be kept in mind that the line taken by the ECtHR has been developed in the context of justifying interferences with the right to respect for private life under Art 8(1) of the ECHR. Whether the drafters of the EC Directive view processing of personal data as generally involving such an interference is not entirely clear. The structure and content of Art 7 ('personal data may be processed only if …') would suggest that they do view processing as at least *potentially* involving such an interference; the same applies *a fortiori* with respect to the structure and content of Art 8. This view would accord with the case law of the ECtHR: see generally Bygrave, *supra* n 102, 259–270.

1162 Again, the same line is taken by the ECtHR when applying the necessity criterion pursuant to Art 8(2) of the ECHR: see *ibid*, 273–274.

The generation and application of profiles based on processing of the data types listed in Art 8 will be considerably more difficult than with respect to other types of personal data. Accordingly, an important issue is whether or not the list of data categories in Art 8(1) is exhaustive or not. Some commentators claim that the list is exhaustive;[1163] others claim the opposite, primarily due to the subsequent inclusion in Art 8(5) of data relating to 'criminal convictions' etc.[1164] In my opinion, the latter point is scarcely decisive of the issue: although para 5 is described (in para 6) as a derogation from para 1, it appears on its face to be quite independent of para 1. Moreover, the wording of para 1 itself does not indicate any intention that the data types listed therein are mere instances of a broader set of data. Recital 13 describes the data in para 1 as 'data which are capable by their nature of infringing fundamental freedoms or privacy'. Certainly, within given cultural-legal contexts, it is possible to apply such a description to some types of data not listed in para 1; but there is no indication in recital 13 (or the *travaux préparatoires*) that the Directive treats this description as allowing for an extension of the para 1 data types.[1165]

At the same time, the loose way in which these data types are formulated makes it possible to interpret them broadly. Moreover, the fact that determination of sensitivity tends to be coloured by context requires a softening of any fixed, relatively *a priori* division of data into sensitive and non-sensitive categories. In certain situations, data that are ordinarily non-sensitive will become sensitive and/or regulated by provisions dealing with ordinarily sensitive data on account of their being drawn into a system for processing the latter type of data. A pertinent example here would be address data for medical patients.

Determining which data ordinarily fall within the categories listed in Art 8(1) will not always be easy. If, for example, a person purchases an information product concerning a certain religious or sexual theme, and the product is registered against the purchaser's name (or pseudonym or other unique identifier), it could be argued that sensitive data about the purchaser have thereby been processed. Yet it could also be argued that the link between the product's theme and the purchaser's personality in such a case is too loose: ie, just because a person buys the product does not necessarily mean that the product reflects the person's own taste; he/she may simply be sampling or analysing a range of products or buying the product for someone else. The strength of this argument is dependant on several factors, including the nature of the product (eg, an academic treatise on satanism will tend to say less about the

1163 See, eg, Blume, *Personregistrering*, *supra* n 93, 297.

1164 See, eg, D Bainbridge & G Pearce, 'The Data Protection Directive: A Legal Analysis' [1996] 12 *CLSR*, 160, 163.

1165 From the Council minutes, the intention of both the Council and Commission appears to be that Member States, in the light of their respective legal and social circumstances, may specify data categories that are an *elaboration* of the categories in para 1 ('eg data relating to genetic identity, party-political membership, physical health, personal persuasion, lifestyle etc'), but that States may not introduce totally new data categories: see declaration 11 of the Council minutes, set out in Blume, *Personregistrering*, *supra* n 93, 432.

purchaser's personal religious inclinations than, say, a video-clip depicting satanistic rituals for the purpose of viewer entertainment) and the nature of the transaction (eg, a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products on a similar theme).[1166]

Article 8(7) permits EU Member States to determine largely as they see fit 'the conditions under which a national identification number or any other identifier of general application may be processed'. Such PINs are useful, though by no means indispensable,[1167] for linking data from various sources and thereby generating profiles. This is one important reason why their utilisation has been of long-standing concern in data protection discourse.[1168] It also helps explain why data protection law and policy have often sought to restrict PIN utilisation.[1169] Through Art 8(7), the EC Directive again refrains from attempting to enforce the minimality principle along rigid, pan-European lines with respect to a type of data processing that has special significance for profiling. At the same time, the Directive's stance on this point is scarcely surprising given that the issue of how best to regulate use of PINs is a vexed one from a data protection perspective. While PINs are by no means indispensable for profile creation, they will tend to improve the quality (validity) of the profiles generated (assuming, of course, that the PINs are relatively unique to the person they identify) – an improvement that can benefit some of the data protection interests of data subjects,[1170] though indirectly detract from other of these interests.

1166 See also Bygrave & Koelman, *supra* n 316, 79.

1167 See espec *Personregister – Datorer – Integritet*, SOU 1978:54, 96 (citing Swedish studies showing that data linkage carried out on the basis of personal names, dates of birth and/or addresses is nearly as accurate as linkage carried out using a multi-purpose PIN).

1168 See *supra* n 340 and references cited therein. Another important reason, though, concerns the alienating effect of PIN utilisation on the way in which we wish to perceive our human individuality: see, eg, RA Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7 *Information Technology & People*, 6, 30; Bing, *supra* n 349, 69.

1169 See, eg, the restrictive line taken by the Norwegian Data Inspectorate and Ministry of Justice in this regard, as illustrated by cases 84/734, 84/301, 85/505, 82/505, 87/821, 92/296, 93/1619, 93/1386 (set out in Bygrave, *supra* n 37, 42–43, 55–58, 74–78, 170–171).

1170 Cf cases 92/2967, 93/1619 and 93/1386 (described in Bygrave, *supra* n 37, 170–171) dealt with by the Norwegian Data Inspectorate and Ministry of Justice. These cases concerned requests by two telecommunications companies to register their customers' respective official PINs ('birth numbers') so as to ensure accurate customer identification and thereby reduce the possibility of swindle. Both the Inspectorate and Ministry (on appeal) refused to accede to the requests. The Ministry, however, recognised that the registration of the PINs would significantly help the companies to reduce swindle and, by ensuring accurate identification, would help to protect the privacy and integrity of innocent customers. Nevertheless, it decided to place more weight on the fact that such registration would be viewed by most people as involving a violation of their integrity. Before allowing registration, the Ministry stated, there would need to be better public awareness of what 'birth numbers' are and how they can be used to protect the integrity of individuals. For further elaboration on the privacy-enhancing potential of PIN utilisation, see, eg, P Redfern, 'Precise Identification through a Multi-Purpose Personal Number Protects Privacy' (1994) 1 *Int J of Law and Information Technology*, 305,

Last but not least, the minimality principle is manifested in rules requiring anonymity of persons in certain contexts. The most common type of such rules in data protection laws is exemplified by Art 6(1)(e) of the EC Directive which provides for the anonymisation of personal data once the need for person-identification lapses; ie, personal data must be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. Derogation from this requirement is permitted, though, with respect to data processing for 'historical, statistical or scientific purposes', if EU Member States provide 'appropriate safeguards'. Recital 29 states, ia, that such safeguards 'must in particular rule out the use of the data in support of measures or decisions regarding any particular individual'.

The provisions in Art 6(1)(e) stand in contrast to the more far-reaching requirements for transactional anonymity laid down in Germany's *Federal Data Protection Act*. Section 3a of the Act provides that '[t]he design and selection of data processing systems shall be oriented to the goal of collecting, processing or using no personal data or as little personal data as possible'. Further, it provides that 'use is to be made of the possibilities for anonymisation and pseudonymisation, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection'. Similarly, Germany's *Teleservices Data Protection Act* stipulates that a teleservice provider 'shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable' and that the user 'shall be informed about these options' (s 4(6)).[1171] This requirement is reinforced by several other provisions.[1172]

Rules such as s 3a of Germany's *Federal Data Protection Act* are currently rare, at least within data protection laws.[1173] It is perhaps plausible, though, to argue that Art 6(1)(e) of the EC Directive, in conjunction with the stipulations in Arts 6(1)(c), 7 and 8, already embody a general principle requiring that there be transactional anonymity unless overriding legitimate interests exist to the contrary. More

---

(Cont.)

317–319. See too s 12(2) of Norway's *Personal Data Act* of 2000 (the Data Inspectorate may instruct a data controller to use means of identification in order to ensure adequate quality of personal data).

1171 The criterion 'anonymisation' is defined in s 3(6) as 'modification of personal data so that the information concerning personal or material circumstances can no longer be attributed to an identified or identifiable individual or only with a disproportionately great expenditure of time, money and labour'. The criterion 'pseudonymisation' is defined in s 3(6a) as 'replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult'.

1172 See espec ss 4(4) and 6(5) set out above in section 18.3.2.

1173 Express provision for anonymity is made also in NPP 8 in Schedule 3 to Australia's *Federal Privacy Act* and IPP 8 in Schedule 1 to the *Information Privacy Act 2000* of the Australian State of Victoria ('Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation').

tenuously, such a principle could also be read as implying that active consideration be given to crafting technical solutions for ensuring transactional anonymity.[1174]

We find an increasing number of policy documents in which transactional anonymity is expressly promoted. These policy documents originate from a broad range of organisations, including the CoE,[1175] Data Protection Working Party,[1176] and Information Infrastructure Task Force set up by the Clinton Administration in the USA.[1177] The documents' recommendations on anonymity can be expected to influence the drafting of future data protection laws, at least in relation to certain sectors of activity.

In relation to the telecommunications sector, the EC Directive on telecommunications privacy seeks to limit the registration and dissemination of personal data along lines that are broadly similar to the thrust of Germany's *Teleservices Data Protection Act*. Although the Directive does not contain provisions equivalent to s 4(6) of the German Act, one of its basic points of departure is that traffic data on telecommunications users/subscribers which are processed to establish 'calls' must be erased or made anonymous upon termination of the calls (Art 6(1)). Article 6(2) of the Directive permits service providers to process only such data on users/subscribers as are necessary for billing purposes and interconnection payments. This processing is 'permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued' (Art 6(2)). Further, the data may only be used for the purpose of marketing the provider's own services if the subscriber has consented (Art 6(3)).

The coming Directive on privacy of electronic communications contains equivalent rules (see Art 6), though these apply to a broader class of traffic data[1178] and stipulate subscriber/user consent not just when the data are to be used for the purpose of marketing but for the purpose of providing 'value added services' (Art 6(3)). The latter concept is broadly defined as 'any service which requires the processing of traffic data or location data … beyond what is necessary for the transmission of a communication or the billing thereof' (Art 2(g)). Most

---

1174 Some support for these claims can be indirectly derived from recital 30 in the preamble to the coming EC Directive on privacy of electronic communications: see further below.

1175 See, eg, *Recommendation R (83) 10 on the Protection of Personal Data used for Scientific Research and Statistics* (adopted 23.9.1983), para 2.2: 'Whenever possible, research should be undertaken with anonymous data. Scientific and professional organisations, as well as public authorities, should promote the development of techniques and procedures securing anonymity'.

1176 See, eg, Recommendation 1/99, *supra* n 1073, stating, ia, that '[t]he configuration of hard- and software products should not, by default, allow for collecting, storing or sending of client persistent information [ie, 'information related to the client (the user's PC) and remaining longer than one session on the computer equipment']'.

1177 See Principles for Providing and Using Personal Information, adopted 6.6.1995 (<http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>), Principle III.B.4 of which stipulates that '[i]ndividuals should be able to safeguard their own privacy by having … [t]he opportunity to remain anonymous when appropriate'.

1178 See *supra* n 782 and accompanying text.

significantly, recital 30 in the preamble to the Directive explicates these rules by stating:

> 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users …'

All of the above provisions obviously impinge significantly on the ability of (tele)communications service providers to both generate and apply specific profiles of their customers. They will thereby impinge also on the ability to generate (though not necessarily apply) abstract customer profiles.

18.4.4 PRINCIPLE OF INFORMATION QUALITY

The extent to which profiling results in unfair or unwarranted treatment of data subjects, and the extent to which profilers realise the advantages they envisage from profiling, depend largely on the quality of the profiling operations concerned.[1179] More specifically, what is at stake is the validity (accuracy, etc) of the profiles generated, along with their utility (relevance, etc) in relation to the purposes for which they are applied. Thus, an important issue is to what degree rules in data protection laws contribute to ensuring adequate quality of profiling operations, particularly from the viewpoint of the data subjects.

Two provisions in the EC Directive stand out as especially pertinent to this issue: Arts 6(1)(c) and 6(1)(d).[1180] The former provision stipulates that personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. Article 6(1)(d) requires that personal data be 'accurate and, where necessary, kept up to date'; further, 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete ... are erased or rectified'. Both provisions complement and are complemented by the principle of purpose specification laid down in Art 6(1)(b) and described in section 18.4.2.

The criteria of accuracy in Art 6(1)(d) and adequacy in Art 6(1)(c) have to be read as embracing the dimensions of precision, comprehensiveness and correctness – as defined in Chapter 7 (section 7.2.5)[1181] – if they are not to be found wanting in

---

1179 See further Chapter 17 (section 17.3).

1180 Note also the rectification right laid down in Art 12(b), dealt with in section 8.4.5.

1181 Precision refers to the level of detail at which data describe or define the RWO they are intended to describe or define; comprehensiveness refers to the extent to which all data that are necessary to

their coverage of the interest in data validity. Both criteria are conceptually/logically capable of covering all of these dimensions without much problem. At the same time, it is noteworthy that Art 6(1)(d) supplements reference to the accuracy criterion with references to an up-to-dateness criterion and, more indirectly, a criterion of completeness (which would seem to equate with comprehensiveness). These additions are probably in order to draw out, for the benefit of both data controllers and data subjects, the various dimensions of data quality. As such, they play a useful role given the rather woolly meaning of the terms 'accurate' and 'adequate'.[1182]

What is problematic – at least from the viewpoint of data subjects – is that Art 6(1)(c) links the adequacy and relevance criteria merely to the purposes for which data are to be processed, without qualifying these purposes by reference to the needs of data subjects. The same sort of dynamic occurs in Art 6(1)(b) with respect to the criterion of compatibility/non-incompatibility. On the face of these provisions, it is largely left up to the data controllers to define the purposes of processing; thus, controllers *prima facie* determine the levels of adequacy, relevance, etc which are required. In other words, the provisions appear to operate with a criterion of controller-internal efficiency. This does not present any problems for data subjects if the levels of adequacy, etc required by data controllers are commensurate with the data protection needs of data subjects. However, such commensurability cannot be assumed.[1183] It is probable, though, that the fairness criterion in Art 6(1)(a) implicitly requires levels of adequacy, etc to be such as to ensure that data subjects are not significantly affected by weaknesses in the quality of the data. Even so, the failure to spell out this requirement in Arts 6(1)(c) and 6(1)(b) is problematic both in terms of legal certainty for data controllers and data protection for data subjects.[1184]

It is especially problematic since these sorts of provisions are the closest the Directive and most other data protection laws get in terms of addressing data controllers' cognitive quality – more specifically, the quality of controllers' comprehension of: (i) the nature of the problems/tasks for which they process data; and (ii) the quality (adequacy, relevance, etc) of the data they process to address these problems/tasks. This cognitive quality plays an important part in determining the extent to which the outcomes of profiling are fair and just for data subjects (and/or conform with the expectations of data controllers).[1185] The material presented

---

(Cont.)
represent the RWO are present; while correctness refers to the extent to which the correspondence between the data and RWO is error-free.

1182 Cf Switzerland's federal *Data Protection Act* which merely mentions the need for 'Richtigkeit' in its central provision (Art 5(1)) addressing data quality.

1183 See further Chapter 7 (section 7.3).

1184 Cf section 8(1) of the Norwegian PDRA (repealed) which stipulated, ia, that incorrect or irrelevant data be amended, deleted or supplemented 'insofar as the inadequacy ['mangelen'] can *significantly affect* ['få betydning for'] the data subject' (emphasis added).

1185 See further Chapter 17 (section 17.3).

in Chapter 6 (section 6.2.3)[1186] points to the possibility of such cognitive quality being sometimes, if not frequently, insufficient to ensure fairness of profiling outcomes for data subjects.

Moving to the stringency with which the EC Directive requires checks on the validity of personal data, the standard set by Art 6(1)(d) is in terms of 'every reasonable step must be taken'. The reference to 'reasonable' implies that data controllers are permitted to take into account cost and resource factors when deciding upon measures to erase or rectify data. Yet it implies also that such factors have to be counter-balanced by consideration of other factors, such as the purposes for which the data are to be used and the potential impact of poor data quality on the data subject(s). Less certain is the extent to which Art 6(1)(d) requires data controllers to check *regularly* the validity of data *in advance* of evidence of data error. The reference in the provision to the need for up-to-dateness could signal that data quality should be checked regularly. If so, the signal is not especially perspicuous. This relative lack of certainty may be contrasted with the 'principle of accuracy' (principle 2) in the UN Guidelines which emphasises the duty of data controllers to carry out *regular checks* of the quality of personal data.[1187] Unfortunately, many other data protection instruments, including the OECD Guidelines and CoE Convention, do not explicitly address the issue of quality checks at all (though their requirements that personal data 'should' or 'must' be of a certain quality imply the need for some sort of checking system).[1188]

This failure to provide substantial guidance on the character of quality controls reduces legal certainty for data controllers. It might also be taken advantage of to reduce levels of protection for data subjects. Such a failure goes hand-in-hand with the tendency for data protection laws to address many of the quality dimensions of information systems – in particular, IS manageability, robustness, accessibility, reliability and comprehensibility – in an indirect way only.[1189] This tendency is also problematic in terms of ensuring adequate data protection for data subjects. The rapidly increasing exploitation of personal data as evidenced by, for instance, the

---

1186 Recall particularly the controversial data-matching operation undertaken by Kungsbacka municipality in Sweden.

1187 Principle 2 reads in full: 'Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed'.

1188 Some laws, nevertheless, have set down specific and seemingly stringent checking requirements. See, eg, Art 26(1) of Luxembourg's Act of 1979: '[o]wners and managers of data banks *must make every effort* to keep their contents up to date, correct inaccurate data and delete obsolete data or data obtained by unlawful or fraudulent means' (emphasis added). Cf the apparently more lenient rule in s 8(1) of Sweden's *Data Act* of 1973 (repealed): 'Should there be *cause to suspect* that personal information ... is incorrect or misleading' then the data controller 'shall institute an inquiry without delay'.

1189 See further Chapter 7 (section 7.2.5).

emergence of a profiling industry, inevitably puts strains on the ability of information systems to perform in ways that accord with the data protection interests of data subjects (and the expectations of data controllers).

Few provisions in the EC Directive (and most other data protection laws) deal specifically with the quality of profiling. The one major exception to this pattern is provisions like Art 15(1) of the Directive (dealt with in section 18.3.1). These sorts of provisions can be viewed as reflecting, ia, scepticism to the utility (especially completeness) of fully computerised assessments of human personality. However, the reach of such provisions is narrow and their current practical impact fairly marginal.[1190] Moreover, they encourage (manual) assessment of the quality of fully automated profiling in an indirect manner only. This comment applies *a fortiori* with regard to the *creation* of profiles.

The paucity of provisions dealing specifically with the quality of profiling is mirrored by the failure of many data protection laws to expressly require data controllers to check the validity of personal opinions and other assessments before utilising them. However, there do exist instances of such requirements in policy documents which can serve as useful models for future legislation.[1191]

Finally, we must not overlook the fact that Art 6(1)(c) and 6(1)(d) – like Art 6(1)(b) and the rest of the Directive – are only directed at 'personal' data; they do not require anything of the quality of non-personal data (eg, group/aggregate data). This severely diminishes their ability to ensure adequate quality of profiling operations since profiles (primarily abstract profiles but possibly also elements of specific profiles) are often built up using non-personal data.

18.4.5 PRINCIPLE OF DATA SUBJECT PARTICIPATION AND CONTROL

The extent to which the outcomes of profiling operations will detrimentally affect data subjects is partly determined by the extent to which the latter are made aware of the operations and given an opportunity to influence them.

