ACCOUNTABILITY UNCHAINED: BULK DATA RETENTION, PREEMPTIVE SURVEILLANCE, AND TRANSATLANTIC DATA PROTECTION

Kristina Irion

INTRODUCTION

The innovations on which today's Internet proliferated have been a major gift from its founders and the U.S. government to the world. Ever since the rise of the Internet it has attracted utopian ideas of a free and borderless cyberspace, a man-made global commons that serves an international community of users. First commercialization and now the prevalence of state surveillance have significantly depreciated the utopian patina.

The Internet's borderless nature, which was once heralded as rising above the nation state, has actually enabled some states to rise above their borders when engaging in mass surveillance that affects users on a global scale. International human rights law and emerging Internet governance principles have not been authoritative enough to protect users' privacy and the confidentiality of communications.[1]

Kristina Irion is Assistant Professor at the Department of Public Policy and Research Director, Public Policy, with the Center for Media and Communications Studies (CMCS) at Central European University.

More or less openly, Western democracies embarked on the path of mass surveillance with the aim of fighting crime and defending national security. Although country-specific approaches vary, reflecting political and ideological differences, mass surveillance powers frequently raise issues of constitutional compatibility. Beyond striking a balance between public security and privacy, systemic surveillance carries the potential to erode democracy from the inside.[2]

This chapter's focus is on the safeguards and accountability of mass surveillance in Europe and the United States and how these affect transatlantic relations. It queries whether national systems of checks and balances are still adequate in relation to the growth and the globalization of surveillance capabilities. Lacking safeguards and accountability at the national level can exacerbate transnational surveillance. It can lead to asymmetries between countries that are precisely at the core of the transatlantic rift over mass surveillance. The chapter concludes with a brief review of proposals for how to reduce them.

FROM TARGETED TO MASS SURVEILLANCE

As a transcendent technology, communications permeates every aspect of contemporary life because it satisfies humans' need to socialize and connect with others. Apart from the actual content of electronic communications, metadata[3] and log files are routinely available by-products, which can be used to reconstruct the circumstances of a communications event. The framework for the state's legitimate interferences with communications content and metadata is called "lawful" interception

authority, which can be further broken down into intelligence and law enforcement powers.

Due to various technical and ideological leaps, surveillance capabilities could expand exponentially. Wiretapping electronic communications has become low-hanging fruit since it is now technically feasible to access, copy, store, and analyze large amounts of electronic communications. Moreover, Internet traffic does not conform to the political geography offline; instead the topography of cyberspace gravitates toward Western countries, in particular the United States. At neuralgic points, such as core infrastructure and popular online services, international communications are especially exposed to wiretapping.[4]

Against the backdrop of counterterrorism and the fight against crime surveillance, ideology appears to have morphed with technological determinism, where feasibility determines strategies. The two new strategies that have been added to the arsenal of "lawful" interception are preemptive monitoring[5] and bulk data retention.[6] Both aim at whole populations of inconspicuous users, which marks a quantitative and qualitative shift away from targeted surveillance.

On both sides of the Atlantic, this trend is reflected in the passing of legislation that authorizes transnational surveillance, notably the 2008 U.S. FISA Amendment Act[7] and the national intelligence laws of the UK, Sweden, France, and Germany.[8] From what has been revealed by international news media, the United States and the UK are believed to engage in the large-scale upstream collection of electronic communications while the other countries may not command comparable capabilities as of yet.[9]

NEW SURVEILLANCE MEETS ACCOUNTABILITY STANDARDS

In its 2013 resolution "The Right to Privacy in the Digital Age," the United Nations General Assembly affirms that fundamental rights apply undiminished online, including the right to privacy.[10] Mass surveillance constitutes a particularly serious interference with the right to privacy, notwithstanding if it is actually taking place or a lingering threat as long as individuals form an impression of surveillance. Privacy has a supporting function for the exercise of other fundamental rights and collective freedoms, notably the freedom of speech and assembly, which jointly underpin the functioning of democracy.

Democracies' respect for fundamental rights would already dictate substantive boundaries curtailing surveillance powers and complementary safeguards against excesses and abuse thereof. As a recent report from the Center for European Policy Studies explained, "It is the purpose and the scale of surveillance that are precisely at the core of what differentiates democratic regimes from police states."[11]

Moreover, state actions are situated within the chain of democratic legitimization, which is the reason for insisting on a precise surveillance mandate but also for ex post facto measures to hold competent authorities accountable for their actions. Together, the protection of fundamental rights and democratic accountability make a strong argument for claiming that at the national level surveillance should be nested in rigorous checks and balances.

Every country has its unique system of constitutional protections, safeguards, and due process requirements that surveillance

measures have to comply with. However, these arrangements evolved in the context of targeted surveillance of limited capacity, with intelligence work being a secretive affair conducted under equally closed oversight mechanisms.[12] Without significant modifications, mass monitoring has been fitted inside these arrangements, although the circumstances are to an appreciable extent different.

Preemptive and systemic surveillance exceeds qualitatively and quantitatively the situation of targeted surveillance. It is incumbent upon the states that issued these new powers to revise these mandates to correspond with national constitutions and international human rights law. The 2014 NETmundial multistakeholder meeting resolved that

> procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, [. . .] should be reviewed, with a view to upholding the right to privacy.[13]

This would involve revisiting taken-for-granted intelligence paradigms, such as secrecy, discretionary powers, and national security exemptions,[14] to name just a few, in relation to large-scale surveillance programs.

Ultimately, the legitimacy of electronic surveillance is increasingly intertwined with the classical set of checks and balances associated with government accountability. The 2013 resolution of the United Nations General Assembly calls on states to

> establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as ap-

> propriate, and accountability for state surveillance of communications, their interception and collection of personal data.[15]

States are responsible for devising safeguards that would afford a measure of transparency, supervision, and accountability commensurate with the dangers of the state's interference in fundamental rights and the risks for democratic institutions.

TRANSPARENCY

At the most basic level, transparency is certainly appropriate with regard to the statutes that should afford clarity on the scope, boundaries, and consequences of surveillance powers.[16] However, it is often not possible to infer from the legal mandate this information with certainty without accessing accompanying but classified interpretations.[17] In many instances, the exact meaning of surveillance authorities remains largely abstract to the public, unless they make headlines that would convey a more accessible account.

The flip side of legal certainty is that generalized terms in statutes may actually not contain surveillance powers but involuntarily facilitate their expansion. Bigo et al. state that

> law-making has not kept pace with the technological developments seen in surveillance practices in recent years, often designed for traditional intelligence techniques such as wiretapping.[18]

Transparency is a prerequisite of accountability, and where it is not mission-critical, the cloak of secrecy that covers entire electronic surveillance programs by national intelligence

should be lifted.[19] The knowledge about the mere existence of blanket surveillance schemes is not equally as compromising as it would be for targeted actions. To the contrary, democratic societies should rethink the contours of secrecy, because the public sacrifice to national security must be transparent to its constituency.

A principle flowing from both due process and Fair Information Practices is that individuals should be informed when access to their data has been given to intelligence services.[20] What should be uncontroversial is the release on an annual basis of statistical data about electronic surveillance that provides accessible and meaningful information about its scope, scale, origin, and effects.

SUPERVISION

At the national level, supervision of surveillance powers is also not static but an evolving concept that has already been responsive to emerging needs. For example, parliamentary and/or judicial oversight of the activities of national intelligence agencies is now widely accepted, but for some countries this is a relatively recent development.[21] Local arrangements of supervision are very diverse but have certain structural elements in common, such as a combination of internal and external oversight with a link to democratic accountability. The efficiency of external supervision mechanisms remains a matter of concern, often due to a lack of independence, competences, resources, and even information.[22]

Additionally, large-scale electronic surveillance calls for new directions in supervision that are cognizant of compliance with

relevant data protection standards. The assembly of EU data protection authorities considers that

> an effective and independent supervision of intelligence services implies a genuine involvement of the data protection authorities. [. . .] This [oversight] should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers.[23]

Even where data protection authorities will not play the envisaged role, oversight has to extend to the systems and schemes used for data collection and processing in electronic communications surveillance.

Independent judicial oversight and access to justice continue to make inroads toward upholding the rule of law in the context of electronic surveillance. Aside from national courts, the two top European courts, in Strasbourg (European Court of Human Rights) and Luxembourg (Court of Justice of the European Union), quite frequently now decide on instruments of electronic surveillance. Their respective case law covers preemptive surveillance and the retention of communications metadata, with two more cases pending concerning electronic mass surveillance in Sweden and the UK.[24] Both courts stress the role of "adequate and effective guarantees against abuse" and "substantive or procedural conditions" that would limit the interference with fundamental rights to what is necessary and proportionate.

ACCOUNTABILITY

Accountability is valid currency in government and privacy protection, interests that converge in state surveillance of electronic communications. At an institutional level, accountability requires that an organization take appropriate and effective measures to ensure internal compliance with relevant laws and procedures. For authorities competent to conduct electronic surveillance, assuming internal accountability should be an evident consequence of deriving their mandate from statutes. However, accountability cannot be treated as an internal affair but must be demonstrated and verifiable if necessary. Hence, accountability is linked to internal checks and external supervision.