Data subject awareness of profiling operations can be promoted by a variety of rules. One such set of rules are those requiring data controllers to communicate to data protection authorities basic details of their processing of personal data, combined with a requirement that this information be stored by the authorities in a

---

1190 See further Chapter 19.

1191 See, eg, para 5.5.ii of CoE *Recommendation R (87) 15 Regulating the Use of Personal Data in the Police Sector* (adopted 17.9.1987): 'As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and *data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated*' (emphasis added).

publicly accessible register. These rules are laid down in, ia, Arts 18, 19 and 21 of the EC Directive.[1192]

Another, arguably more important, set of rules are those requiring data controllers to inform data subjects *directly* about basic details of their processing operations. In the Directive, these rules are laid down in Arts 10–11. Article 10 provides that when data are collected from the data subject, he/she must be informed of 'at least' the identity of the data controller and the latter's representatives, together with the intended purposes of the data processing (unless the data subject already has this information); other types of information may also be provided insofar as is 'necessary' in the circumstances 'to guarantee fair processing in respect of the data subject'. Article 11 contains broadly similar requirements in cases when data are not collected directly from the data subject.

Unfortunately, the Directive fails to specify *when* information is to be provided pursuant to Art 10. By contrast, the information to be provided pursuant to Art 11 is expressly required to be provided either when the data are recorded or, if disclosure of the data to a third party is envisaged, no later than the time of the first disclosure. Given that Art 10 aims at ensuring 'fair processing in respect of the data subject', the information should presumably be provided before or at the time of data collection.

A third set of relevant rules in this context are those providing access rights to data subjects. The central provision here is Art 12 of the Directive:

> 'Member States shall guarantee every data subject the right to obtain from the controller:
>
> (a) without constraint at reasonable intervals and without excessive delay or expense:
>
> – confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
>
> – communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
>
> – knowledge of the logic involved in any automated processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1).'

1192 Described in Chapter 4 (sections 4.2–4.3).

The right of access in Art 12 goes further than the duty-of-information provisions dealt with above by specifically mentioning a right to knowledge about the logic behind certain automated data-processing operations.[1193]

At the same time, Art 13(2) allows derogation from Art 12 with respect to personal data that are 'processed solely for purposes of scientific research' or kept no longer than 'necessary for the sole purpose of creating statistics', but only where these data are '[s]ubject to adequate legal safeguards' and 'there is clearly no risk of breaching the privacy of the data subject'. Further derogations to Art 12, along with Arts 10–11 and 21, are allowed pursuant to Arts 9 and 13(1), while Arts 18–19 may be restricted pursuant to Art 9.[1194]

The ability of the above three sets of rules to promote data subject awareness of profiling operations is subject to two significant limitations. The first limitation is that the rules fail to extend, at least expressly, in any significant way to non-personal data (eg, group/aggregate data). As stated at numerous points above, such data tend to form the basis for abstract profiles and possibly also elements of specific profiles. The second limitation is that the rules fail to require, at least expressly, that persons be given information specifically about profiling practices affecting them. It is possible, though, to read into Arts 10–12 a requirement for the supply of some such information pursuant to the fairness criterion in Arts 10, 11 and 6(1)(a). As pointed out in section 18.4.1, this sort of requirement could arise when the profiling practices involve at least some processing of personal data and impinge significantly on the data protection interests of the data subjects. However, it is difficult to determine in the abstract exactly what sort of information would need to be given pursuant to such a requirement, in addition to the categories of information already listed in Arts 10–12. Arguably, the classes of information listed in s 21 of the Norwegian *Personal Data Act*, as described in section 18.3.4 above, would need to be supplied; ie, the data constituting the profile and the source(s) of these data (in addition to the identity of the profiler). The fairness criterion – especially when construed in the light of Art 12(a) and recitals 9–10[1195] – could also require in some circumstances supply of information about the assumptions or logic behind the profile.[1196]

Section 21 of the Norwegian PDA is not the only provision against which Arts 10–12 of the Directive can be instructively compared. Several of the provisions of Germany's *Teleservices Data Protection Act* are worth canvassing too. In addition to making provision in 4(7) for ordinary data access rights,[1197] the Act places a teleservice provider under a duty to inform users about aspects of its data-processing

---

1193 The latter right is no doubt inspired by s 3 of the French Act of 1978 which provides: 'Any person shall be entitled to know and to dispute the data and logic used in automatic processing, the results of which are asserted against him'.

1194 See further section 18.4.6.

1195 See *supra* n 135.

1196 Cf s 21 of the Norwegian PDA under which such information does not need to be given.

1197 Use of the adjective 'ordinary' is somewhat misleading as s 4(7) extends to data on pseudonyms.

operations on its own accord. This duty of information elaborates upon and extends what is required on the face of Arts 10–11 of the Directive. Section 4(1) stipulates that, '[i]n case of automatic processing, which *permits subsequent identification* of the user and which *prepares* the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure' (emphasis added). Although this provision seems primarily intended to address cookies mechanisms and the like,[1198] it could, on its face, be applied also to the generation of abstract profiles insofar as the process results in subsequent identification of a teleservice user and prepares the processing of personal data. Another innovative rule is s 4(6) stipulating that a teleservice user be informed of whatever options exist for making anonymous or pseudonymous use and payment of teleservices. All of these stipulations could be read into Arts 10–11 of the Directive on the basis of a liberal interpretation of the fairness criterion.

The coming EC Directive on privacy of electronic communications also expands Arts 10–11 of the Directive in somewhat similar ways to the German legislation. It requires Member States to ensure 'that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user receives in advance clear and comprehensive information, inter alia about the purposes of the processing …' (Art 5(3)). The preamble states that this requirement extends to the use of 'spyware, web bugs, hidden identifiers and other similar devices' which may, ia, 'trace the activities of the user' (recital 24), and to the use of 'cookies' (recital 25). Further duties of information are laid down with respect to:

- network security risks and means ('for instance … using specific types of software or encryption technologies': recital 20) to remedy such risks (Art 4(2));
- processing of traffic data (Art 6(4));
- processing of geographic location data (Art 9(1)); and
- functioning of subscriber directories (Art 12(1)).

As for rules promoting the ability of data subjects to influence profiling operations, these are mainly of two kinds:

1) rules providing data subjects with a right to demand that invalid or illegally processed data on themselves be rectified or deleted by the data controllers;
2) rules providing data subjects with a right to object to others' processing of data on themselves.

In the context of the EC Directive, the first category of rule is laid down in Art 12(b). This provision complements the rules on information quality in Arts 6(1)(c) and 6(1)(d). In terms of addressing the quality of profiling, it suffers from the same weakness as the rest of the Directive in that it applies only to personal data.

1198 Engel-Flechsig, *supra* n 784, 12; *Gesetzentwurf*, *supra* n 786, 22.

The second category of rules is found spread over several provisions in the Directive. First, there is the very general provision in Art 14(a) which states that, 'at least in the cases referred to in Article 7(e) and (f)',[1199] a data subject is to be given the right

> 'to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.'

Article 14(a) is essentially a default provision; ie, the right to object provided by it will only eventuate in the absence of contrary national legislation. Its practical impact on national laws and, accordingly, profiling practices covered by these laws, is highly uncertain.

Secondly, there are the provisions in Arts 7 and 8(2) – set out in section 18.4.3 – which prohibit processing of personal data without the informed consent of the data subjects. The extent of data subject empowerment flowing from these provisions is diminished by the fact that consent is just one of several alternative prerequisites for processing, though this reduction in empowerment is considerably less in relation to the processing of the classes of data listed in Art 8.[1200] As pointed out in section 18.4.3, just how much profiling based on the processing of personal data will be able to escape these consent requirements is very difficult to determine at this stage.

A greater degree of data subject empowerment, and a greater degree of certainty in terms of how such empowerment will impact on profiling, flows from Art 14(b). This provision specifically addresses the right of data subjects to object to direct marketing. Here Member States are to provide data subjects with two options:

1) 'to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing'; or
2) 'to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses'.

Further, Member States are required to take 'necessary measures to ensure that data subjects are aware of' the right to object pursuant to Art 14(b). This right to object does not provide data subjects with a possibility of influencing the generation of profiles (abstract or specific), but it does provide them with a possibility of influencing the application of profiles (primarily specific and, secondarily, abstract) for direct-marketing purposes.

1199 See section 18.4.3 above.

1200 See further the relatively detailed analysis of the reach of these consent requirements (albeit in the context of digital rights management systems) in Bygrave & Koelman, *supra* n 316, 75 ff.

The right in Art 14(b) is followed up in Art 6(3) of the EC Directive on telecommunications privacy: data on telecommunications users/subscribers which are processed to establish 'calls' may only be used for the purpose of 'marketing' the services of the telecommunications service provider if the subscriber has consented. The coming EC Directive on privacy of electronic communications is more restrictive by applying a consent rule also when the data are to be applied for the purpose of providing 'value added services' (Art 6(3)). Thus, under the coming Directive, users/subscribers are able to influence the application of profiles for more than strictly direct-marketing purposes.

18.4.6 GENERAL EXCEPTIONS AND DEROGATIONS

All of the core principles canvassed in the preceding sections are subject to exceptions. A reasonably representative distillation of the basic categories of these exceptions as they appear or will appear in the bulk of data protection laws is provided by the EC Directive.

To begin with, Art 9 of the Directive requires derogation from all of the Directive's provisions canvassed above, insofar as the processing of personal data 'is carried out solely for journalistic purposes or the purpose of artistic or literary expression' and the derogation is 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.

Secondly, Art 13(1) permits restriction of the scope of the rights and obligations set down in Arts 6(1), 10, 11(1), 12 and 21 (but, notably, not Art 15) insofar as is 'necessary' to safeguard:

> '(a) national security;
> (b) defence;
> (c) public security;
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
> (g) the protection of the data subject or of the rights and freedoms of others.'[1201]

1201 Many of the matters listed in Art 13(1) – notably those in paras (a), (b), (c) and, to a large extent, (d) – lie outside the Directive's ambit and the scope of EC law generally. Their inclusion in Art 13 is probably due to the possibility that data-processing activities ordinarily falling within the Directive's scope need to be exploited for, say, national security or defence purposes.

In addition, Art 13(2) allows derogation from Art 12 with respect to personal data that are 'processed solely for purposes of scientific research' or kept no longer than 'necessary for the sole purpose of creating statistics', but only where these data are '[s]ubject to adequate legal safeguards' and 'there is clearly no risk of breaching the privacy of the data subject'.

No attempt is made here to interpret the proper ambit of each of the above exemptions; such an analysis would quickly turn into a quagmire of speculation where little fruitful is gained despite lengthy effort. However, it is worth underlining the relatively obvious and uncontroversial point that the criterion 'necessary' in Arts 9 and 13 is to be construed similarly to how it is construed in relation to Arts 7 and 8 (as analysed in section 18.4.3).

How the above categories of exceptions will otherwise impact on profiling practices is far from clear. It is also difficult to see how some of them can have any extensive practical relevance for at least some such practices. This is the case, for instance, with the application of Art 9 to the sort of decision making dealt with by Art 15(1). On the latter point, however, one can envisage the emergence of a kind of automated journalism that bases its portrayals of the character of particular persons exclusively on the automated searching and combination of data from, say, various Internet sources. This sort of activity might have a chance of falling within the scope of Art 15(1), though its ability to meet the decisional criteria of the provision is uncertain.

The most important observation to be made here is that the extensive literal breadth of the exemptions in Arts 9 and 13 give EU Member States (and possibly other States) a tremendous freedom to legitimise a large range of processing activities, including profiling practices, at the complete expense of many core data protection principles. There is also a distinct likelihood of Arts 9 and 13 leading to significant disparites between the data protection regimes of the various Member States.

18.4.7 REGULATION PURSUANT TO A LICENSING REGIME

This section describes how profiling can be restricted pursuant to a licensing regime that operates with relatively few substantive rules in which the core principles of data protection, as described in the previous sections, are prominent. The licensing regime presented here is that established pursuant to Norway's repealed *Personal Data Registers Act* (PDRA).

The focus of analysis in this section differs somewhat from the focus in the previous sections. Whereas the latter concentrate primarily on the scope of core data protection principles largely irrespective of the monitoring and control regimes under which they (the principles) are applied, this section focuses primarily on the scope of a particular type of monitoring and control regime. Nevertheless, as shown below, the

restrictions on profiling instituted under this regime were often inspired and shaped by the same sorts of principles as are dealt with in the previous sections, despite the fact that some of the principles were far from prominent in the text of the PDRA.

What were the basic features of the licensing regime established pursuant to the PDRA? To begin with, the PDRA required, with some exceptions, that all personal data registers which are computerised or which contain certain kinds of extra-sensitive data (ie, data on race, political or religious beliefs, criminal offences, health, sexual life and certain family affairs: s 6(2)) must be licensed by the Data Inspectorate prior to their establishment (s 9(1)).[1202] When considering applications for licenses, the Inspectorate was to assess 'whether the establishment and use of the register in question may cause problems for the individual person which cannot be solved satisfactorily by rules prescribed under section 11 ...' (s 10). Section 11(1) empowered the Inspectorate to prescribe in detail how the licensed registers are to be used (s 11(1)). The Inspectorate was permitted to set down rules on, ia, the matching of such registers with other registers (s 11(2)(3)) and on use of the 'birth number' ('fødselsnummer') assigned to each member of the country's population (s 11(2)(4)).

A precondition for the Inspectorate issuing a license was that the data registration in question was 'justified on objective grounds ['saklig begrunnet'] having due regard to the administrative and operational activities of the institution or enterprise undertaking such registration' (s 6(1)). This criterion of objective justifiability was sharpened to one of 'necessity' when the extra-sensitive data listed in s 6(2) were sought registered (see s 6(2)).[1203]

A supplementary set of licensing requirements was provided for in chapts 5–8 of the PDRA. These required that certain types of enterprises be licensed before beginning operations. Such enterprises were credit-reporting agencies (see chapt 5), enterprises that sell or distribute addresses, advertisements and other notices (see chapt 7), enterprises that conduct market surveys and opinion polls (see chapt 8) and enterprises that carry out electronic processing of personal data on behalf of third

---

1202 There were two exceptions to the licensing rule in s 9. First, licensing was not required for registers established pursuant to other statutes (s 41). Secondly, licensing was not required for certain categories of registers set out in chapt 2 of the main regulations to the Act (*Forskrifter i medhold av lov om personregistre mm 21 desember 1979*). Examples of registers set out in chapt 2 of the regulations included: associations' registers over their members (s 2-2); registers of customers, subscribers and suppliers (s 2-3 and, in relation to banks' customer registers, s 2-4); registers for distribution of catalogues, books and similar publications (s 2-5); and personell registers (s 2-12). All such registers were to be established and used in accordance with the rules set out in chapts 2 and 3 of the regulations. These rules specified the permissible content, purpose, disclosure, matching, security and destruction of the data in the registers. With regard to matching, for example, s 3-5(1) of the regulations stipulated that this could occur only with the specific permission of the Inspectorate unless the results of the matching were not used for 'control purposes' ('kontrollformål') or for reaching decisions that were 'directed towards individuals' ('rettet mot enkeltpersoner').

1203 In practice, this necessity criterion was often supplemented by a requirement for informed and freely given consent by the data subject(s) to the registration: see, eg, cases 85/32, 87/625, 86/372, 87/792, 94/2180, set out in Bygrave, *supra* n 37, 49–51, 79–81, 86–90, 190–192.

parties (see chapt 6). In addition to being subjected to licensing conditions, such enterprises were required to comply with a small number of sector-specific rules laid down in chapts 5–8 of the PDRA (along with the more general rules in chapts 3–4 of the Act). Some of these rules proved to be of considerable importance in the regulation of the enterprises' profiling practices. With regard to credit-reporting agencies, for example, two such provisions were ss 13(1) and 15(1) – as illustrated further below. Section 13(1) defined credit-reporting activity as constituted by the reporting of data that reveal 'creditworthiness or financial reliability' ('kredittverdighet eller økonomisk vederheftighet'), while s 15(1) required credit-reporting agencies to ensure, ia, that they do not use data that can 'lay the basis for groundless or unfairly negative attitudes' ('danne grunnlag for ugrunnet eller urimelig avvisende holdning') towards the data subject(s).

Taken together, all of these rules provided the Inspectorate (and the Ministry of Justice as appeal instance) with ample opportunity to subject the planned registration and use of a great deal of personal data to a relatively broad test of social desirability. Concomitantly, they gave the Inspectorate (along with the Ministry) an extensive ability to restrict the generation and application of profiles for a relatively broad range of reasons. As shown below, this ability was exploited in a variety of contexts.

In the context of credit reporting, for instance, the Inspectorate was able to prevent the use of particular abstract profiles (and thereby the creation and use of particular specific profiles) on the ground that the profiles were insufficiently reliable as evidence of creditworthiness.[1204] In such cases, concern was shown for ensuring that the quality (validity and utility) of the profiles was sufficiently adequate to guarantee fair credit-reporting outcomes for the data subjects.

In the same context, the use of certain other abstract profiles (and thereby, again, the creation and use of certain specific profiles) was restricted in order to prevent the registers of credit-reporting agencies from becoming so comprehensive that they revealed the complete economic status of the data subjects.[1205] Concern here was not

---

1204 See, eg, case 90/1715 (set out in Bygrave, *supra* n 37, 105–106) in which the Inspectorate (and Ministry of Justice) refused to permit a credit-reporting company to register and disclose, for credit-reporting purposes, data on past applications for reports on the creditworthiness of persons/enterprises. According to the company, statistical analysis showed a correlation between the number of times a debitor asks for credit and the degree of difficulty with which a debitor can meet loan repayments. In coming to their respective decisions, both the Inspectorate and Ministry expressed scepticism towards placing weight on such statistical correlations; the latter, they held, would not be sufficiently reliable to be of real relevance for assessing creditworthiness. Hence, any registration and use of the data for credit-reporting purposes was found to be in breach of ss 13 and 15 of the PDRA.

1205 See, eg, case 96/1324 (reported in St meld 44 (1998–99), *Datatilsynets årsmelding 1998*, 28) concerning an application by credit-reporting agencies to register and apply data on car ownership for the purposes of assessing creditworthiness. Both the Inspectorate and Ministry rejected the application, holding that the registration and use of such data would bring credit-reporting agencies perilously close to being able to reveal the 'total economic situation' ('totale økonomiske situasjon') of data subjects: see letter of 29.12.1998 from the Ministry to the Norwegian Association of Credit-

only directed at upholding the data subjects' privacy-related interests; it was also directed at discouraging the automation of credit-reporting operations, thereby helping to ensure, once again, fairness in profiling outcomes for the data subjects.

More generally, the Inspectorate took a restrictive attitude to matching operations.[1206] This was especially so with respect to matching initiated for control purposes. Behind this restrictive attitude lay, in part, a formal concern to uphold the purpose specification principle, which matching can often breach.[1207] This concern, however, was symptomatic of other concerns – most notably, a desire to ensure that persons are not subjected to unwarranted suspicion or pressure due to poor information quality or poor cognitive quality, and a desire to ensure that overall levels of citizen transparency and, obversely, societal control do not become excessive. At the same time, the Inspectorate allowed matching operations for control purposes to go ahead under certain conditions. The most significant of these conditions were:

1) the matching does not violate existing laws;
2) the matched data are valid and refer to the same person/object/value (such that any 'hits' are valid and useful);
3) the matching is able to achieve its aims;
4) these aims are legitimate and cannot be fulfilled by use of other means less detrimental to the data protection interests of the data subjects;
5) any 'hits' are checked for error before being used against the data subjects;

(Cont.)
Reporting Agencies (Norske Kredittopplysningsbyråers forening); and letter of 15.09.1998 from the Inspectorate to the Ministry. In the opinion of both bodies, such a possibility would also open up for an increasing degree of automation in the process of credit reporting, at the expense of data subject involvement in the process. This would undermine, in turn, the thrust of s 15(1) of the PDRA (set out above). Moreover, the Inspectorate held that the planned use of the data would violate the purpose specification principle insofar as the data were obtained from the government-run Central Automobile Register (Motorvognregisteret), which is maintained for administrative purposes only. The Ministry, however, refrained from addressing this point.