With a view to accountability, there are some striking parallels between independent regulatory agencies, such as energy regulators and central banks, and those national authorities competent to conduct electronic surveillance. In both cases, there is a delegation of competences from the state to an authority that enjoys a special status vis-à-vis the government, which requires a more sophisticated setup to protect the status and mandate of the agency while ensuring that in their operations they remain accountable to the public interest, the national constitution, and democracy at large.

In democracies, through general elections governments can be held accountable to the citizens, including for the extent of state surveillance. Admittedly, democratic accountability is a broad concept in which issues of surveillance compete with other salient policies. Nonetheless, surveillance touches upon a principle relationship between the state and the citizens, which in some countries may become a premise for parties' ideological

differentiation. For a global user community democratic accountability cannot be achieved, except indirectly via the proxy of the local electorate.

TRANSATLANTIC SURVEILLANCE ASYMMETRIES

Over the last decade, EU-U.S. relations have been probed by transnational surveillance in a variety of areas.[25] The 2013 revelations in international news media about U.S. and UK electronic mass surveillance programs as well as a flourishing transatlantic intelligence cooperation reached a new climax. While national security is not part of its remit, the EU finds itself in the difficult position of having to defend the fundamental rights of European citizens against U.S. surveillance in a context where several EU member states, such as the UK, Sweden, France, and Germany, are implicated in mass surveillance to varying degrees.[26]

EU institutions are particularly alarmed by the massive violation of European citizens' fundamental rights through the suspected unfettered surveillance of electronic communications.[27] Interpretations of the U.S. FISA section 702 powers come to the conclusion that it permits the warrantless interception of international communications during transit through the United States and the targeting of non-U.S. persons reasonably believed to be located outside the United States.[28] However, several EU member states, for example Germany, Sweden, and the UK, follow a similar approach.[29]

The distinction between domestic and international communications is a legacy of telecommunications, when this was a

straightforward exercise. The political geography was ingrained in the public switched telephony network, but this is no longer the case with decentralized Internet traffic. By maintaining the distinction between domestic and external communications, national surveillance could subtly expand in scope with mass surveillance capabilities adding scale. In practice, this distinction is hard to sustain, which calls into question the rationale of keeping it intact.[30]

This leads to a key difference between the United States and Europe, i.e., regional human rights with supranational oversight by an international court.[31] The European Convention on Human Rights protects the privacy of the correspondence of everyone in the territory of a member state of the Council of Europe. The European Court of Human Rights, based in Strasbourg, reviews the compatibility of member state actions with the convention, and its jurisprudence on domestic surveillance laws offers a rich framework of reference on their legality.[32] By contrast, Europeans have no agency to protect them from U.S. surveillance.

EU politics is now exploring a wide array of strategies that would reestablish the respect for European citizens' fundamental rights online at various levels. In several fora the transatlantic dialogue continues with the aim of entering into bilateral agreements and reviving the EU-U.S. Mutual Legal Assistance Agreement (MLAA). International law, however appealing, may not bring about the desired change for the simple reasons that it would have little to add to existing international human rights law and that national security exceptions may prove highly resistant.

At the EU level, the general data protection framework

restricts the transfer of personal data originating in the EU to nonmember countries, which, under the risk of electronic surveillance, may be further restricted to prohibit passing on personal data for the purpose of national security. This would primarily create a conflict of law on the part of the organizations processing such data, for example in the context of business. There are also various initiatives that explore the feasibility of European services capable of evading U.S. surveillance, such as certified e-mail services, EU preferential routing, and European cloud legislation, among others.

Outside politics, the loss of trust in Internet communications and services develops its own dynamic in which public- and private-sector organizations are increasingly risk-averse. If government cloud computing makes a good indicator, then organizations change strategies in acquisition of IT services with a view to avoiding the legal risks of foreign intelligence gathering.[33] There are also signs that Internet users are increasingly open to privacy-enhancing technologies, such as anonymous browsing and encryption. When diplomacy has no leverage to tame surveillance, the real pressure is economic.

NOTES

1. See UN News Center, "General Assembly backs right to privacy in digital age," December 19, 2013; NETmundial, "NETmundial Multistakeholder Statement," São Paulo, Brazil, April 24, 2014.
2. The European Court of Human Rights (ECtHR) observes that "a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it." See *Gabriele Weber and Cesar Richard Savaria v.*

Germany, ECtHR no. 54934/00, decision of June 29, 2006, para. 106. Cf. D. Bigo et al., "Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law," study for the European Parliament (Brussels: European Union, 2013), 5, 14.