1206 Thus, the standard license conditions issued by the Inspectorate usually prohibited any matching of the data in the licensed register with other data except when expressly permitted by the Inspectorate. It has been asserted that the Inspectorate's attitude to matching has become less restrictive in recent years: see H Egede-Nissen, 'Brukernes epoke', in P Gottschalk (ed), *IT nest TI. Informasjonsteknologi de neste ti år* (Oslo: Ad Notam Gyldendal, 1993), 255, 260. However, I have not found any solid evidence supporting this assertion. See further LA Bygrave, 'Informasjon som felles ressurs – mulige konsekvenser for regelverk som berører personvern', in *Informasjonsteknologi og nye medier i den offentlige informasjonens tjeneste* (Oslo: Norges forskningsråd, 1996), 69, 79–80.

1207 The principle has constituted a cornerstone for Inspectorate policy, even though it was not expressly laid down in the PDRA: see, eg, St meld 18 (1992–93), *Årsmelding for Datatilsynet 1991*, 5.

6) persons affected by the matching are informed about it and, in some cases (usually when the matched data were classified as sensitive pursuant to s 6(2)), have consented to it.[1208]

Through its extensive regulation of matching operations, the Inspectorate has been able to restrict the generation and application of profiles, including abstract profiles, in a variety of contexts. One such context, for example, is law enforcement;[1209] another such context is sociological research.[1210] It should be stressed that, in these cases (as opposed to the credit-reporting cases described above), the limitations on profiling have tended to arise incidentally to limitations on matching. Nevertheless, through these limitations, the Inspectorate has also hindered the possible generation of multiple specific profiles and the re-elaboration, modification and/or confirmation of the original abstract profiles. Similar sorts of obstacles have been laid through the Inspectorate's restrictive attitude to certain other data-processing operations, including the use of birth numbers[1211] and commercial exploitation of personal income data.[1212]

1208 See further, eg, St meld 23 (1985–86), *Datatilsynets årsmelding 1984*, 15–16; St meld 43 (1990–91), *Om personvern – erfaringer og utfordringer og om Datatilsynets årsmelding for 1990*, 46–47; St meld 18 (1992–93), *Datatilsynets årsmelding 1991*, 10–11. See also, eg, cases 91/1563 & 94/2180 (set out in Bygrave, *supra* n 37, 126–129, 190–192), along with case 93/0185 presented *infra* n 1211.

1209 See, eg, case 94/1776, set out in Bygrave, *supra* n 37, 228–231. The case concerned plans in 1995 by the Norwegian Broadcasting Corporation (Norsk Rikskringkasting – NRK) to match its register of persons who have paid television license fees with a register (maintained by the main Norwegian telecommunications company, Telenor) of persons who have telephones. The aim of the planned matching operation was to identify persons who have telephones but do not pay television license fees. These persons were to be subsequently sent a letter requesting that they examine whether or not they have paid their television license fees and to pay up if necessary. The planned matching operation was based on a type of abstract profile: those who have telephones are very likely to have television sets. The Data Inspectorate refused to permit the planned operation to go ahead for several reasons. One reason was the Inspectorate's view of the planned operation as involving a type of control that many of those persons who would receive letters could find offensive, especially given that the profile concerned could not be totally accurate. This view was shared by the Ministry of Justice on appeal.

1210 See, eg, case 93/0185 (set out in Bygrave, *supra* n 37, 172–174) concerning plans in 1993 by a group of social scientists to match personal data in order to find what correlation exists between the learning problems of school pupils and subsequent adult criminality. The Inspectorate laid down as a precondition for permitting the plans to proceed that the data subjects first consent (in writing) to the matching – a precondition that was upheld by the Ministry of Justice on appeal. This precondition effectively killed the project.

1211 See *supra* nn 1170–1171 and cases cited therein.

1212 See, eg, case 94/1199 (set out in Bygrave, *supra* n 37, 186–187) in which the Inspectorate and Ministry refused to allow a company engaged in mail distribution and marketing to insert data on personal income in its address register so that it could increase service efficiency. See also cases 92/1879, 93/296, 94/668 (set out in Bygrave, *supra* n 37, 123–125, 162–167) in which the Inspectorate and Ministry placed restrictions on electronic access to income data held by the tax authorities. Cf the inconsistent line taken by the Ministry in cases 93/2443 & 94/492 (set out in Bygrave, *supra* n 37, 144–148, 160–161).

Although the regulatory controls outlined above were instigated pursuant to legislation that is now repealed, similar controls are likely to persist under the *Personal Data Act*. This is not just because the new legislation incorporates as substantive provisions the core principles that were applied by the Data Inspectorate (and Ministry of Justice) pursuant to the licensing regime of the old Act. Just as significant is the fact that the new legislation retains licensing requirements with the potential to apply to a considerable number of profiling practices. As noted in Chapter 4 (section 4.2), s 33 of the PDA requires that the processing of sensitive data[1213] be licensed, albeit with some exceptions.[1214] The Data Inspectorate is also empowered to determine on a case-by-case basis that other data-processing operations require licensing when they 'obviously infringe weighty privacy/data protection interests' ('åpenbart vil krenke tungtveiende personverninteresser') (s 33(2)). An indication of what such interests may involve is provided in s 1(2), which elaborates the need for 'personal integrity', 'private life' and 'adequate quality of personal information' as figuring amongst 'fundamental privacy/data protection concerns' ('grunnleggende personvernhensyn'). Thus, the Inspectorate retains the ability to subject numerous profiling practices (and related data-processing operations) to a relatively open-ended assessment based on a broad test of social desirability.

1213 These being data on a person's racial or ethnic origin, political, religious or philosophical beliefs, criminal record, trade-union membership, health or sex life (s 2(8)).

1214 Exemptions apply when the data subject voluntarily supplies the data or the processing is carried out by a government agency pursuant to statutory authorisation (s 33(1)) or the processing consists of video surveillance for the purposes of crime control (s 37(2)).

19. Concluding Remarks on Part IV

From the preceding chapters of Part IV, we see an increase in the intensity, sophistication and ambition of organisational profiling practices, at least in certain fields (eg, marketing, credit assessment, insurance, crime control). Within these fields, profiling is no longer simply a relatively informal, non-systematic process; it is rapidly becoming an industry in its own right. Driving this development are the same sorts of factors – described in Part II – as are driving growth in electronic interpenetration generally.

While this development has obvious benefits for the profilers, and for data subjects and society in general, it also carries major risks from a data protection perspective. It tends to augment the transparency of data subjects, thereby undermining a large number of their privacy- and autonomy-related interests. Concomitantly, it tends to undermine broader societal interests in, eg, plurality, democracy and balanced control.

At the same time, the extent to which the touted benefits of organisational profiling practices are realised will depend on the quality of the informational and cognitive elements constituting these practices. The quality of such elements will also bear upon the extent to which the profiling results in unfair or unwarranted treatment of the data subjects.

One is almost always entitled to set a question mark against the quality of these elements, as profiles are basically a set of assumptions born(e) on the stilts of probability equations. The risk of profiling error is heightened by several tendencies. First, profiling frequently involves the re-purposing of data. Some of these data could be invalid, incomplete or irrelevant in relation to what the profile is intended to represent or the purposes it is supposed to serve. Moreover, profiling is increasingly automated. Thus, it often occurs without any corrective input from data subjects; indeed, it is often relatively invisible or incomprehensible to them. The latter tendency is a problem in itself from a data protection perspective.

Paradoxically, some of the rules of data protection laws can indirectly heighten the risk of profiling error. Stringent application of rules embodying the minimality principle can contribute to the generation and misapplication of relatively coarse-grained profiles, at least when the profilers combine a high degree of inferential ambition with ignorance or incomprehension of rules embodying the principle of information quality. This is just one of numerous ways in which organisational profiling practices put the rules and principles of data protection laws to the test.

The bulk of data protection laws appear to have been enacted without legislators giving much specific consideration to profiling practices. Hence, the regulation of these practices by the laws tends to be (in the words of Clarke) 'generic, or accidental and incidental'.[1215]

Nevertheless, as implementation of Norway's PDRA illustrates, old laws providing data protection authorities with broad discretionary powers to regulate planned data-processing operations have (had) a potential to put significant limits on profiling, even if they do/did not contain provisions specifically addressing such practices. Additionally, rules embodying the core principles of data protection laws have considerable potential to restrict profiling or to reduce its detrimental effects.

A problem affecting much of this regulation is that the legislative provisions upon which it is based are often vaguely formulated; they give relatively little prescriptive guidance as to what kinds of profiling are permissible. This is particularly the case with the principle of fair and lawful processing as formulated in Art 6(1)(a) of the EC Directive. Yet also more wordy provisions are afflicted by considerable ambiguity. For instance, regarding the purpose specification principle as formulated in Art 6(1)(b) of the Directive, ambiguity inheres in the types of purposes for which data may be processed and in the meaning of the compatibility/non-incompatibility criterion. With respect to the information quality principle as laid down in Art 6(1)(c) and (d), there is considerable ambiguity in terms of the criteria by which the specified quality elements should be assessed and in terms of the steps that should be taken to monitor these elements.

Such ambiguity can be used to serve different ends. On the one hand, it provides data protection authorities with an opportunity to construe the relevant rules in an expansive, privacy-friendly manner. On the other hand, it provides data controllers with the opportunity of construing the rules in a way that favours their profiling interests – particularly in the absence of notice about any contrary lines of interpretation by the authorities.

The relatively few rules in data protection laws which *specifically* regulate profiling practices tend also to be vaguely formulated. Moreover, there is a paucity of authoritative guidance on their scope and application. As for Art 15 of the EC Directive, its efficacy as a regulatory tool is further reduced by the fact that its application is contingent upon a large number of conditions being satisfied – if one of these conditions is not met, the right in Art 15(1) does not apply. As such, Art 15 resembles a house of cards. In the context of *current* data-processing methods, this house of cards is easy to topple. However, this situation might well change in the future. Even now, though, the principle embodied in Art 15(1) is normatively important as a signal to profilers about where the limits of automated profiling should

1215 Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance', *supra* n 1031, 415.

roughly be drawn. We see also that this principle is beginning to be elaborated upon in concrete contexts, such as the assessment of worker conduct.[1216]

At the same time, though, the 'safe harbor' agreement which has been concluded between the USA and EU,[1217] and which stipulates conditions for permitting the flow of personal data from the EU to the USA, puts a question mark over the status of the Art 15 principle for non-European jurisdictions. The principle is nowhere to be found in the terms of the agreement.[1218] Other countries outside the EU/EEA could take this as a signal that they too will not be required by the EU to implement the principle. So far, legislators in these countries have shown little willingness to implement the principle of their own accord.[1219] Fortunately, though, the EU has recently made moves to amend this state of affairs by including the principle in the standard contractual clauses it has developed to govern the transfer of data to third countries that otherwise do not offer adequate data protection.[1220] I write 'fortunately' because, despite its special character relative to the bulk of other data protection rules, the principle laid down by Art 15 should be regarded as a *core* data protection principle; ie, a principle that is indispensable for defining the future agenda of data protection law and policy, and one that should therefore be embodied in most if not all future data protection instruments around the globe. Otherwise, data protection instruments risk being deprived of a significant (albeit imperfect) counterweight to the ongoing expansion, intensification and refinement of automated profiling practices.

Looking at the EC Directive more generally, our ability to reach firm conclusions as to its regulatory impact on profiling practices is hampered not just by the ambiguities mentioned above; it is also reduced by uncertainty over the ways in which the many permissible derogations to the Directive's basic rules will be applied in national data protection regimes. Most of the relevant rules analysed in Chapter 18

1216 See here the provisions of the ILO Code of Practice on Protection of Workers' Data, set out *supra* n 1085.

1217 See *supra* n 324.

1218 This is despite the opinion of the Data Protection Working Party that the safe harbour agreement should make provision for the principle. See especially 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', Working Document adopted 24.7.1998, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf>, 6–7 (cf 17). This standpoint is followed up (though rather obliquely) by the European Parliament in its Resolution of 5.7.2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Principles and related Frequently Asked Questions issued by the US Department of Commerce (A5-0177/2000), Point B(d) (stating that the data protection regimes of third countries should provide a data subject with a right to object to the processing of data on him/her 'in certain situations').

1219 For instance, no specific provision has been made for the principle in Canada's *Personal Information Protection and Electronic Documents Act* of 2000 or in Australia's *Privacy Amendment (Private Sector) Act* of 2000.

1220 See *Decision 2001/497/EC of 15.6.2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC* (OJ L 181, 4.7.2001, 19), Annex, Appendix 2, Principle 9.

– specifically those in Arts 6(1), 10, 11(1) and 12 of the EC Directive – may be subject to derogation pursuant to Art 13. Further, all of the rules in Chapter II of the Directive – more specifically, Arts 6–21 – may be subject to derogation pursuant to Art 9. These derogations are in addition to the exemptions inserted into the various rules themselves. Both the derogations and exemptions will markedly affect the extent to which profiling practices are regulated.

Besides the above ambiguities and uncertainties, other problems are apparent in the regulatory capabilities of data protection laws with respect to profiling. One such problem is that the laws tend not to apply to the processing of non-personal data, upon which profiles are frequently built. This limitation reduces their value as a means of controlling the quality of profile generation; more specifically, it reduces their ability to proactively ensure that data subjects are not subjected to unwarranted or unjust treatment on the basis of profiling.

A related problem – and one with similar consequences – is that the laws rarely address directly the quality of the *information systems* supporting profiling operations (and data processing more generally). Certainly, one can read into some of the rules (eg, those embodying the principles of fair and lawful processing, minimality, information quality and data subject participation) requirements that the systems architecture be configured such as to enable compliance with the rules. Yet otherwise the structure and design of these systems are usually taken for granted. In this regard, we can say that the rules of data protection laws tend to be systems-passive. We find, though, some exceptions to this pattern, particularly in recent German legislation. These exceptions seem to be emerging mainly around the themes of anonymity and, to a slightly lesser extent, pseudonymity. There appears to be relatively little emerging around, say, the themes of IS manageability, reliability and comprehensibility particularly with respect to the monitoring and control of data/information quality. Even the rules on anonymity vary considerably in terms of the degree to which they are systems-active; ie, positively require or encourage the (re-)configuration of information systems architecture in order to ensure a high degree of transactional anonymity (and thus reduce possibilities for at least fine-grained profiling).[1221]

In light of the above findings, I advance the following proposals. To begin with, the central rules embodying the fairness and purpose specification principles should be re-worded in order to elucidate their implicit concern for the reasonable expectations of data subjects. More specifically, these rules should be re-formulated to make clear that when information is collected and processed for a particular purpose, it should not be processed for another purpose that is not within the reasonable expectations of the data subject, unless the latter consents or the re-

1221 Compare, eg, the anonymity requirements of s 3a of the German *Federal Data Protection Act* (set out in section 18.4.3) with the relatively systems-passive requirements of anonymity formulated in the Australian legislation (*supra* n 1174). See further G Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21 *University of New South Wales LJ*, no 2, 593–622.

purposing is either legally authorised or justified by a compelling public interest. A useful point of departure for such re-formulation could be the Fairness Principle adopted by the US Information Infrastructure Task Force:[1222]

> '[i]nformation users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.'

Secondly, the central rules embodying the information quality principle should be reviewed to determine whether they adequately and consistently capture the various facets of information quality and the various facets of assuring such quality. As indicated in Chapter 18 (section 18.4.4), some variation exists between data protection laws in terms of the degree of detail with which they formulate the dimensions of information quality. Concomitantly, there is some inconsistency in terms of the terminology they employ to describe these quality dimensions and the sorts of steps to be taken in quality assurance.[1223] Overall, these rules appear to have been drafted somewhat haphazardly.

At the same time, there are dilemmas to be faced when determining the appropriate level of detail for defining these quality criteria. The more detail we add to the rules, the more complicated the rules become. Nevertheless, rules that appear simple (eg, rules which refer simply to the criterion of adequacy or accuracy)[1224] are probably too ambiguous; they have a superficial simplicity which hides considerable complexity. Such rules are probably just as confusing as rules setting out a plurality of quality attributes. In my opinion, it is best to have honest rules; ie, rules giving reasonable guidance, on their face, about what information quality and assurance of such quality involve. Information quality and quality assurance are both multifacetted. Rules on them should accurately reflect this fact, especially in view of the need for legal certainty on the part of data controllers and in view of the importance of ensuring adequate information quality in an age of increasing electronic interpenetration.

This notwithstanding, some caution is vital when formulating requirements for quality *assurance*. Such requirements have the potential of generating operating costs for data controllers which are disproportionately high relative to the risk of error causing detriment to the data subjects. Some form of 'reasonable steps' standard is probably most appropriate. At the same time, this standard should not be determined solely or primarily by the needs of data controllers; rather, it should be linked primarily to what is necessary to ensure fair data-processing outcomes for the data

---

1222 *Supra* n 1178.

1223 See also Chapter 3 (section 3.5).

1224 The simplest formulation I have come across is in Switzerland's federal *Data Protection Act* which merely mentions 'Richtigkeit' (Art 5(1)).

subjects. A point of departure for drafting a general rule on information quality could be the following:

> *All reasonable steps shall be taken to check and ensure that data are correct, complete, relevant and not misleading in relation to what they are intended to describe and in relation to the purposes for which they are processed. In assessing what is reasonable, primary regard shall be given to the extent to which data-processing error can have detrimental consequences for the data subject(s).*

Thirdly, data protection legislation needs to be supplemented with more detailed rules on the quality of information systems. More specifically, a set of rules should be drawn up stipulating that the development of information systems shall be oriented to maximising – within the boundaries of what is technically feasible and reasonable – the manageability, reliability, robustness, comprehensibility and accessibility of the systems, both from the point of view of systems users and of data subjects. A useful point of departure for the drafting of such rules are the nine core principles of the OECD *Guidelines for the Security of Information Systems*.[1225] Despite being somewhat prolix and, on their face, only tangentially relevant to data protection concerns, these principles are worth citing in full as there is a paucity of equivalent principles in data protection discourse. Moreover, they appear to have been quickly passed over in this discourse and now seem largely forgotten – which is both surprising and unfortunate. The principles are as follows:

> **'1. Accountability Principle**
>
> The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.
>
> **2. Awareness Principle**
>
> In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

1225 *Supra* n 48.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

7. Timeliness Principle

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.'

It is not suggested that these principles be incorporated word for word in data protection legislation. Rather, it is suggested that the ideas they express should inspire the drafting of a similar set of rules dealing with the quality of information systems from a data protection perspective. For example, in light of the above-cited awareness principle and, to some extent, the reassessment, accountability, ethics and democracy principles, a rule ought to be formulated which requires that information systems be designed so as to improve the extent to which they are able to (i) automatically test aspects of the quality of the data/information they process, and (ii) communicate the results of such tests to the data controllers.[1226]

The above principles can also help to inspire a range of other rules. One such rule should require data controllers to issue information quality declarations. These declarations would describe the means by which the quality of information processed by the controllers has been checked, the results of such tests and any remaining uncertainty about the quality. The declarations would be handed to the relevant data protection authorities. Such a rule would build upon and extend Arts 17 and 19 of the EC Directive (which institute broadly similar requirements, though mainly in relation to measures for protecting the confidentiality and integrity of data).[1227]

Another such rule should require that formalised (documented) agreement be reached as to (i) which person(s)/organisation(s) is/are directly responsible and liable for the quality of the information in the system concerned and (ii) how this quality is to be monitored.

A third such rule should specifically address the need for education/training of the persons who actually carry out data processing. Pursuant to such a rule, data processors would need to be made aware of at least the following: (i) the core principles and rules of data protection; (ii) the basic rationale and importance of these principles and rules; (iii) how these principles and rules apply to their own work tasks.[1228]

1226 Cf Ivanov, *supra* n 716, 50–51 (pointing out that the quality of an IS involves the capacity of the system for taking account of alternative contradictory assessments of data or building in possibilities of indicating: (i) margins of uncertainty; or (ii) when classifications and definitions are inapplicable; or (iii) when a whole database has to be closed down). See also KC Laudon, 'Data Quality and Due Process in Large Interorganizational Record Systems' (1986) 29 *Communications of the ACM*, no 1, 4 (noting that information systems differ in terms of how easily they allow persons to discover erroneous data kept in the systems).

1227 See further Chapters 3 and 4 (sections 3.8 and 4.2).

1228 Cf principle 5.9 of the ILO Code of Practice on Protection of Workers' Personal Data (*supra* n 74) which stipulates: 'Persons who process personal data should be regularly trained to ensure an

A fourth such rule should require data controllers to subject their information systems to periodical data protection audits by a competent and independent third party.[1229] These audits would endeavour to ascertain strengths and weaknesses in the data protection measures taken by the controller concerned, using existing laws as the primary point of reference. The rule should further stipulate conditions for disclosing the audit results to the relevant data protection authorities and the general public.

Extending the latter rule, data controllers should be encouraged, if not required, to undertake *ex ante* assessments of the impact that their planned data-processing operations or planned changes to the information system(s) supporting such operations, might have on data protection interests. An appropriate point of departure for defining these interests could be the interest catalogue outlined in Chapter 7 (section 7.2.5). This kind of assessment tends to be championed under the name of 'privacy impact assessment'.[1230] The latter nomenclature is somewhat misleading as the assessment is intended to evaluate more than the possible effects of planned activity on privacy as such. Ideally, the assessment should be carried out by a competent and independent third party, and its results made public.[1231]

Closely related to the above proposals for rules on IS quality, more explicit and systems-active provisions should be drafted on anonymity. Opportunities for anonymity should be promoted more obviously in the rules embodying the minimality principle. Indeed, allowance for anonymity should be made a basic data protection principle in itself.[1232] Data protection laws should additionally be infused with provisions explicitly addressing the need to develop organisational-technological infrastructures that promote transactional anonymity. Useful model provisions in this regard are ss 3a and 9 of Germany's *Federal Data Protection Act* and s 4(6) of Germany's *Teleservices Data Protection Act* (set out in Chapter 18 (section 18.4.3). Following on from the latter provisions, it is desirable that rules promoting anonymity be supplemented by rules promoting pseudonymity. The appropriate rules should stipulate anonymity as the primary goal with pseudonymity

---

(Cont.)
understanding of the data collection process and their role in the application of the principles in this code'.

1229 This sort of rule is already present in s 9a of Germany's *Federal Data Protection Act* and s 21 of Germany's *Interstate Agreement over Media Services* (*supra* n 784) but, surprisingly, not in the *Teleservices Data Protection Act*. Section 9a reads: 'Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und –programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt'.

1230 See further B Stewart, 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies' (1999) 5 *PLPR*, 147–149; DH Flaherty, 'Privacy impact assessments: an essential tool for data protection' (2000) 7 *PLPR*, 85–90.

1231 See also Stewart, *ibid*; Clarke, *ibid*.

1232 As it is, for instance, in the Victorian *Information Privacy Act*, *supra* n 1174.

as the first fall-back option when anonymity cannot be achieved for legal or technical reasons.

With the regulation of profiling practices in mind, we must remember that use of pseudonyms does not in itself prevent profiles being created and applied. Indeed, this is precisely why pseudonym usage could prove to be popular for data controllers, at least if they are faced with anonymity requirements as the only alternative. Nevertheless, use of pseudonyms can hamper the ability of profilers (particularly those who do not possess the 'master keys' for the pseudonyms) to apply the profiles in a manner that specifically targets the persons behind the pseudonyms, at least outside the area of activity in which the pseudonym is applied. If such targeting is to be seriously restricted, rules must be introduced laying down stringent conditions for (i) accessing the 'master keys' to the pseudonyms and (ii) connecting the pseudonym-linked profiles to the pseudonym bearers.[1233]

All of the above proposals link up with and supplement a now considerable body of literature urging a more systemic focus for data protection law and policy.[1234] At the same time, they do not radically depart from the basic thrust of existing rules in data protection laws; rather, they elaborate what is already present in the penumbra of these rules. It goes without saying that they will need to be fine-tuned in accordance with the powers, resources and practices of the relevant data protection authorities. For instance, the proposal for a rule on data protection audits will need to be adjusted in light of the nature of these authorities' auditing activities. The same applies with respect to the proposal for 'privacy impact assessments'.

The above proposals should be augmented by rules dealing specifically with profiling. One such rule should be along the lines of s 21 in Norway's *Personal Data*

1233 Recall the prohibition on such connection in s 4(4) of the German *Teleservices Data Protection Act* (see Chapter 18 (section 18.3.2)).

1234 See, eg, A Büllesbach, 'Informationsverarbeitungssicherheit, Datenschutz und Qualitätsmanagement' (1995) 11 *RDV*, 1–6; K Johnsen, *Systemtekniske konsekvenser av persondatalovgivningen*, CompLex 4/81 (Oslo: Universitetsforlaget, 1981); K Johnsen, 'System Implications of Privacy Legislation', in J Bing & KS Selmer (eds), *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980), 92–118; Steinmüller, *supra* n 47, 663ff; Information and Privacy Commissioner of Ontario & Registratiekamer of the Netherlands, *supra* n 377; Rossnagel, Pfitzmann & Garstka, *supra* n 638. Closely related to this literature, and partly overlapping with it, is a body of work addressing the quality (in particular, the legal validity) of automated decision-making systems in public administration: see, eg, DW Schartum, 'Dirt in the Machinery of Government? Legal Challenges Connected to Computerized Case Processing in Public Administration' (1995) 2 *Int J of Law and Information Technology*, 327–354; Schartum, *supra* n 546, Part V; C Magnusson Sjöberg, *Rättsautomation* (Stockholm: Norstedts Juridik, 1992), espec chapt 7; Bing, *supra* n 1054, 234; Selmer, *supra* n 19, 63–65. Also related are proposals for a more systemic focus in the application of administrative law doctrines on rule of law: see, eg, Boe, *supra* n 1012, 366–377, 866–868. Usefully supplementing and linking up with the above literature are analyses of the way in which the architecture of information systems regulates conduct with respect to information usage: see espec L Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); JR Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 *Texas L Rev*, 553–593; Greenleaf, *supra* n 1222.

Act (set out in Chapter 18 (section 18.3.4)). It will be recalled that s 21 lays down a duty on the part of a data controller to supply a person with certain types of information about a profile when it (the profile) is used to establish contact with or make a decision about the person. The provision does not require notification of the logic or assumptions behind the profile concerned; nor does it specify the time frame in which the information is to be provided. New rules modelled on s 21 should correct the latter omission by specifying that the information be supplied at the time contact with the person is made. They should additionally require notification of the logic or assumptions behind the profile, at least when it is used to ground a decision significantly affecting the person's rights or interests. The new rules should also make clear that the duty they lay down applies not just in relation to specific profiles but also abstract profiles. The introduction of a duty of information along the lines drawn here will also involve a duty on the part of data controllers to document the profiles and the logic used to generate them.

Consideration should further be given to introducing a rule stipulating that the use of profiles for certain purposes may only occur on the basis of a broad cost/benefit analysis.[1235] Such a rule could apply when a profile is to be used for purposes that are reasonably likely to have a significant effect upon the rights or interests of persons (eg, when the profile is to be used for control purposes). The rule would directly augment the more general proposal above on 'privacy impact assessments'. As part and parcel of the suggested cost/benefit analysis, the profiles would need to be checked for their validity. Moreover, consideration would need to be taken of a range of other factors, including the nature of the decision(s) for which the profiles are to be applied, the number of persons to be subjected to the profiling, the criteria and data upon which the profiles are based, and the data sources used. Again, the proposal would encompass both abstract and specific profiles.

Exactly who would be best suited to carry out such analysis is a vexed issue. An ideal regime would involve the data controllers themselves carrying out such analysis, with appropriate guidance from data protection authorities. However, it is questionable whether such a degree of self-regulation would also lead to an appropriate degree of self-restraint. Broadly similar rules instituted in the USA and Australia in relation to data matching have evidently had little dampening effect on matching practices.[1236] Although these results cannot be applied uncritically and wholesale to other jurisdictions, they are worth keeping in mind. They also prompt consideration of alternative methods of subjecting profiling practices to cost/benefit assessment.

An obvious alternative method in this respect is to subject profiling to licensing by data protection authorities. A licensing regime such as that which was set up under Norway's PDRA – with the broad formulations found in ss 10 and 11 of the

---

1235 Support for such a rule has been expressed by, ia, the OTA, *supra* n 1030, 94.

1236 See RA Clarke, 'Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism' (1995) 4 *Information Infrastructure and Policy*, 29–65.

Act – gives data protection authorities immense capability to regulate both the generation and application of profiles. The Directive allows for some degree of licensing in relation to 'processing operations likely to present specific risks to the rights and freedoms of data subjects' (Art 20(1)).[1237] Insofar as the licensing applies to the planned processing of *personal* data, the criteria for assessment and regulation of the processing must be commensurate with the rules for processing laid down by the Directive. Given the broad formulation of these criteria, especially in Art 6(1), it would seem that a data protection authority could subject processing plans to a test of social desirability which is approximately as broad and flexible as the test that was applied by the Norwegian Data Inspectorate pursuant to the PDRA. Despite its attendant disadvantages in terms of bureaucracy, such a licensing system could ultimately prove to be the most effective means of ensuring that data protection principles do not remain simply 'law-in-books' with respect to profiling practices.

I am sceptical of outright bans on profiling or bans on the use of particular technologies for profiling. Some support has been expressed for introducing a general legal prohibition on the use of cookies mechanisms and intelligent agents, at least when these are applied for the purpose of profiling Internet users.[1238] Such a prohibition appears extreme given that cookies and intelligent agents have legitimately useful functions to play, even when used for profiling purposes. A prohibition would also be difficult if not impossible to enforce (as its proponents sometimes admit). It should therefore be eschewed, at least until after other, more accommodating regulatory strategies are tested. With respect to the Internet, there exist a large range of such strategies, relying on a mixture of technological, ethical, contractual and legislative mechanisms.[1239] The bulk of these strategies are able to complement the proposals advanced above.

In light of the conclusions of Part III, the above proposals should extend – at least as a point of departure – to the processing of data on organised collective

---

1237 See further Chapter 4 (section 4.2).

1238 See, eg, Blume, *supra* n 463, 13–14.

1239 Note, eg, the proposal of the UK Data Protection Registrar (now 'Information Commissioner') for development and use of 'suppression markers' or 'privacy markers' in e-mail addresses: see *Thirteenth Report of the Data Protection Registrar, June 1997* (HMSO, 1997), Appendix 14 ('Privacy Enhancing Technologies: Suppression Markers in Internet Addresses'). Such markers would consist of codes indicating whether or not, and under what conditions, the person linked to the address wants to receive unsolicited e-mail advertising. It has been rightly pointed out, though, that the use of these markers could itself engender new types of profiles – '[t]hus, a kind of meta-privacy preference might also be needed regarding the fair use of privacy markers in settings outside the Internet': Reidenberg & Schwartz, *supra* n 1073, 81. For lists of other types of relevant strategies, see, eg, Data Protection Working Party, Recommendation 1/99, *supra* n 1073; Data Protection Working Party, 'Privacy on the Internet: An Integrated EU Approach to On-line Data Protection', *supra* n 220; International Working Group on Data Protection in Telecommunications (IWGDPT), 'Common Position on Intelligent Software Agents', adopted 29.4.1999, <http://ig.cs.tu-berlin.de/~dsb/doc/int/iwgdpt/agent_en.htm>; IWGDPT, 'Common Position on Data Protection and Search Engines on the Internet', adopted 15.4.1998, <http://ig.cs.tu-berlin.de/~dsb/doc/int/iwgdpt/find_en.htm>.

entities (as well as individuals). Consideration should also be given to making the above proposals apply not just in relation to the processing of personal data but also aggregate/group data. Any such extension carries, of course, a risk of regulatory overreaching. However, this risk needs to be weighed against the risk of collective entities (and the individuals attached to them) suffering detriment through the processing of data on them. Another factor to be weighed here is the frequent difficulty in drawing a hard and fast line between personal and aggregate/group data. With the adoption of a more systemic regulatory focus for data protection law, such line-drawing loses much of its practical relevance. An appropriate compromise might be to subject the processing of aggregate/group data to certain basic rules of data protection laws when there is a reasonable likelihood that the processing will affect the rights and freedoms of one or more individuals or one or more organised collective entities.[1240]

Another compromise strategy worth considering is to make the traditional definition of 'personal data' more flexible by supplementing the identifiability criterion with a contactability/reachability criterion. More specifically, 'personal data' would be defined as data that facilitate either identification of a particular individual or *contact* to be made with him/her.[1241] This strategy might well prove useful in an Internet context where there is uncertainty as to whether, say, a machine address is 'personal data',[1242] yet where the person(s) using the address are subjected to profiling or to measures instituted on the basis of profiling.[1243]

1240 See also Chapter 15 (section 15.7).

1241 Cf section 21 of the Norwegian Act (set out in Chapter 18 (section 18.3.4)) which creates a duty to provide information about a profiling practice when, ia, a person is *contacted* on the basis of the profile.

1242 Cf the discussion in Chapter 18 (section 18.2).

1243 Greenleaf advocates this strategy too: see espec Greenleaf, *supra* n 381.

20. Conclusion

At first sight, data protection law appears to constitute a neatly bounded legislative package with a simple agenda and origins. Closer analysis, however, confirms the age-old adage that appearances are deceptive. The rationale, logic and limits of data protection law are considerably more complex, heterogeneous and open-ended than is commonly thought. Traditional perceptions about this body of law need to be expanded and revised to take proper account of this complexity.

In terms of aetiology, data protection law is more than a technology-induced legislative reaction. It owes its origins to a complex array of factors (ideological, organisational, economic, etc) of which computers are just one (albeit important) element. At the same time, the rationale for data protection can be analysed at various levels. Traditionally, such law is viewed as a recent instance of a long line of legal innovations attempting to secure certain interests and values – most notably the privacy of individuals – made vulnerable by technological change. Yet such law should also be seen as an attempt to shore up public confidence in organisations' processing of personal data in an age in which the problem of 'risk' has intensified in human consciousness. Building on the latter view, such law should further be seen as attempting to enhance the legitimacy of data-processing operations in the public eye.

Concomitantly, data protection law is concerned with a great deal more than safeguarding simply the privacy of individuals. It serves a multiplicity of other interests as well (democracy, pluralism, information quality, etc). These interests can attach to collective entities in addition to individuals, and to data controllers as well as data subjects. However, the interests will not necessarily be shared by each actor to the same degree or for the same reasons.

Just as we should expand our views on the range of interests safeguarded by data protection law, so too should we expand our perception about the constellations of relationships in which these interests – and regulatory strategies for their protection – are relevant. Data protection discourse has traditionally focused on the relationship between State agencies and the individual, and between (large) private organisations and the individual. We need to take into consideration other relationships as well, such as those between State agencies and private organisations, and between private organisations and other private organisations. When analysing such relationships, account must additionally be taken of the role of non-organised groups.[1244]

1244 At the same time, other relationships not touched upon in the book could be analysed too (eg, the relationships between nations, between individuals and between State agencies).

Further, we need to work towards developing a more systems-active regulatory policy on information processing. Such a policy must aim to create a greater degree of what Germans term 'Systemdatenschutz' ('systemic data protection') involving the integration of data protection concerns with the development and functionalities of information technology. Such a policy must concomitantly aim to build bridges between the concepts, goals and measures that traditionally have been associated with the field of data protection, and the concepts, goals and measures that traditionally have been associated with other fields concerned with regulating information use – especially the fields of information/IT security, quality management and administrative law.

Fortunately, a growing body of data protection experts are calling for such a policy.[1245] This book strengthens their call. More generally, the book feeds into the emerging interdisciplinary field of 'value-sensitive design' which aims at ensuring that thorough account be taken of key human values during the process of designing technology.[1246]

It is doubtful, though, that all of the lines of argument advanced in the book will receive general support in the near future. This is especially so in the wake of the terrorist attacks in the USA of 11 September 2001 and the resultant push by governments in many countries to enhance national security at the probable expense of civil liberties. In the current political climate, dominated as it is by the 'war on terrorism', initiatives to strengthen data protection regimes are likely to be trumped by the introduction of new State surveillance and control measures. Advocacy of data protection rights for organised collective entities is likely to face the greatest uphill battle given the probability that such rights will be perceived by governments as hampering State security initiatives. Moreover, the trend to propose and/or enact general laws expressly providing such rights petered out to a large extent in the 1980s and has never gained a solid foothold in jurisdictions outside Europe.

Nevertheless, indications exist – at least in Europe – of a re-emerging readiness to give data protection rights to legal persons in relation to certain sectors of activity. The EC Directive on telecommunications privacy and the coming Directive on privacy of electronic communications are prime examples of such readiness. In the long term, there could well be greater support for expressly incorporating data on collective entities into more comprehensive legislative regimes on data protection with a 'systemic' focus.[1247] This support might come as a result of growing

---

1245 See, eg, the works listed *supra* n 1235. See also, ia, H Burkert, 'Public Sector Information: Towards a More Comprehensive Approach in Information Law?' (1992) 3 *J of Law and Information Science*, 47, espec 59–62; S Rodotà, 'Policies and Perspectives for Data Protection', in *Beyond 1984*, *supra* n 1039, 13, 24.

1246 See, eg, B Friedman (ed), *Human Values and the Design of Computer Technology* (New York: Cambridge University Press, 1997); B Friedman; PH Kane Jnr & DC Howe, 'Trust Online' (2000) 43 *Communications of the ACM*, no 12, 34–40.

1247 See, eg, the recent report by Rossnagel *et al*, *supra* n 638 advocating protecting legal person data as part of a 'modernisation' of German data protection law which involves more 'Systemdatenschutz'.

recognition of the need to develop holistic legislative policies on the processing of information generally. For the issue of whether or not collective entities should be given data protection rights should ultimately be linked to broader questions concerned with the development, structure and content of a legal policy on the processing of all types of information.[1248]

As for the regulation of profiling, the signs seem relatively encouraging, especially in Europe. This is particularly the case with respect to the telecommunications sector. The EC Directive on telecommunications privacy, the coming EC Directive on privacy of electronic communications and Germany's *Teleservices Data Protection Act* exhibit legislative willingness to restrict significantly the ability of telecommunications service providers to generate and apply profiles of their customers. The *Teleservices Data Protection Act* goes furthest in this regard. While it is sectoral legislation only, the sector it governs is of increasing social and commercial importance. By being the first piece of data protection legislation to specifically address the challenges of the on-line world, its influence on future data protection initiatives cannot be underestimated. Yet the Act should not be viewed as an ideal endpoint of regulatory strategy. It is rather a useful point of departure that, like all law in this area, will have to be continuously revised in the light of technological developments and changing societal attitudes.

(Cont.)

At the same time, Rossnagel *et al.* ground their support for protecting legal person data in a range of other factors, not least of which is that such protection would be consistent with – if not required by – the *Basic Law*: see *ibid*, n 65.

1248 See also Hogrebe, *supra* n 635, 61 ('the issue of legal person data protection appears not so much as the missing piece of the data protection puzzle but rather as the beginning of the road leading to a general concept of data law ... [P]utting the legal person issue into this wide perspective ... reduces at the same time much debated questions like whether or not legal persons have a privacy of their own, or whether or not legal person data should be dealt with within general data protection legislation along with physical person data or within existing bodies of commercial and other laws, to what they really are: issues of legal doctrine and technique which albeit of importance are not to be confounded with the general underlying data policy issues which constitute the general substance of the matter (and of which the legal person issue is but a part')).

Select Bibliography[1249]

A. Books and Journal Articles

Allars, M: *Introduction to Australian Administrative Law* (Sydney: Butterworths, 1990).

Agre, PE & Rotenberg, M (eds): *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT Press, 1997).

Allen, AL: 'Rethinking the Rule Against Corporate Privacy Rights: Some Conceptual Quandries for the Common Law' (1987) 20 *John Marshall L Rev*, 607–639.

— *Uneasy Access: Privacy for Women in a Free Society* (Totowa, New Jersey: Rowman & Littlefield, 1988).

— 'Genetic Privacy: Emerging Concepts and Values', in MA Rothstein (ed), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (New Haven: Yale University Press, 1997), 31–59.

Altes, WFK; Dommering, EJ; Hugenholtz, PB & Kabel, JJC (eds): *Information Law Towards the 21st Century* (Deventer/Boston: Kluwer Law & Taxation, 1992).

Altman, I: 'Privacy: A Conceptual Analysis', in DH Carson (ed), *Man-Environment Interactions: Evaluations and Applications* (Stroudsberg, Pennsylvania: Dowden, Hutchinson & Ross, 1974), 3–28.

Amann, D: '*Publicker Industries v Cohen*: public access to civil proceedings and a corporation's right to privacy' (1986) 80 *North Western University L Rev*, 1319–1354.

Andenæs, J & Bratholm, A: *Spesiell strafferett* (Oslo: Universitetsforlaget, 1993, 2nd ed, 3rd issue).

Andersen, M & Boer, M den (eds): *Policing Across National Boundaries* (London: Pinter, 1994).

Anér, K: *Datamakt* (Falköping: Gummesson, 1975).

Arendt, H: *The Human Condition* (Chicago: University of Chicago Press, 1958).

Arnesen, F: *Introduksjon til rettskildelæren i EF* (Oslo: Universitetsforlaget, 1995, 3rd ed).

Aubert, V: *Sosiologi 1. Sosialt samspill* (Oslo: Universitetsforlaget, 1981, 2nd ed).

Aulehner, J: '10 Jahre 'Volkzählungs'-Urteil: Rechtsgut und Schutzbereich des Rechts auf informationelle Selbstbestimmung in der Rechtsprechung' (1993) 9 *CR*, 446–455.

Backer, IL: *Rettslig interesse for søksmål, skjønn og klage – særlig ved naturinngrep* (Oslo: Universitetsforlaget, 1984).

Bailey, RW: *Human Error in Computer Systems* (Englewood Cliffs, New Jersey: Prentice-Hall, 1983).

1249 This bibliography contains only works referred to in the book.

Bainbridge, DI: *EC Data Protection Directive* (London: Butterworths, 1996).

— & Pearce, G: 'The Data Protection Directive: A Legal Analysis' [1996] 12 *CLSR*, 160–168.

Baldwin-Edwards, M & Hebenton, B: 'Will SIS be Europe's Big Brother?', in M Andersen & M den Boer (eds), *Policing Across National Boundaries* (London: Pinter, 1994), 137–157.

Bayne, P: 'Privacy dimensions of administrative law' (1995) 69 *Australian LJ*, 13–19.

Beck, U: *Risk Society: Towards a New Modernity* (London: Sage, 1992).

Beckman, S: 'A world-shaping technology', in M Karlsson & L Sturesson (eds), *The World's Largest Machine: Global Communications and the Human Condition* (Stockholm: Almqvist & Wiksell International, 1995), 260–287.

Beniger, JR: *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Massachusetts: Harvard University Press, 1986).

Benn, SI: 'The Protection and Limitation of Privacy' (1978) 52 *Australian LJ*, 601–612 (Part I of article); 686–692 (Part II).

— *A Theory of Freedom* (Cambridge: Cambridge University Press, 1988).

Bennett, CJ: *Regulating Privacy. Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

— & Grant, R (eds): *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

Benno, J: *Consumer Purchases through Telecommunications in Europe – Application of Private International Law to Cross-Border Contractual Disputes*, CompLex 4/93 (Oslo: TANO, 1993).

— 'Transaktionens anonymisering och dess påverkan på rättsliga problemställningar', in R Punsvik (ed), *Elektronisk handel – rettslige aspekter* (Oslo: Tano Aschehoug, 1998), 50–75.

— 'The 'anonymisation' of the transaction and its impact on legal problems', The IT Law Observatory Report 6/98, Swedish IT Commission, Stockholm, 1998.

Berg, JP: 'Finansinstitusjonenes rapporteringsplikt til ØKOKRIM ved mistanke om hvitvasking av penger – et gjennombrudd for 'informant'-samfunnet?' (1996) *Kritisk Juss*, 147–163.

— 'Offentlige skattelister – i strid med EMK?' (1998) *Kritisk Juss*, 203–204.

— 'Personopplysningsvern i et nytt årtusen – kritikk av personopplysningslov-proposisjonen' (1999) *Kritisk Juss*, 351–377.

Bergmann, M: *Grenzüberschreitende Datenschutz* (Baden-Baden: Nomos, 1985).

Bernt, JF: 'Rettskildebruk for forskeren – En sammenligning med domstolenes og forvaltningens rettskildebruk' (1989) 102 *TfR*, 265–294.

Bigus, JP: *Data Mining with Neural Networks: Solving Business Problems from Application Development to Decision Support* (New York: McGraw-Hill, 1996).

Bing, J: 'Classification of Personal Information with Respect to the Sensitivity Aspect', in *Proceedings of the First International Oslo Symposium on Data Banks and Society* (Oslo: Universitetsforlaget, 1972), 98–141.

— 'Personvern og EDB: En internasjonal oversikt', in *Den personliga integriteten: Föredrag vid den XX:e nordiska studentjuristtämman i Lund* (Lund: Juridiska Föreningen i Lund, 1979), 49–67.
— 'Information Law?' (1981) 2 *J of Media Law and Practice*, 219–239.
— *Data Protection in Practice – International Service Bureaux and Transnational Data Flows*, CompLex 1/85 (Oslo: Universitetsforlaget, 1985).
— 'Beyond 1984: the Law and Information Technology in Tomorrow's Society' (1986) 8 *Information Age*, 85–94.
— 'Three Generations of Computerized Systems for Public Administration and Some Implications for Legal Decision-Making' (1990) 3 *Ratio Juris*, 219–236.
— *Personvern i faresonen* (Oslo: Cappelen, 1991).
— 'Data Protection in a Time of Changes', in WFK Altes, EJ Dommering, PB Hugenholtz & JJC Kabel (eds), *Information Law Towards the 21st Century* (Deventer/Boston: Kluwer Law & Taxation, 1992), 247–259.
— 'The informatics of public administration: introducing a new academic discipline' (1992) *Informatica e diritto*, no 1–2, 23–34.
— 'From footprints to electronic trails: Some current issues of data protection policy', in *Proceedings of the 17th International Conference on Data Protection, Copenhagen 1995* (Copenhagen: Registertilsynet/Data Protection Agency, 1995), no pagination.
— & Selmer, KS (eds): *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980).
— & Torvund, O (eds): *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995).
Birks, P (ed): *Privacy and Loyalty* (Oxford: Clarendon Press, 1997).
Blanck, LJ: 'Personvern – nytt navn på 'gamle' rettsspørsmål?' (1979) *LoR*, 117–123.
Blankenburg, E: 'The invention of privacy', in P Ippel, G de Heij & B Crouwers (eds), *Privacy disputed* (The Haag: SDU/Registratiekamer, 1995), 31–41.
Blekeli, RD: 'Individ og informasjonsbehandling – et teoribidrag' (1974) 7 *Jus og EDB*, 1–40.
— 'Hva er personvern?', in RD Blekeli & KS Selmer (eds), *Data og personvern* (Oslo: Universitetsforlaget, 1977), 13–26.
— 'Framework for the Analysis of Privacy and Information Systems', in J Bing & KS Selmer (eds), *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980), 21–31.
— 'Contacts between Clients and Organizations', in J Bing & KS Selmer (eds), *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980), 32–44.
— & Selmer, KS (eds): *Data og personvern* (Oslo: Universitetsforlaget, 1977).
Bloustein, EJ: 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University L Rev*, 962–1007.
— *Individual and Group Privacy* (New Brunswick: Transaction Books, 1978).
Blume, P: 'The Personal Identity Number in Danish Law' (1989–90) 3 *CLSR*, 10–13.
— 'Kommercialisering af offentlig information', in *Ret & Privatisering* (Copenhagen: GadJura, 1995), 65–84.
— 'Formålsbestemthedsprinsippet i databeskyttelsesretten' (1995) 9 *UfR*, 110–115.
— *Personregistrering* (Denmark: Akademisk forlag, 1996, 3rd ed).

— 'New Technologies and Human Rights: Data Protection, Privacy and the Information Society', Paper no 67, Institute of Legal Science, Section B, University of Copenhagen, 1998.
— *Databeskyttelsesret* (Copenhagen: Jurist- og Økonomforbundets Forlag, 2000).
— *Personoplysningsloven* (Denmark: Greens§Jura, 2000).
Boe, E: *Innføring i juss: Statsrett og forvaltningsrett* (Oslo: TANO, 1993).
— 'Pseudo-Identities in Health Registers? Information Technology as a Vehicle for Privacy Protection' (1994) 2 *The Int Privacy Bulletin*, no 3, 8–13.
— 'Domstolskontroll med forvaltningen: Åpne fullmakter og Høyesteretts svar i 90-årene' (1994) *LoR*, 323–348.
— 'The Right to Privacy' i USA' (1994) *LoR*, 577–578.
— 'Forholdet mellom rule of law og rettssikkerhet', in DR Doublet, K Krüger & A Strandbakken (eds), *Stat, politikk og folkestyre: Festskrift til Per Stavang på 70-årsdagen* (Bergen: Alma Mater, 1998), 43–65.
Bok, S: *Secrets: On the Ethics of Concealment and Revelation* (New York: Pantheon, 1982).
Borchgrevink, M: *Ny teknologi i arbeidslivet: rettslige aspekter* (Oslo: Universitetsforlaget, 1985).
Bottomley, S: 'Taking Corporations Seriously' (1990) 19 *Federal L Rev*, 203–222.
Bratholm, A & Stuevold Lassen, B: 'Personlighetens rettsvern', in K Lilleholt (ed), *Knophs oversikt over Norges rett* (Oslo: Universitetsforlaget, 1998, 11th ed), 102–113.
Bråten, S: *Dialogens vilkår i datasamfunnet. Essays om modellmonopol og meningshorisont i organisasjons- og informasjonssammenheng* (Oslo: Universitetsforlaget, 1983).
Buergenthal, T: 'To Respect and to Ensure: State Obligations and Permissible Derogations', in L Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (New York: Columbia University Press, 1981), 72–91.
Bull, HP: *Datenschutz oder Die Angst vor dem Computer* (Munich: Piper, 1984).
Burkert, H: 'Die Eingrenzung des Zusatswissens als Rettung der Anonymisierung?' (1979) 8 *DVR*, 63–73.
— 'Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws' (1981–1982) 3 *Computer/LJ*, 167–188.
— 'The Law of Information Technology – Basic Concepts' (1988) *DuD*, 383–387.
— 'Data Protection and Access to Data', in P Seipel (ed), *From Data Protection to Knowledge Machines* (Deventer/Boston: Kluwer Law & Taxation, 1990), 49–69.
— 'Systemvertrauen: Ein Versuch über einige Zusammenhänge zwischen Karte und Datenschutz' (1991) *á la Card Euro-Journal*, no 1, 52–66.
— 'The Commercial Use of Government Controlled Information and its Information Law Environment in the EEC', in WFK Altes, EJ Dommering, PB Hugenholtz & JJC Kabel (eds), *Information Law Towards the 21st Century* (Deventer/Boston: Kluwer Law & Taxation, 1992), 223–246.
— 'Public Sector Information: Towards a More Comprehensive Approach in Information Law?' (1992) 3 *J of Law and Information Science*, 47–62.

— 'Access to Information and Data Protection Considerations', in C de Terwangne, H Burkert & Y Poullet (eds), *Towards a Legal Framework for a Diffusion Policy for Data held by the Public Sector* (Deventer/Boston: Kluwer Law & Taxation, 1995), 23–54.
— 'Data-Protection Legislation and the Modernization of Public Administration' (1996) 62 *Int Rev of Administrative Sciences*, 557–567.
— 'Privacy-Enhancing Technologies: Typology, Critique, Vision', in PE Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT Press, 1997), 125–142.
Burnham, D: *The Rise of the Computer State* (London: Weidenfeld and Nicholson, 1981).
Büllesbach, A: 'Informationsverarbeitungssicherheit, Datenschutz und Qualitäts-management' (1995) 11 *RDV*, 1–6.
Buttarelli, G: *Banche dati e tutela della riservatezza: La privacy nella Società dell'Informazione* (Milan: Giuffrè Editore, 1997).
Bygrave, LA: 'The Privacy Act 1988 (Cth): A Study in the Protection of Privacy and the Protection of Political Power' (1990) 19 *Federal L Rev*, 128–153.
— 'Ensuring Right Information on the Right Person(s): Legal Controls of the Quality of Personal Information – Part I', Manuscript Series on Information Technology and Administrative Systems, University of Oslo, 1996, vol 4, no 4.
— 'Informasjon som felles ressurs – mulige konsekvenser for regelverk som berører personvern', in *Informasjonsteknologi og nye medier i den offentlige informasjonens tjeneste* (Oslo: Norges forskningsråd, 1996), 69–85.
— *Personvern i praksis: Justisdepartementets behandling av klager på Datatilsynets enkeltvedtak 1980–1996* (Oslo: Cappelen, 1997).
— 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *Int J of Law and Information Technology*, 247–284.
— 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law', in P Wahlgren (ed), *IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000* (Stockholm: Jure AB, 2001), 113–125 (also published in (2000) 7 *PLPR*, 11–14, 33–36).
— 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16 *CLSR*, 252–257.
— 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2000) 7 *PLPR*, 67–76.
— 'Balancing data protection and freedom of expression in the context of website publishing – recent Swedish case law' (2001) 8 *PLPR*, 83–85.
— 'Electronic Agents and Privacy: A Cyberspace Odyssey 2001' (2001) 9 *Int J of Law and Information Technology*, 275–294.
— 'The Technologisation of Copyright: Implications for Privacy and Related Interests' (2002) 24 *EIPR*, 51–57.
— 'A right to privacy for corporations? *Lenah* in an international context' (2002) 8 *PLPR*, 130–134.

— 'An international data protection stocktake @ 2000 – Part 4: The issue of nomenclature' (2002) 9 *PLPR* (forthcoming).
— & Aarø: 'Norway', in M Henry (ed), *International Privacy, Publicity and Personality Laws* (London: Butterworths, 2000), 333–346.
— & Berg, JP: 'Reflections on the Rationale for Data Protection Laws', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 3–39.
— & Koelman, K: 'Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems', in PB Hugenholtz (ed), *Copyright and Electronic Commerce* (The Hague/London/Boston: Kluwer Law International, 2000), 59–124.
Cannataci, JA: *Privacy and Data Protection Law: International Developments and Maltese Perspectives*, CompLex 1/87 (Oslo: Norwegian University Press, 1986).
Carter-Ruck, PF & Starte, HNA: *Carter-Ruck on Libel and Slander* (London: Butterworths, 1997, 5th ed).
Chamoux, J-P: 'Data Protection in Europe: The Problem of the Physical Person and the Legal Person' (1981) 2 *J of Media Law and Practice*, 70–83.
Christie, N: *Hvor tett et samfunn?* (Oslo: Universitetsforlaget, 1982, 2nd rev ed).
Clarke, RA: 'Information Technology and Dataveillance', in D Dunlop & R Kling (eds), *Computerization and Controversy: Value Conflicts and Social Choices* (San Diego: Academic Press, 1991), 496–522 (originally published in (1989) 31 *Communications of the ACM*, 498–512).
— 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' (1993) 4 *J of Law and Information Science*, 403–419.
— 'Profiling and its privacy applications' (1994) 1 *PLPR*, 128–129, 138.
— 'The Digital Persona and its Application to Data Surveillance' (1994) 10 *The Information Society*, no 2, 77–92.
— 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7 *Information Technology & People*, 6–37.
— 'Dataveillance by Governments: The Technique of Computer Matching' (1994) 7 *Information Technology & People*, no 2, 46–85.
— 'A Normative Regulatory Framework for Computer Matching' (1995) 13 *John Marshall J of Computer and Information Law*, 585–633.
— 'Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism' (1995) 4 *Information Infrastructure and Policy*, 29–65.
Coates, JC: 'State Takeover Statutes and Corporate Theory: The Revival of an Old Debate' (1989) 64 *New York University L Rev*, 806–876.
Cohen, JE: 'A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace' (1996) 28 *Connecticut L Rev*, 981–1039.
Cole, PE: 'New Challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws' (1985) 17 *New York University J of Int Law and Politics*, 893–947.

Coll, L: *Innsyn i personopplysninger i elektroniske markedsplasser*, CompLex 3/2000 (Oslo: Universitetsforlaget, 2000).

Conard, AF: *Corporations in Perspective* (Mineola, New York: Foundation Press, 1976).

Coombe, GW & Kirk, SL: 'Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations' (1983) 39 *The Business Lawyer*, November, 33–66.

Craig, P & de Búrca, G: *EU Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 1998, 2nd ed).

Damman, U; Karhausen, M; Müller, P & Steinmüller, W: *Datenbanken und Datenschutz* (Frankfurt am Main: Herder & Herder, 1974).

Damman, U & Simitis, S: *EG-Datenschutzrichtlinie: Kommentar* (Baden-Baden: Nomos, 1997).

Dan-Cohen, M: *Rights, Persons, and Organizations* (Berkeley: University of California Press, 1986).

Dandeker, C: *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Cambridge: Polity, 1990).

Date, CJ: *An Introduction to Database Systems* (Reading, Massachusetts: Addison-Wesley, 1995, 6th ed).

Davey, K: 'Privacy Protection for Internet E-mail in Australia' (1998) *Computers & Law*, no 35, 21–33.

Davies, SG: *Monitor: Extinguishing Privacy on the Information Superhighway* (Sydney: Pan Macmillan Australia, 1996).

Davis, JP: *Corporations: A Study of the Origin and Development of Great Business Combinations and of Their Relation to the Authority of the State* (New York: Burt Franklin, 1971; first published New York, 1905).

DeCew, JW: *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca/London: Cornell University Press, 1997).

— 'The Scope of Privacy in Law and Ethics' (1986) 5 *Law and Philosophy*, 145–173.

'Definitionsversuche zum Datenschutz' (1975) 5 *Öffentliche Verwaltung und Datenverarbeitung*, 91–92.

Dillon, RS (ed): *Dignity, Character, and Self-Respect* (New York/London: Routledge, 1995).

Djønne, E; Grønn, T & Hafli, T: *Personregisterloven med kommentarer* (Oslo: TANO, 1987).

Djønne, E (ed): *Datatilsynet: 10 år som personvernets vokter*, CompLex 4/90 (Oslo: TANO, 1990).

Dohr, W; Pollirer, H-J & Weiss, EM: *Datenschutzgesetz* (Vienna: Manzsche Verlags- und Universitätsbuchhandlung, 1988).

Donk, WBHJ van de & Duivenboden, H van: 'Privacy as policy: a policy implementation perspective on data protection at shopfloor level in the Netherlands' (1996) 62 *Int Rev of Administrative Sciences*, 513–534.

Donk, WBHJ van de; Bennett, CJ & Raab, CD: 'The politics and policy of data protection: experiences, lessons, reflections and perspectives' (1996) 62 *Int Rev of Administrative Sciences*, 459–464.

— 'The politics and policy of data protection: concluding observations' (1996) 62 *Int Rev of Administrative Sciences*, 569–574.

Donk, WBHJ van de; Snellen, ITM & Tops, PW (eds): *Orwell in Athens: A Perspective on Informatization and Democracy* (Amsterdam: IOS Press, 1995).

Druey, JN: ''Daten-Schmutz' – Rechtliche Ansatzpunkte zum Problem der Über-Information', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Stämpfli & Cie, 1990), 379–396.

Dumortier, J (ed): *Recent Developments in Data Privacy Law* (Leuven: Leuven University Press, 1992).

Dutton, WH & Meadow, RG: 'A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties', in KB Levitan (ed), *Government Infostructures* (New York: Greenwood Press, 1987), 147–170.

Dörr, E & Schmidt, D: *Neues Bundesdatenschutzgesetz: Handkommentar* (Cologne: Datakontext, 1997, 3rd ed).

Dworkin, G: *The Theory and Practice of Autonomy* (Cambridge: Cambridge University Press, 1988).

Dworkin, R: *Taking Rights Seriously* (London: Duckworth, 1977).

Eckhoff, T: 'Guiding Standards in Legal Reasoning' (1976) 29 *Current Legal Problems*, 205–209.

— (with Helgesen, JE): *Rettskildelære* (Oslo: Tano Aschehoug, 1997, 4th ed).

— & Sundby, NK: *Rettssystemer* (Oslo: TANO, 1991, 2nd ed).

— & Smith, E: *Forvaltningsrett* (Oslo: Tano Aschehoug, 1997, 6th ed).

Egede-Nissen, H: 'Brukernes epoke', in P Gottschalk (ed), *IT neste TI. Informasjonsteknologi de neste ti år* (Oslo: Ad Notam Gyldendal, 1993), 255–264.

Eger, JM: 'Emerging Restrictions on Transborder Data Flow: Privacy Protection or Non-Tariff Trade Barriers' (1978) 10 *Law and Policy in International Business*, 1055–1103.

Ehmann, E & Helfrich, M: *EG Datenschutzrichtlinie: Kurzkommentar* (Cologne: O Schmidt, 1999).

Elgesem, D: 'Remarks on the Right of Data Protection', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 83–104.

Ellger, R: *Der Datenschutz im grenzüberschreitende Datenverkehr: eine rechtsvergleichende und kollisionsrechtliche Untersuchung* (Baden-Baden: Nomos, 1990).

— 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 1)' (1991) 7 *RDV*, 57–65.

— 'Datenschutzgesetz und europäischer Binnenmarkt (Teil 2)' (1991) 7 *RDV*, 121–135.

Ellul, J: *The Technological Society*, trans J Wilkinson (New York: Vintage, 1964).

Engel-Flechsig, S: 'Teledienstedatenschutz' (1997) 21 *DuD*, 8–16.

— & Maennel, FA & Tettenborn, A: 'Das neue Informations- und Kommunikationsdienste-Gesetz' (1997) *Neue juristische Wochenschrift*, 2981–2992.

Falck, P: *Personvern som menneskerett. Den europeiske menneskerettighetskonvensjon artikkel 8 som skranke for innsamling, behandling og bruk av personopplysninger*, Det juridiske fakultets skriftserie nr 56 (Bergen: University of Bergen, 1995).

Fayyad, U & Uthurusamy, R (eds): 'Data Mining and Knowledge Discovery in Databases' (1996) 39 *Communications of the ACM*, no 11, 24–68.

Feldman, D: 'Privacy-related Rights and their Social Value', in P Birks (ed), *Privacy and Loyalty* (Oxford: Clarendon Press, 1997), 15–50.

Flaherty, DH: 'Nineteen Eighty-Four and After' (1984) 1 *Government Information Quarterly*, 431–442.

— 'Cumulative Data are Not Always Anonymous' (1985) 11 *Privacy J*, no 9, 3, 6.

— *Protecting Privacy in Surveillance Societies* (Chapel Hill/London: University of North Carolina Press, 1989).

— 'Data Protection and National Information Policy', in P Seipel (ed), *From Data Protection to Knowledge Machines* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990), 29–47.

— 'Privacy Impact Assessments: An essential tool for data protection' (2000) 7 *PLPR*, 85–90.

— (ed): *Privacy and Data Protection. An International Bibliography* (London: Mansell, 1984).

Flynn, JJ: 'The Jurisprudence of Corporate Personhood: The Misuse of a Legal Concept', in WJ Samuels & AS Miller (eds), *Corporations and Society: Power and Responsibility* (New York: Greenwood Press, 1987), 131–159.

Foucault, M: *Discipline and Punish: The Birth of the Prison*, trans A Sheridan (Harmondsworth: Penguin, 1977).

Freese, J: *Den maktfullkomliga oförmågan* (Stockholm: Wahlström & Widstrand, 1987).

— 'Rapport om skyddet för enskilda personers privatliv – ett mer samlat grepp?', Report for the Swedish Ministry of Justice, delivered 15.3.1995.

— & Holmberg, S: *Datasäkerhet* (Stockholm: Affärsinformation, 1989).

Freund, PA: 'Privacy: One Concept or Many', in JR Pennock & JW Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), 182–198.

Fried, C: 'Privacy (A Moral Analysis)' (1968) 77 *Yale LJ*, 475–493.

— *An Anatomy of Values: Problems of Personal and Social Choice* (Harvard: Harvard University Press, 1970).

Friedman, B (ed): *Human Values and the Design of Computer Technology* (New York: Cambridge University Press, 1997).

— & Kane, PH Jnr & Howe, DC: 'Trust Online' (2000) 43 *Communications of the ACM*, no 12, 34–40.

Frihagen, A: *Forvaltningsrett*, Vol I (Oslo: Frihagen, 1991).

— *Offentlighetsloven*, Vol II (Bergen: Frihagen, 1994, 2nd ed).

Froomkin, AM: 'Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases' (1996) 15 *U of Pittsburgh J of Law and Commerce*, 395–507.

— 'The Death of Privacy?' (2000) 52 *Stanford L Rev*, 1461–1543.

Frowein, JA & Peukert, W: *Europäische MenschenRechtsKonvention: EMRK-Kommentar* (Kehl am Rhein: NP Engel, 1996, 2nd ed).

Gandy, OH Jr: *The Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993).

Gassmann, H-P: 'Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa', in R Dierstein, H Fiedler & A Schulz (eds), *Datenschutz und Datensicherung* (Cologne: JP Bachem, 1976), 11–26.

— 'Privacy Implications of Transborder Data Flows: Outlook for the 1980s', in LJ Hoffman (ed), *Computers and Privacy in the Next Decade* (New York: Academic Press, 1980), 109–117.

Gavison, R: 'Privacy and the Limits of Law' (1980) 89 *Yale LJ*, 421–471.

— 'Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs. Free Speech' (1992) 43 *South Carolina L Rev*, 437–471.

Geiger, H: 'Europäischer Informationsmarkt und Datenschutz' (1989) 5 *RDV*, 203–210.

Gellman, RM: 'Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions' (1993) VI *Software LJ*, 199–238.

Gerety, T: 'Redefining Privacy' (1977) 12 *Harvard Civil Rights-Civil Liberties L Rev*, 233–296.

Gerstein, RS: 'Intimacy and Privacy' (1978) 89 *Ethics*, 76–81.

Gibson, D (ed): *Aspects of Privacy: Essays in Honour of John M Sharp* (Toronto: Butterworths, 1980).

Giddens, A: *The Consequences of Modernity* (Cambridge: Polity Press, 1990).

— *Modernity and Self-Identity: Self and Society in the Late Modern Age* (Cambridge: Polity Press, 1991).

Greenberger, M (ed): *Computers, Communications, and the Public Interest* (Baltimore/London: Johns Hopkins Press, 1971).

Greenleaf, G: 'The European privacy Directive – completed' (1995) 2 *PLPR*, 81–86.

— 'Privacy principles – irrelevant to cyberspace?' (1996) 3 *PLPR*, 114–119.

— 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21 *University of New South Wales LJ*, no 2, 593–622.

— ''IP, Phone Home': The Uneasy Relationship between Copyright and Privacy, illustrated in the Laws of Hong Kong and Australia' (2002) 32 *Hong Kong LJ* (forthcoming).

Gross, H: 'Privacy and Autonomy', in JR Pennock & JW Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), 169–181.

Grossman, GS: 'Transborder Data Flows: Separating the Privacy Interests of Individuals and Corporations' (1982) 4 *Northwestern J of Int Law & Business*, no 1, 1–36.

Guadamuz, A: 'Habeas Data: The Latin American Response to Data Protection' (2000) *Journal of Information, Law and Technology*, no 2, <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html>.

Gunning, P: 'Central features of Australia's private sector privacy law' (2001) 7 *PLPR*, 189–199.

Haas, JE & Drabek, TE: *Complex Organizations: A Sociological Perspective* (New York: Macmillan, 1973).

Habermas, J: *Faktizität und Geltung. Beiträge zur Diskurstheori des Rechts und des demokratischen Rechtsstaates* (Frankfurt am Main: Suhrkamp, 1992).

Hailer, M & Ritschl, D: 'The General Notion of Human Dignity and the Specific Arguments in Medical Ethics', in K Bayertz (ed), *Sanctity of Life and Human Dignity* (Dordrecht/Boston/London: Kluwer Academic, 1996), 91–104.

Hansen, J: *SAFE-P: Sikring av foretak, EDB-anlegg og personverninteresser etter personregisterloven*, CompLex 12/88 (Oslo: TANO, 1988).

Harris, DJ; O'Boyle, M & Warbrick, C: *Law of the European Convention on Human Rights* (London/Dublin/Edinburgh: Butterworths, 1995).

Harris, PR: 'A Right to Privacy for Incorporated and Unincorporated Associations?' (1965) 16 *Virginia Law Weekly DICTA Comp*, 97–103.

Hartley, TC: *The Foundations of European Community Law* (Oxford: Clarendon Press, 1998, 4th ed).

Henke, F: *Die Datenschutzkonvention des Europarates* (Frankfurt am Main/Bern/New York: Peter Lang, 1986).

Hjort Kraby, I: 'Hva er lov? – Særlig om legalitetsprinsippet og faktiske handlinger' (1996) *Jussens Venner*, 145–160.

Hoffman, LJ (ed): *Computers and Privacy in the Next Decade* (New York: Academic Press, 1980).

Holgersen, G: 'Den rettskildemessige vekt av praksis ved spesielle håndhevings- og kontrollorganer innen forvaltningen' (1987) 100 *TfR*, 404–444.

Hondius, FW: *Emerging Data Protection in Europe* (Amsterdam: North Holland, 1975).

Horwitz, MJ: '*Santa Clara* Revisited: The Development of Corporate Theory', in WJ Samuels & AS Miller (eds), *Corporations and Society: Power and Responsibility* (New York: Greenwood Press, 1987), 13–63.

Hov, J: *Rettergang i sivile saker* (Oslo: Papinian, 1994).

Hoyle, C: 'Legal Aspects of Transborder Data Flow' (1992) 8 *CLSR*, 166–172.

— 'Trans-Border Data Flows: Many Barriers Stand in the Way for Users' (1992) 1 *The Int Computer Lawyer*, no 1, 14–22.

Hubick, KT: *Artificial Neural Networks in Australia* (Canberra: Department of Industry Technology and Commerce, 1992).

Hubmann, H: *Das Persönlichkeitsrecht* (Cologne/Graz: Böhlau, 1967, 2nd ed).

Ims, KJ: *Informasjonsetikk i praksis. Datasikkerhet og personvern* (Oslo: TANO, 1992).

Inness, JC: *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1992).

Ippel, P; de Heij, G & Crouwers, B (eds): *Privacy disputed* (The Hague: SDU/Registratiekamer, 1995).

Ivanov, K: *Systemutvekling och rättssäkerhet: Om statsförvaltningens datorisering och de långsiktiga konsekvenserna för enskilda och företag* (Stockholm: Svenska Arbetsgivarföreningen, 1986).

Johnsen, K: *Systemtekniske konsekvenser av persondatalovgivningen*, CompLex 4/81 (Oslo: Universitetsforlaget, 1981).

— 'System Implications of Privacy Legislation', in J Bing & KS Selmer (eds), *A Decade of Computers and Law* (Oslo: Universitetsforlaget, 1980), 92–118.

Joinet, L: 'French Law in Relation to Information Privacy', in *Data Regulation: European & Third World Realities* (Uxbridge: Online Conferences Ltd, 1978), 215–221.

Kang, J: 'Information Privacy in Cyberspace Transactions' (1998) 50 *Stanford L Rev*, 1193–1294.

Karlsson, M & Sturesson, L (eds): *The World's Largest Machine. Global Telecommunications and the Human Condition* (Stockholm: Almqvist & Wiksell International, 1996).

Kaspersen, HWK & Oskamp, A (eds): *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990).

Katsh, ME: *Law in a Digital World* (New York: Oxford University Press, 1995).

Katz, JE & Tassone, AR: 'Public Opinion Trends: Privacy and Information Technology' (1990) 54 *Public Opinion Quarterly*, 124–153.

Keenan, D: *Smith & Keenan's English Law* (London: Pitman Publishing, 1995, 11th ed).

Kilian, W; Lenk, K & Steinmüller, W (eds): *Datenschutz* (Frankfurt am Main: Athenäum, 1973).

Kirby, MD: 'Legal Aspects of Transborder Data Flows' (1991) 5 *Int Computer Law Adviser*, no 5, 4–10.

— 'Information Security – OECD Initiatives' (1992) 3 *J of Law and Information Science*, 25–46 (also published in (1992) 8 *CLSR*, 102–110).

— 'Transborder Data Flows and the 'Basic Rules' of Data Privacy' (1981) 16 *Stanford J of Int Law*, 27–66.

Kirsch, WJ: 'The Protection of Privacy and Transborder Flows of Personal Data: the Work of the Council of Europe, the Organization for Economic Co-operation and Development and the European Economic Community' (1982) *Legal Issues of European Integration*, no 2, 21–50.

Kling, R: 'Automated Welfare Client-Tracking and Service Integration: The Political Economy of Computing' (1978) 21 *Communications of the ACM*, 484–493.

Kolnai, A: 'Dignity', in RS Dillon (ed): *Dignity, Character, and Self-Respect* (New York/London: Routledge, 1995), 53–75.

Korff, D: 'The Effects of the EC Draft Directive on Business', in J Dumortier (ed), *Recent Developments in Data Privacy Law* (Leuven: Leuven University Press, 1992), 43–57.

Koskull, A von: 'Personvärn och personalrekrytering, eller transformation och skygglappar' (1996) *Tidsskrift utgiven av Juridiska Föreningen i Finland*, no 6, 391–433.

Kuopos, J: 'Finland', in D Campbell & J Fisher (eds), *Data Transmission and Privacy* (Dordrecht/Boston/London: M Nijhoff, 1994), 161–187.

Laudon, KC: *Computers and Bureaucratic Reform: The Political Functions of Urban Information Systems* (New York: Wiley, 1974).

— 'Data Quality and Due Process in Large Interorganizational Record Systems' (1986) 29 *Communications of the ACM*, no 1, 4–11.

— 'Markets and Privacy' (1996) 39 *Communications of the ACM*, no 9, 92–104.

Lenk, K: 'Information Technology and Society', in G Friedrichs & A Schaff (eds), *Microelectronics and Society: For Better or For Worse* (Oxford: Pergamon Press, 1982), 273–310.

Lenth, C: *Adgangen til å benytte personopplysninger med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor*, CompLex 2/2000 (Oslo: Universitetsforlaget, 2000).

Lessig, L: *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

Lindblom, PH: *Grupptalan. Det anglo-amerikanska class actioninstitutet ur svenskt perspektivt* (Stockholm: Norstedts, 1989).

— 'Group Actions in Civil Procedure in Sweden', in S Strömholm & C Hemström (eds), *Swedish National Reports to the XIIIth International Congress of Comparative Law* (Uppsala: Almqvist & Wiksell International, 1990), 59–100.

Lindsay, WC: 'When Uncle Sam Calls does Ma Bell Have to Answer? Recognizing a Constitutional Right to Corporate Informational Privacy' (1985) 18 *John Marshall L Rev*, 915–935.

Litman, J: 'Information Privacy/Information Property' (2000) 52 *Stanford L Rev*, 1283–1313.

Lloyd, IJ: 'The Data Protection Act – Little Brother Fights Back?' (1985) 48 *Modern L Rev*, 190–200.

Longworth, E & McBride, T: *The Privacy Act: A Guide* (Wellington: GP Publications, 1994).

Lowell, CH: 'Corporate Privacy: A Remedy for the Victim of Industrial Espionage' (1972) 4 *Patent L Rev* (renamed *Intellectual Property L Rev*), 407–449.

Luhmann, N: *Risk: A Sociological Theory* (Berlin: Walter de Gruyter, 1993).

Lukes, S: *Individualism* (Oxford: Blackwell, 1973).

Lunheim, R & Sindre, G: 'Privacy and Computing: A Cultural Perspective', in R Sizer, L Yngström, H Kaspersen & S Fischer-Hübner (eds), *Security and Control of Information Technology in Society* (Amsterdam: North-Holland, 1994), 25–40.

Lusky, L: 'Invasion of Privacy: A Classification of Concepts' (1972) 72 *Columbia L Rev*, 693–710.

Lyon, D: *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994).

Løchen, TC & Grimstad, A: *Markedsføringsloven med kommentarer* (Oslo: Tano Aschehoug, 1997, 6th ed).

Maass, H-H: *Information und Geheimnis im Zivilrecht* (Stuttgart: Ferdinand Enke, 1970).

Madsen, W: *Handbook of Personal Data Protection* (London: Macmillan, 1992).

Magnusson Sjöberg, C: *Rättsautomation* (Stockholm: Norstedts Juridik, 1992).

Mallmann, O: *Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information; mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen* (Frankfurt am Main: A Metzner, 1977).

Markgren, S: *Datainspektionen och skyddet av den personliga integriteten* (Lund: Studentlitteratur, 1984).

Marx, GT: *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988).

— & Reichman, N: 'Routinizing the Discovery of Secrets: Computers as Informants' (1985) 1 *Software LJ*, 95–121.

Matheson, W & Woxholth, G (eds): *Lovavdelingens uttalelser* (Oslo: Juridisk Forlag AS, 1990).

Maurer, U & Vogt, NP (eds): *Kommentar zum Schweizerischen Datenschutzgesetz* (Basel/Frankfurt am Main: Helbing & Lichtenhahn, 1995).

Mayer-Schönberger, V: 'Generational Development of Data Protection in Europe', in PE Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts: MIT Press, 1997), 219–241.

— 'The Internet and Privacy Legislation: Cookies for a Treat?' (1998) 14 *CLSR*, 166–174.

McBride, T: 'Coerced release of criminal history information' (1998) 5 *PLPR*, 119.

McGoldrick, D: *The Human Rights Committee: Its Role in the Development of the International Covenant on Civil and Political Rights* (Oxford: Clarendon Press, 1991).

McGuire, RP: 'The Information Age: An Introduction to Transborder Data Flow' (1979–80) 20 *Jurimetrics J*, 1–7.

Meissner, M: *Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht* (Frankfurt am Main: Peter Lang, 1998).

Mell, P: 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness' (1996) 11 *Berkeley Technology LJ*, 1–92.

Merrills, JG: *The Development of International Law by the European Court of Human Rights* (Manchester: Manchester University Press, 1993, 2nd ed).

Mestad, I: *Elektroniske spor: Nye perspektiver på personvern*, CompLex 3/86 (Oslo: Universitetsforlaget, 1986).

— 'Velferdsstat, folkehelsa og personvern' (1992) *Hefte for kritisk juss*, 204–216.

Michael, J: *The Politics of Secrecy* (Harmondsworth: Penguin, 1982).

— *Privacy and Human Rights. An International and Comparative Study, with Special Reference to Developments in Information Technology* (Paris/Aldershot: UNESCO/Dartmouth, 1994).

Michelman, F: 'Law's Republic' (1988) 97 *Yale LJ*, 1493–1537.

Miller, A: *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971).

Moore, B: *Privacy: Studies in Social and Cultural History* (Armonk: ME Sharpe, 1984).

Morgan, G: *Images of Organization* (London: Sage, 1986).

Morton, J: 'Data Protection and Privacy. R v Brown' [1996] 18 *EIPR*, 558–561.

Müller, PJ: 'Funktion des Datenschutzes aus soziologischer Sicht' (1974) 5 *DVR*, 107–118.

Mæland, JH: *Ærekrenkelser* (Bergen: Universitetsforlaget, 1986).

Napier, BW: 'International Data Protection Standards and British Experience' (1992) *Informatica e diritto*, no 1–2, 83–100.

Nékam, A: *The Personality Conception of the Legal Entity* (Cambridge, Massachusetts: Harvard University Press, 1938).

Nimmer, RT & Krauthaus, PA: 'Information as Property: Databases and Commercial Property' (1993) 1 *Int J of Law and Information Technology*, 3–34.

Nobel, P: 'Gedanken zum Persönlichkeitsschutz juristischer Personen', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Stämpfli & Cie, 1990), 411–425.

Novek, E; Sinha, N & Gandy, O: 'The Value of Your Name' (1990) 12 *Media, Culture & Society*, 525–543.

Nowak, M: *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Rhein/Strasbourg/Arlington: Engel, 1993).

Nugter, ACM: *Transborder Flow of Personal Data within the EC* (Deventer/Boston: Kluwer Law & Taxation, 1990).

Nyberg, B: *Samkörning av personregister*, IRI-rapport 1984:2 (Stockholm: Institutet för Rättsinformatikk, 1984).

O'Brien, DM: *Privacy, Law, and Public Policy* (New York: Praeger, 1979).

Olsson, AR: *IT och det fria ordet – myten om Storebror* (Stockholm: Juridik & Samhälle, 1996).

Parent, WA: 'A New Definition of Privacy for the Law' (1983) 2 *Law & Philosophy*, 305–338.

Patton, MQ: *Qualitative Evaluation and Research Methods* (Newbury Park/London/New Delhi: Sage, 1990, 2nd ed).

Pawlikowsky, GJ (ed): *Datenschutz: Leitfaden und Materialen* (Vienna: Orac, 1979).

Pennock, JR & Chapman, JW (eds): *Privacy: Nomos XIII* (New York: Atherton Press, 1971).

Peter, JT: *Das Datenschutzgesetz im Privatbereich* (Zurich: Schulthess Polygraphischer Verlag, 1994).

Pilon, R: 'Corporations and Rights: On Treating Corporate People Justly' (1979) 13 *Georgia L Rev*, 1245–1370.

Pinegar, KR: 'Privacy Protection Acts: Privacy Protectionism or Economic Protectionism?' (1984) 12 *Int Business Lawyer*, 183–188.

Posner, RA: 'The Right to Privacy' (1978) 12 *Geogia L Rev*, 393–422.

— 'Privacy, Secrecy and Reputation' (1979) 28 *Buffalo L Rev*, 1–55.

— 'An Economic Theory of Privacy', in FD Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), 333–345.

Post, RC: 'The Social Foundations of Privacy: Community and Self in the Common Law' (1989) 77 *California L Rev*, 957–1010.

Poster, M: *The Mode of Information: Poststructuralism and Social Context* (Cambridge: Polity Press, 1990).

Poullet, Y: 'Data Protection between Property and Liberties – A Civil Law Approach', in HWK Kaspersen & A Oskamp (eds), *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990), 161–181.

— & Poullet, D: 'Applicabilité aux Entreprises d'une Legislation protectrice des Données', paper given at conference entitled 'Banque de Données, Entreprises, Vie Privée', held in Namur, Belgium, 25–26 September 1979.

Prosser, WL: 'Privacy' (1960) 48 *California L Rev*, 338–423.

Raab, CD: 'Data Protection in Britain: Governance and Learning' (1993) 6 *Governance*, 43–66.

— 'Police Cooperation: The Prospects for Privacy', in M Andersen & M den Boer (eds), *Policing Across National Boundaries* (London/New York: Pinter, 1994), 121–136.

— 'Implementing data protection in Britain' (1996) 62 *Int Rev of Administrative Sciences*, 493–511.

— & Bennett, CJ: 'Protecting Privacy Across Borders: European Policies and Prospects' (1994) 72 *Public Administration*, 95–112.

Rachels, J: 'Why Privacy is Important' (1975) 4 *Philosophy & Public Affairs*, 323–333.

Raes, K: 'The Privacy of Technology and the Technology of Privacy: The Rise of Privatism and the Deprivation of Public Culture', in A Sajó & FB Petrik (eds), *High-Technology and Law: A Critical Approach* (Budapest: Institute of Political and Legal Sciences, Hungarian Academy of Sciences, 1989), 73–100.

— 'De skjulte dimensioner i rätten til privatliv' (1989) 12 *Retfærd*, no 45, 4–17.

Rankin, TM: 'Business Secrets across International Borders: One Aspect of the Transborder Data Flow Debate' (1985) 10 *Canadian Business LJ*, 213–246.

Rasmussen, H: 'Datenschutz im Internet' (2002) *CR*, no 1, 36–45.

Rasmussen, Ø: *Kommunikasjonsrett og taushetsplikt i helsevesenet* (Ålesund: AS Borgund, 1997).

Rawls, J: *A Theory of Justice* (Oxford: Oxford University Press, 1972).

— *Political Liberalism* (New York: Columbia University Press, 1993).

Redfern, P: 'Precise Identification through a Multi-Purpose Personal Number Protects Privacy' (1994) 1 *Int J of Law and Information Technology*, 305–323.

Regan, PM: 'Protecting Privacy and Controlling Bureaucracies: Constraints of British Constitutional Principles' (1990) 3 *Governance*, 33–54.

— *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill/London: University of North Carolina Press, 1995).

— 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics', in CJ Bennett & R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999), 199–216.

Reidenberg, JR: 'Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?' (1992) 44 *Federal Communications LJ*, 195–243.

— 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 *Texas L Rev*, 553–593.

— 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford L Rev*, 1315–1371.

— 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 *Houston L Rev*, 717–749.

Reiman, JH: 'Privacy, Intimacy, and Personhood' (1976) 6 *Philosophy & Public Affairs*, no 1, 26–44.

— 'Driving to the Panopticon' (1995) 11 *Santa Clara Computer & High Technology LJ*, 27–44.

Rigaux, F: *La protection de la vie privée et des autres biens de la personnalité* (Brussels/Paris: Bruylant/Libraire Générale de Droit et de Jurisprudence, 1990).

Rodotà, S: 'Privacy and Data Surveillance: Growing Public Concern', in *Policy Issues in Data Protection and Privacy* (Paris: OECD, 1976), 130–143.

— 'Policies and Perspectives for Data Protection', in *Beyond 1984: The Law and Information Technology in Tomorrow's Society*, Proceedings of the Fourteenth Colloquy on European Law held in Lisbon, 26–28 September 1984 (Strasbourg: CoE, 1985), 13–41.

— 'Protecting Informational Privacy: Trends and Problems', in WFK Altes, EJ Dommering, PB Hugenholtz & JJC Kabel (eds), *Information Law Towards the 21st Century* (Deventer/Boston: Kluwer Law & Taxation, 1992), 261–272.

Ross, A: *On Law and Justice*, trans M Dutton (London: Stevens & Sons Ltd, 1958).

Rothstein, MA (ed): *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (New Haven: Yale University Press, 1997).

Ruiz, BR: *Privacy in Telecommunications: A European and an American Approach* (The Hague/London/Boston: Kluwer Law International, 1997).

Rule, J: *Private Lives and Public Surveillance* (New York: Schocken, 1974).

— & McAdam, D; Stearns, L & Uglow, D: *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980).

— & McAdam, D; Stearns, L & Uglow, D: 'Preserving Individual Autonomy in an Information-Oriented Society', in LJ Hoffman (ed), *Computers and Privacy in the Next Decade* (New York: Academic Press, 1980), 65–87.

— & Hunter, L: 'Towards Property Rights in Personal Data', in CJ Bennett & R Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999), 168–181.

Rumbelow, C: 'Privacy and Transborder Data Flow in the UK and Europe' (1984) 12 *Int Business Lawyer*, 153–157.

Rumpf, H: 'Datenschutz für juristische Personen und Personenvereinigungen?' (1984) 13 *Datenverarbeitung – Steuer – Wirtschaft – Recht*, 135–143.

Rutgers, JA: 'Privacy Legislation, Data Protection, and Legal Persons', in *Transborder Data Flows*, Proceedings of an OECD Conference held December 1983 (Amsterdam: OECD/Elsevier, 1985), 393–397.

Rydén, N: *Företagsintegriteten i datasamhället* (Stockholm: Svenska Arbetsgivare-föreningen, 1986).

Saarenpää, A: 'Data Protection: In Pursuit of Information. Some Background to, and Implementations of, Data Protection in Finland' (1997) 11 *Int Rev of Law Computers & Technology*, 47–64.

Samuels, WJ & Miller, AS (eds): *Corporations and Society: Power and Responsibility* (New York: Greenwood Press, 1987).

Samuelsen, E: *Statlige databanker og personlighetsvern* (Oslo: Universitetsforlaget, 1972).

Sandström, M & Peterson, C: 'Lex Lata – Lex Ferenda. Fakta eller Fiktion?', in J Rosén (ed), *Lex Ferenda* (Stockholm: Juristförlaget/Norstedts Juridik, 1996), 159–177.

Schaar, P: 'Neues Datenschutzrecht für das Internet' (2002) *DVR*, no 1, 4–14.

Schack, DP: 'The right to privacy for business entities' (1984) 24 *Santa Clara L Rev*, 53–63.
Schartum, DW: *Rettssikkerhet og systemutvikling i offentlig forvaltning* (Oslo: Universitetsforlaget, 1993).
— 'Mot et helhetlig perspektiv på publikumsinteresser i offentlig forvaltning? – Rettssikkerhet, personvern og service' (1993) 16 *Retfærd*, no 63, 43–59.
— 'Dirt in the Machinery of Government? Legal Challenges Connected to Computerized Case Processing in Public Administration' (1995) 2 *Int J of Law and Information Technology*, 327–354 (also published in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 151–192).
— 'Proportional Control?' (1997) 11 *Int Rev of Law Computers & Technology*, 107–116.
— 'Den kontrollerende forvaltning' (1997) 20 *Retfærd*, no 77, 51–66.
Schoeman, FD: *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992).
— (ed): *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984).
Schwartz, B: 'The Social Psychology of Privacy' (1968) 73 *American J of Sociology*, 741–752.
Schwartz, PM: 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37 *American J of Comparative Law*, 675–701.
— 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 *Iowa L Rev*, 471–496.
— 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 *Iowa L Rev*, 553–618.
— 'Privacy and Democracy in Cyberspace' (1999) 52 *Vanderbilt L Rev*, 1609–1704.
— & Reidenberg, JR: *Data Privacy Law: A Study of United States Data Protection* (Charlottesville: Michie Law Publishers, 1996).
Schweizer, A: *Data Mining, Data Warehousing: Datenschutzrechtliche Orientierungshilfen für Privatunternehmen* (Zürich: Orell Füssli Verlag, 1999).
Schweizer, RJ: 'Europäisches Datenschutzrecht – Was zu tun bleibt' (1989) *DuD*, 542–546.
— & Sutter, P: 'Die Revision des Datenschutzgesetzes in der Schweiz' (2002) *DuD*, no 3, 156–161.
Seip, H: 'Unfair Competition in Computer Services?' (1981) 4 *TDR*, no 8, 33.
— 'More Countries to Protect Legal Person Data' (1982) 5 *TDR*, no 2, 105–108.
— 'Data Protection, Privacy and National Borders', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 67–82.
Seipel, P: *Computing Law* (Stockholm: Liber, 1977).
— 'Transnational Data Flows', in KE Johansson (ed), *Internationell företagsdataöverföring i juridisk belysning* (Stockholm: Sveriges Industriförbundets Förlag, 1981), 67–73.
— 'Transborder Flows of Personal Data: Reflections on the OECD Guidelines' (1981) 4 *TDR*, no 1, 32–44.
— (ed): *From Data Protection to Knowledge Machines* (Deventer/Boston: Kluwer Law & Taxation Publishers, 1990).
Selmer, KS: 'Elektronisk databehandling: Kan trollet temmes?' (1973) *LoR*, 195–215.

— 'Det stramme samfunn', in RD Blekeli & KS Selmer (eds), *Data og personvern* (Oslo: Universitetsforlaget, 1977), 27–39.
— 'Elektronisk databehandling og rettssamfunnet', in *Forhandlingene ved Det 30. nordiske juristmøtet, Oslo 15.–17. august 1984* (Oslo: Det norske styret for De nordiske juristmøter, 1984), Part II, 41–53.
— 'Datatilsynets kontroll med forvaltningen', in A Bratholm, T Opsahl & M Aarbakke (eds), *Samfunn, Rett, Rettferdighet: Festskrift til Torstein Eckhoffs 70-årsdag* (Oslo: TANO, 1986), 586–598.
— 'Innledning', in E Djønne, T Grønn & T Hafli, *Personregisterloven med kommentarer* (Oslo: TANO, 1987), 9–25.
— 'Borgenes vakthund – Forvaltningens vokter', in G Hansen, E Erichsen, H Sørebø, T Hafli & E Djønne (eds), *Mennesket i sentrum: Festskrift til Helge Seips 70-årsdag* (Oslo: TANO, 1989), 145–157.
— 'Datatilsynets rolle i et komplisert samfunn', in E Djønne (ed), *Datatilsynet - 10 år som personvernets vokter*, CompLex 4/90 (Oslo: TANO, 1990), 59–87.
— 'Hvem er du? Om systemer for registrering og identifikasjon av personer' (1992) *LoR*, 311–334.
— 'Realising Data Protection', in J Bing & O Torvund (eds), *25 Years Anniversary Anthology in Computers and Law* (Oslo: TANO, 1995), 41–65.
— 'Personvern og pasientvern', in *Oppsøkende genetisk veiledning* (Oslo: De nasjonale forskningsetiske komitéer, 1996), 39–46.
Shaffer, G: 'Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale J of Int L*, 1–88.
Shils, EA: 'Privacy: Its Constitution and Vicissitudes' (1966) 31 *Law & Contemporary Problems*, 281–306.
Sieghart, P: *Privacy and Computers* (London: Latimer, 1976).
Simitis, S: 'Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung' (1973) 2 *DVR*, 138–189.
— 'Die informationelle Selbstbestimmung – Grundbedingung einer verfassungs-konformen Informationsordnung' (1984) *Neue juristische Wochenschrift*, 398–405.
— 'Auf dem Weg zu einem neuen Datenschutzrecht' (1984) *Informatica e diritto*, no 3, 97–116 (also published as 'Reicht unser Datenschutzrecht angesichts der technischen Revolution? – Strategien zur Wahrung der Freiheitsrechte', in *Informationsgesellschaft oder Überwachungsstaat*, Proceedings of a symposium held by the Hessian State Government in Wiesbaden, 3–5 September 1984 (Wiesbaden: Hessendienst der Staatskanzlei, 1984), 27–48).
— 'Data Protection and Assault on Freedom of Information', in Council of Europe, *Legislative Problems of Data Protection*, Proceedings of a conference held in Madrid, 11–13 June 1984, on problems relating to legislation in the field of data protection (Madrid: Servicio Central de Publicaciones, 1986), 95–99.
— 'Reviewing Privacy in an Information Society' (1987) 135 *University of Pennsylvania L Rev*, 707–746.

— 'Datenschutz und Europäische Gemeinschaft' (1990) 6 *RDV*, 3–23.
— ''Sensitive Daten' – Zur Geschichte und Wirkung einer Fiktion', in E Brem, JN Druey, EA Kramer & I Schwander (eds), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Bern: Verlag Stämpfli & Cie, 1990), 469–493.
— 'New Trends in National and International Data Protection Law', in J Dumortier (ed), *Recent Developments in Data Privacy Law* (Leuven: Leuven University Press, 1992), 17–28.
— 'From the Market To the Polis: The EU Directive on the Protection of Personal Data' (1995) 80 *Iowa L Rev*, 445–469.
— 'The EU Directive on Data Protection and the Globalization of the Processing of Personal Data', paper presented at conference, 'Visions for Privacy in the 21st Century: A Search for Solutions', held in Victoria, British Columbia, Canada, 9–11 May 1996.
— 'Das Volkzählungsurteil oder der lange Weg zur Informationsaskese – (BVerfGE 65, 1)' (2000) 83 *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, no 3–4, 359–375.
— & Dammann, U; Mallmann, O & Reh, H-J: *Kommentar zum Bundesdatenschutzgesetz* (Baden-Baden: Nomos, 1981, 3rd ed).
— & Dammann, U; Geiger, H; Mallmann, O & Walz, S: *Kommentar zum Bundesdatenschutzgesetz* (Baden-Baden: Nomos, 1992, 4th ed).
— & Dammann, U & Körner, M (eds): *Data Protection in the European Community: The Statutory Provisions* (Baden-Baden: Nomos, 1992).
Slack, JD & Fejes, F (eds): *The Ideology of the Information Age* (Norwood, New Jersey: Ablex Publishing Corporation, 1987).
Stadler, G (ed): *Datenschutz*, Proceedings of the Vienna Conference on Data Protection held by the Austrian Commission of Jurists, April 1975 (Vienna: Österreichische Juristen-Kommission, 1975).
Stallworthy, M: 'Data Protection: Regulation in a Deregulatory State' (1990) 11 *Statute L Rev*, 130–154.
Steinmüller, W: 'Stellenwert der EDV in der Öffentlichen Verwaltung und Prinzipien des Datenschutzes' (1972) 2 *Öffentliche Verwaltung und Datenverarbeitung*, 453–462.
— 'Objektbereich 'Verwaltungsautomation' und Prinzipien des Datenschutzes', in W Kilian, K Lenk & W Steinmüller (eds), *Datenschutz* (Frankfurt am Main: Athenäum, 1973), 51–76.
— 'Fragestellungen der internationalen Datenschutzdiskussion', in G Stadler (ed), *Datenschutz*, Proceedings of the Vienna Conference on Data Protection held by the Austrian Commission of Jurists, April 1975 (Vienna: Österreichische Juristen-Kommission, 1975).
— *Informationsteknologie und Gesellschaft* (Darmstadt: Wissenschaftliche Buchgesellschaft, 1993).
Stepanek, M: 'Weblining: Companies are using your personal data to limit your choices – and force you to pay more for products', *Business Week Online*, 3.4.2000, <http://www.businessweek.com/2000/00_14/b3675027.htm>.

Stevenson, RB Jr: *Corporations and Information – Secrecy, Access, and Disclosure* (Baltimore: Johns Hopkins University Press, 1980).

Stewart, B: 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies' (1999) 5 *PLPR*, 147–149.

Stokes, M: 'Company Law and Legal Theory', in W Twining (ed), *Legal Theory and Common Law* (Oxford: Basil Blackwell, 1986), 155–166.

Strömholm, S: *Right of Privacy and Rights of the Personality: A Comparative Survey* (Stockholm: Norstedt, 1967).

Swire, PP & Litan, RE: *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998).

Székely, I: 'Hungary Outlaws Personal Number' (1991) 14 *TDR*, no 5, 25–27.

— 'New Rights and Old Concerns: Information Privacy in Public Opinion and in the Press in Hungary' (1994) 3 *Informatization and the Public Sector*, no 2, 99–113.

Taeger, J: 'Umweltschutz und Datenschutz' (1991) *CR*, 681–688.

Tapper, C: *Computer Law* (London: Longman, 1989, 4th ed).

Thomson, JJ: 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs*, 295–314.

Tomuschat, C: 'Freedom of Association', in RStJ Macdonald, F Matscher & H Petzold (eds), *The European System for the Protection of Human Rights* (Dordrecht/Boston/London: Martinus Nijhoff Publishers, 1993), 493–513.

Tuner, L: 'Gehört ein Datenschutz für juristische Personen ins allgemeine Datenschutzrecht?' (1985) *DuD*, 20–27.

Tuori, K: 'Interests and the Legitimacy of Law', in A Aarnio, SL Paulson, O Weinberger, GH von Wright & D Wyduckel (eds), *Rechtsnorm und Rechtswirklichkeit. Festschrift für Werner Krawietz zum 60. Geburtstag* (Berlin: Duncker & Humblot, 1993), 625–640.

Vandvik, R: *Individets og bedriftens integritet i data-alderen*, seminar paper, Norwegian School of Economics and Business Administration, 1970 (unpublished).

Vedder, A: 'Privatization, information technology and privacy: reconsidering the social responsibilities of organizations', in G Moore (ed), *Business Ethics: principles and practice* (Sunderland: Business Education Publishers, 1997), 215–226.

Velecky, LC: 'The Concept of Privacy', in JB Young (ed), *Privacy* (Chichester: Wiley, 1978), 13–34.

Volio, F: 'Legal Personality, Privacy and the Family', in L Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (New York: Columbia University Press, 1981), 185–208.

Wacks, R: 'The Poverty of Privacy' (1980) 96 *L Quarterly Rev*, 73–89.

— *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989).

— (ed): *Privacy*, International Library of Essays in Law & Legal Theory (Aldershot/Hong Kong/Singapore/Sydney: Dartmouth, 1993), Vols I & II.

— 'What has data protection to do with privacy?' (2000) 6 *PLPR*, 143–146, 155.

Walden, IN & Savage, RN: 'Data Protection and Privacy Laws: Should Organisations be Protected?' (1988) 37 *Int & Comparative L Quarterly*, 337–347.

Warner, M & Stone, M: *The Data Bank Society: Organizations, Computers and Social Freedom* (London: Allen & Unwin, 1970).
Warren, S & Brandeis, L: 'The Right to Privacy' (1890) 4 *Harvard L Rev*, 193–220.
Waters, N: case note on *C v ASB Bank Ltd* (1997) 4 *PLPR*, 116.
Weber, M: *The Theory of Social and Economic Organization*, trans AM Henderson & T Parsons (New York: Free Press, 1964).
Weizenbaum, J: *Computer Power and Human Reason. From Judgment to Calculation* (San Francisco: Freeman, 1976).
Westberg, P: 'Avhandlingsskrivande och val av forskningsansats – en idé om rättsvetenskaplig öppenhet', in L Heuman (ed), *Festskrift til Per Olof Bolding* (Stockholm: Juristförlaget, 1992), 421–446.
Westin, AF: *Privacy and Freedom* (New York: Atheneum, 1970).
— 'Civil Liberties and Computerized Data Systems', in M Greenberger (ed), *Computers, Communications, and the Public Interest* (Baltimore: The Johns Hopkins Press, 1971), 151–168.
— & Baker, MA: *Databanks in a Free Society: Computers, Record-Keeping, and Privacy* (New York: Quadrangle Books, 1972).
Wiik Johansen, M; Kaspersen, K-B & Bergseng Skullerud, ÅM: *Personopplysningsloven. Kommentarutgave* (Oslo: Universitetsforlaget, 2001).
Wormell, I: *Understanding Information* (Copenhagen: Danmarks Biblioteksskole, 1992).
Wright, J: 'Protection of Corporate Privacy' (1983) 6 *TDR*, no 4, 231–234.
Woxholth, G: *Foreningsrett* (Oslo: Ad Notam Gyldendal, 1999, 2nd ed).
— *Forvaltningsloven med kommentarer* (Oslo: Juridisk Forlag, 1993, 2nd ed).
Wuermeling, U: 'Multimedia Law – Germany' (1998) 14 *CLSR*, 41–44.
Young, JB (ed): *Privacy* (Chichester: Wiley, 1978).
Yurow, JH: 'National Perspectives on Data Protection' (1983) 6 *TDR*, no 6, 337–339.

B. Reports and other Documents

AUSTRALIA

(i) Federal Privacy Commissioner

Regulation of Data-Matching in Commonwealth Administration – Report to the Attorney-General (Sydney: Privacy Commissioner, September 1994).
Profiling and Privacy, Information Paper 2 (Sydney: HREOC, 1995).
Community Attitudes to Privacy, Information Paper 3 (Sydney: HREOC, 1995).
Minding our own business. Privacy protocol for Commonwealth agencies in the Northern Territory handling personal information of Aboriginal and Torres Strait Islander people (Sydney: Privacy Commissioner, 1998).
Privacy and the Community, July 2001, <http://www.privacy.gov.au/publications/rcommunity.html>.

(ii) New South Wales Privacy Committee

Guidelines for the Operation of Personal Data Systems, Background Paper 31 (Sydney: NSW Privacy Committee, 1977).

Privacy Protection: Guidelines or Legislation? (Sydney: NSW Privacy Committee, 1980).

(iii) Miscellaneous

Australian Law Reform Commission: *Privacy*, Report No 22 (Canberra: AGPS, 1983).

AUSTRIA

Regierungsvorlage in *72 der Beilagen zu den stenographischen Protokollen des Nationalrates XIV.GP 17.12.1975*.

CANADA

Canadian Standards Association: *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-1996 (Rexdale, Ontario: CSA, 1996).

Industry Canada & Justice Canada, Task Force on Electronic Commerce: *The Protection of Personal Information – Building Canada's Information Economy and Society* (Ottawa: Industry Canada/Justice Canada, 1998).

Ontario, Information and Privacy Commissioner: *Data Mining: Staking a Claim on Your Privacy*, January 1998, <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/datamine.htm>.

— & Registratiekamer of the Netherlands, *Privacy-Enhancing Technologies: The Path to Anonymity*, August 1995, <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm> (Vol 1); <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anoni-v2.pdf> (Vol 2).

COUNCIL OF EUROPE

(i) Resolutions

Resolution (73)22 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Private Sector (adopted 26.9.1973).

Resolution (74)29 on the Protection of the Privacy of Individuals *vis-à-vis* Electronic Data Banks in the Public Sector (adopted 24.9.1974).

(ii) Recommendations

Recommendation No R (83) 10 on the Protection of Personal Data used for Scientific Research and Statistics (adopted 23.9.1983).

Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector (adopted 17.9.1987).
Recommendation No R (89) 2 on the Protection of Personal Data used for Employment Purposes (adopted 18.1.1989).
Recommendation No R (91) 10 on the Communication to Third Parties of Personal Data Held by Public Bodies (adopted 9.9.1991).
Recommendation No R (95) 4 on the Protection of Personal Data in the Area of Telecommunications Services, with Particular Reference to Telephone Services (adopted 7.2.1995).
Recommendation No R (97) 5 on the Protection of Medical Data (adopted 13.2.1997).
Recommendation No R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes (adopted 30.9.1997).

(iii) Reports

Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg: CoE, 1981).
New Technologies: A Challenge to Privacy Protection? (Strasbourg: CoE, 1989).
The Introduction and Use of Personal Identification Numbers: The Data Protection Issues (Strasbourg: CoE, 1991).

DENMARK

(i) Data Protection Agency (formerly 'Registertilsynet'; now 'Datatilsynet')

Årsberetning 1981 (Copenhagen: Registertilsynet, 1982).
Årsberetning 1988 (Copenhagen: Registertilsynet, 1989).
Årsberetning 1989 (Copenhagen: Registertilsynet, 1990).
Årsberetning 1990 (Copenhagen: Registertilsynet, 1991).
Årsberetning 1992 (Copenhagen: Registertilsynet, 1993).

(ii) Miscellaneous

Delbetænkning om private registre, Bet 687 (Copenhagen: Statens trykningskontor, 1973).
Delbetænkning om offentlige registre, Bet 767 (Copenhagen: Statens trykningskontor, 1976).
Behandling af personoplysninger, Bet 1345 (Copenhagen: Statens Information, 1997).

EUROPEAN UNION

(i) Commission

Recommendation 81/679/EEC of 29.7.1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (OJ L 246, 29.8.1981, 31).

Press Release IP/95/822 of 25.7.1995: 'Council Definitively Adopts Directive on Protection of Personal Data'.

Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data (Luxembourg: Office for Official Publications of the EC, 1998).

Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (OJ L 215, 25.8.2000, 1).

Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary (OJ L 215, 25.8.2000, 4).

Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215, 25.8.2000, 7).

Decision 2001/497/EC of 15.6.2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, 19).

Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (OJ L 2, 4.1.2002, 13).

Decision 2002/16/EC of 27.12.2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (OJ L 6, 10.1.2002, 52).

Staff Working Paper: 'The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce', Brussels, 13.02.2002 (SEC(2002) 196), <http://europa.eu.int/comm./internal_market/en/dataprot/news/02-196_en.pdf>.

(ii) European Parliament

Legal Affairs Committee, Subcommittee on Data Processing and Individual Rights: *Verbatim record of the public hearing on data processing and the rights of the individual*, Brussels, 6.2.1978 (PE 52.496).

— *Report on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing* (the 'Bayerl Report') (EP Doc 100/79, PE 56.386 final, 4.5.1979).

Resolution of 8.5.1979 on the protection of the rights of the individual in the face of technical developments in data processing (OJ C 140, 5.6.1979, 34).

Resolution of 5.7.2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Principles and related Frequently Asked Questions issued by the US Department of Commerce (A5-0177/2000).

(iii) Data Protection Working Party (established under Art 29 of Directive 95/46/EC)

'Anonymity on the Internet', Recommendation 3/97 adopted 3.12.1997, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6.htm>.

'Notification', Working Document adopted 3.12.1997, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp8en.htm>.

'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', Working Document adopted 24.7.1998, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm>.

'Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware', Recommendation 1/99 adopted 23.2.1999, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm>.

'Privacy on the Internet: An Integrated EU Approach to On-line Data Protection', Working Document adopted 21.11.2000, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf>.

'Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000', adopted 26.1.2001, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40en.htm>.

GERMANY

Gesetzentwurf der Bundesregierung; Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Deutscher Bundestag, 13 Wahlperiode, Drucksache 13/7385, 9.4.1997).

NORWAY

(i) Parliamentary papers

Innst O 47 (1977–78), *Om lov om personregistre mm.*

Ot prp 2 (1977–78), *Om lov om personregistre mm.*

Ot prp 92 (1998–99), *Om lov om behandling av personopplysninger (personopplysningsloven).*

St meld 33 (1994–95), *Personvern og telekommunikasjon*.

(ii) Data Inspectorate (Datatilsynet)

St meld 103 (1981–82), *Datatilsynets årsmelding 1981*.

St meld 14 (1983–84), *Datatilsynets årsmelding 1982*.

St meld 23 (1985–86), *Datatilsynets årsmelding 1984*.

St meld 29 (1986–87), *Datatilsynets årsmelding 1985*.

St meld 48 (1987–88), *Datatilsynets årsmelding 1987*.

St meld 33 (1988–89), *Datatilsynets årsmelding 1988*.

St meld 37 (1989–90), *Datatilsynets årsmelding 1989*.
St meld 43 (1990–91), *Om personvern – erfaringer og utfordringer og om Datatilsynets årsmelding for 1990*.
St meld 18 (1992–93), *Datatilsynets årsmelding 1991*.
St meld 44 (1998–99), *Datatilsynets årsmelding 1998*.

(iii) NOU reports

Persondata og personvern, NOU 1974:22.
Offentlige persondatasytem og personvern, NOU 1975:10.
Pseudonyme helseregistre, NOU 1993:22.
Et bedre personvern – forslag til lov om behandling av personopplysninger, NOU 1997:19.

(iv) Miscellaneous

Den nasjonale forskningsetiske komité for medisin: *Registrering, bruk og gjenbruk av genetiske data* (Oslo: Norges forskningsråd, 1993).
Statistisk sentralbyrå (E Gulløy): *Undersøkelse om personvern: Holdninger og erfaringer 1997*, Notat 97/46 (Oslo: Statistisk sentralbyrå, 1997).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

(i) Guidelines

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980).
Guidelines for the Security of Information Systems (Paris: OECD, 1992).

(ii) Reports

Policy Issues in Data Protection and Privacy (Paris: OECD, 1976).
Privacy and Data Protection: Issues and Challenges (Paris: OECD, 1994).

SWEDEN

(i) SOU reports

Data och integritet, SOU 1972:47.
ADB och samordning, SOU 1976:58.
Personregister – datorer – integritet, SOU 1978:54.
Privatlivets fred, SOU 1980:8.
En ny datalag, SOU 1993:10.
Personnummer: Integritet och effektivitet, SOU 1994:63.
Grupprättegång, SOU 1994:151.
Integritet – Offentlighet – Informationsteknik, SOU 1997:39.

(ii) Miscellaneous

Data Inspection Board (Datainspektionen): *Rätten att få vara ifred – tio år med datainspektionen* (Lund: Studentliteratur, 1983).

SWITZERLAND

(i) Federal Data Protection Commissioner

1. Tätigkeitsbericht 1993/94, <http://www.edsb.ch/d/doku/jahresberichte/tb1/index.htm>.

2. Tätigkeitsbericht 1994/95, <http://www.edsb.ch/d/doku/jahresberichte/tb2/index.htm>.

3. Tätigkeitsbericht 1995/96, <http://www.edsb.ch/d/doku/jahresberichte/tb3/index.htm >.

4. Tätigkeitsbericht 1996/97, <http://www.edsb.ch/d/doku/jahresberichte/tb4/index.htm >.

5. Tätigkeitsbericht 1997/98, <http://www.edsb.ch/d/doku/jahresberichte/tb5/index.htm >.

(ii) Federal Council

Botschaft zum Bundesgesetz über den Datenschutz (DSG), 23 March 1988.

UNITED KINGDOM

(i) Data Protection Registrar (now 'Information Commissioner')

Fifth Report of the Data Protection Registrar, June 1989 (London: HMSO, 1989).

Tenth Report of the Data Protection Registrar, June 1994 (London: HMSO, 1994).

Thirteenth Report of the Data Protection Registrar, June 1997 (London: The Stationery Office, 1997).

Fourteenth Report of the Data Protection Registrar, June 1998 (London: The Stationery Office, 1998).

The Guidelines on the Data Protection Act 1984, Fourth Series (Wilmslow: Data Protection Registrar, 1997).

(ii) Official reports

Committee on Privacy (the Younger Committee): *Report of the Committee on Privacy*, Cmnd 5012 (London: HMSO, 1972).

Committee on Data Processing (the Lindop Committee): *Report of the Committee on Data Protection*, Cmnd 7341 (London: HMSO, 1978).

UNITED NATIONS

Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72).

UNITED STATES OF AMERICA

Congress, Office of Technology Assessment (OTA): *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, OTA-CIT-296 (Washington, DC: US Government Printing Office, June 1986).

Department of Health, Education and Welfare (DHEW), Secretary's Advisory Committee on Automated Personal Data Systems: *Records, Computers, and the Rights of Citizens* (Washington, DC: DHEW, 1973).

Federal Trade Commission: *Privacy Online: A Report to Congress*, June 1998, <http://www.ftc.gov/reports/privacy3/priv-23a.pdf>.

— *Online Profiling: A Report to Congress*, June 2000, <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

Information Infrastructure Task Force: *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, June 1995, <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

Privacy Protection Study Commission: *Personal Privacy in an Information Society* (Washington, DC: US Government Printing Office, 1977).

MISCELLANEOUS

Austin, RV: *Data Protection Legislation: Information Paper on the Legal Person Issue*, ICC Document No 372/8 (Paris: ICC, 1980).

Bancilhon, F; Chamoux, J-P; Grissonanche, A & Joinet, L: 'Das Problem natürliche Person/andere rechtliche Einheiten', in *Studie über Datenschutz und Datensicherheit*, Final Report to the EC Commission by the Gesellschaft für Mathematik und Datenverarbeitung, the Institut de Recherche d'Informatique et d'Automatique and the National Computing Centre, May 1980, vol 3.

Bangemann, M *et al*: *Europe and the Global Information Society. Recommendations to the European Council* (Brussels, 26.5.1994).

Borking, JJ; van Eck, BMA & Siepel, P: *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector* (The Hague: Registratiekamer, 1999).

Business International Corporation: *Transborder Data Flow: Issues, Barriers and Corporate Responses* (New York: Business International Corporation, 1983).

Electronic Privacy Information Center (EPIC) & Privacy International (PI): *Privacy and Human Rights 2001. An International Survey of Privacy Laws and Developments* (Washington, DC: EPIC/PI, 2001).

Fédération nationale des associations de consommateurs du Québec (FNACQ) & Public Interest Advocacy Centre (PIAC): *Surveying Boundaries: Canadians and Their Personal Information* (Ottawa/Quebec: FNACQ/PIAC, 1995).

Korff, D: *Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data relating to such Persons*, report for EC Commission,

October 1998, <http://europa.eu.int/comm/internal_market/en/dataprot/studies/legalen.htm>.

Hogrebe, E: *Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues*, report for OECD Working Party on Information, Computer and Communications Policy (DSTI/ICCP/81.25).

Instituttet for Fremtidsforskning: *Danskernes holdninger til informationsteknologi* (Copenhagen: Post Danmark, 1996).

International Chamber of Commerce: 'Policy Statement on Privacy Legislation, Data Protection and Legal Persons' (1984) 7 *TDR*, no 7, 425–427.

International Labour Office (ILO): *Protection of Workers' Personal Data* (Geneva: ILO, 1997).

International Working Group on Data Protection in Telecommunications: 'Common Position on Intelligent Software Agents', adopted 29.4.1999, <http://ig.cs.tu-berlin.de/~dsb/doc/int/iwgdpt/agent_en.htm>.

— 'Common Position on Data Protection and Search Engines on the Internet', adopted 15.4.1998, <http://ig.cs.tu-berlin.de/~dsb/doc/int/iwgdpt/find_en.htm>.

Law Reform Commission of Hong Kong: *Report on Reform of the Law Relating to the Protection of Personal Data* (Hong Kong: Government Printer, 1994).

Louis Harris & Associates (in association with AF Westin): *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes toward Privacy* (Stevens Point, Wisconsin: Sentry Insurance, 1979).

— *Equifax Canada Report on Consumers and Privacy in the Information Age* (Ville d'Anjou: Equifax Canada, 1995).

— *Harris-Equifax Mid-Decade Consumer Privacy Survey 1995* (Atlanta: Equifax, 1995).

Nordic Council of Ministers: *Grupptalan i konsumentmål – Rapport från ett nordiskt seminarium*, Nord 1990:51, NEK-rapport 1990:7 (Copenhagen: Nordic Council of Ministers, 1990).

— *Information Security in Nordic Countries*, Nordiske Seminar- og Arbejdsrapporter 1993:613 (Copenhagen: Nordic Council of Ministers, 1993).

Reidenberg, JR & Schwartz, PM: *Data Protection Law and On-Line Services: Regulatory Responses*, report for Directorate General XV of the EC Commission, December 1998, <http://europa.eu.int/comm/internal_market/en/dataprot/studies/regul.htm>.

Rossnagel, A; Pfitzmann, A & Garstka, H: *Modernisierung des Datenschutzrechts*, report for the German Federal Ministry of the Interior (Bundesministerium des Innern), September 2001, <http://www.bmi.bund.de/downloadde/11659/Download.pdf>.

Index

Information Law Series

1. *Protecting Works of Fact: Copyright, Freedom of Expression and Information Law*, Egbert J. Dommering and P. Bernt Hugenholtz (eds)
   ISBN 90-6544-5676

2. *Information Law Towards the 21st Century*, Willem F. Korthals Altes, Egbert J. Dommering, P. Bernt Hugenholtz and Jan J.C. Kabel (eds)
   ISBN 90-6544-6273

3. *Challenges to the Creator Doctrine*, Jacqueline Seignette
   ISBN 90-6544-8764

4. *The Future of Copyright in a Digital Environment*, P. Bernt Hugenholtz (ed)
   ISBN 90-411-0267-1

5. *From Privacy Toward a New Intellectual Property Right in Persona*, Julius C.S. Pinckaers
   ISBN 90-411-0355-4

6. *Intellectual Property and Information Law: Essays in Honour of Herman Cohen Jehoram*, Jan J.C. Kabel and Gerard J.H.M. Mom (eds)
   ISBN 90-411-9702-8

7. *Copyright and Photographs: An International Survey*, Ysolde Gendreau, Axel Nordemann and Rainer Oesch (eds)
   ISBN 90-411-9722-2

8. *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management*, P. Bernt Hugenholtz (ed.)
   ISBN 90-411-9785-0

9. *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright*, Lucie M. C. R. Guibault
   ISBN 90-411-9867-9

10. *Data Protection Law: Approaching its Rationale, Logic and Limits*, Lee Bygrave
    ISBN 90-411-9870-9

11. *The Commodification of Information*, Niva Elkin-Koren and Neil Weinstock Netanel (eds)
    ISBN 90-411-9876-8

DATA PROTECTION LAW

Approaching Its Rationale, Logic and Limits

Lee A. Bygrave

Despite the proliferation of data protection laws (or privacy protection laws) in many countries, uncertainty still reigns as to who or what such laws actually protect. Most data protection laws seem to have been drawn up rather diffusely, with the justification that the huge variety of types of information and specific contexts give rise to a complexity that cannot be guessed at as information technology continues to develop.

Nevertheless, as this ground-breaking book demonstrates, it is essential to understand as best we can why data protection laws are passed, what their regulatory mechanisms are, and wherein lies their particular effectiveness. *Data Protection Law* approaches such an analysis along three major avenues of investigation:

- the interests and values that seem to be promoted by data protection laws;
- the extent to which the processing of information on private collective entities should be regulated by these laws; and
- the ability of these laws to control profiling practices.

The author evaluates in detail the costs and/or gains and the interference (positive or negative) in the commercial, public administrative, and social spheres that data protection laws have the potential to create, with numerous references to legislation and administrative decision making in a wide variety of jurisdictions.

Data Protection Law promises to become a cornerstone in the new edifice of legal scholarship in this field. With its penetrating clarification of new and complex legal issues, its focus on interests and values, and its interdisciplinary methodology, it will be of immense usefulness to lawyers, scholars, regulators, and policymakers in this burgeoning area of the law.

ISBN 90-411-9870-9

INFO 10

9 789041 198709