3. In U.S. terminology metadata is called "call-detail records" (CDR); in the EU metadata is referred to as "traffic data."
4. Cf. Bigo, et al., "Mass Surveillance of Personal Data," 20; C. Bowden, "The U.S. surveillance programmes and their impact on EU citizens' fundamental rights," study for the European Parliament (Brussels: European Union, 2013), 13f.
5. Preemptive monitoring concerns the collection of electronic communications or related data according to fairly broad parameters with a view to subsequent analysis intended to detect dangers for national and/or public security.
6. Bulk data retention is a method of data preservation over a certain period of time so that it is thus available for retroactive investigations into electronic communications by competent authorities.
7. U.S. Congress, Foreign Intelligence Surveillance Act of 1978 Amendments of 2008, 122 Stat. 2436, Public Law 110–261, section 702.
8. For a list in order of estimated magnitude, see Bigo et al., "Mass Surveillance of Personal Data," 19f.
9. Ibid.
10. UN General Assembly, "The Right to Privacy in the Digital Age," resolution adopted at the sixty-eighth General Assembly on December 18, 2013, 4(d).
11. Bigo et al., "Mass Surveillance of Personal Data," 5.
12. Regarding EU member states, see Article 29 Working Party, Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes, adopted on April 10, 2014, 9f.; Bigo et al., "Mass Surveillance of Personal Data."
13. NETmundial, "NETmundial Multistakeholder Statement."

14. According to the Article 29 Working Party, "there is no automatic presumption that the national security argument used by a national authority exists and is valid. This has to be demonstrated." Article 29 Working Party, Opinion 04/2014, 6.
15. UN General Assembly, "The Right to Privacy in the Digital Age," 4(d).
16. In Europe, following the ECtHR, "foreseeability" is a prerequisite quality of the law; see *Weber and Savaria v. Germany*, paragraphs 84ff.; *Case of Liberty and Others v. the United Kingdom*, no. 58243/00 (ECtHR, judgment of July 1, 2008), paragraphs 66–67.
17. For example, in the absence of an authoritative interpretation of the surveillance powers, legal accounts of the powers under section 702 of the 2008 FISA amendment are often vaguely dismissed as wrong or exaggerated. See for example U.S. Mission to the EU, "Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US" (2012).
18. Bigo et al., "Mass Surveillance of Personal Data," 25.
19. For European standards, the resistance against data retention laws resembled class actions: 11,128 Austrians filed a lawsuit, cf. *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12 (CJEU, judgment of 8 April 2014); against the German data retention law, 34,939 individuals went to court, cf. BVerfG, 1 BvR 256/08 (German Federal Constitutional Court, judgment of March 2010), BVerfGE 125, 260.
20. Article 29 Working Party, Opinion 04/2014, 2.
21. Bigo et al., "Mass Surveillance of Personal Data," 13.
22. Ibid., 26.
23. Article 29 Working Party, Opinion 04/2014, 8.
24. *Weber and Savaria v. Germany*, *Case of Liberty and Others v. the United Kingdom*, *Digital Rights Ireland and Seitlinger and Others*. Pending: *Centrum för rättvisa v. Sweden*, 35252/08 (ECtHR, application of July 14, 2008); *Big Brother Watch and others vs. the*

United Kingdom, 58170/13 (ECtHR, application of September 4, 2013).

25. For example the global satellite interception system ECHELON, the US-VISIT-related extraction of passenger name records in air transport, and the exploitation of SWIFT data under the U.S. Terrorist Finance Tracking Program.
26. Bigo et al., "Mass Surveillance of Personal Data," 27.
27. See "European Parliament resolution on the U.S. National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy," 2013/2682(RSP), July 4, 2013.
28. Bowden, "The U.S. surveillance programmes and their impact," 19; K. Irion, "International Communications Tapped for Intelligence-Gathering," *Communications of the ACM* 52, no. 2 (February 2009): 26.
29. Bigo et al., "Mass Surveillance of Personal Data," 22.
30. Ibid.
31. Irion, "International Communications Tapped for Intelligence-Gathering," 28. NB: The EU Charter of Fundamental Rights does also afford the fundamental rights to privacy and to data protection for everyone; however, member states' surveillance laws fall outside EU authority and thus review mechanisms.
32. See notes 16 and 24.
33. K. Irion, "Government Cloud Computing and the National Data Sovereignty," *Policy and Internet* 4, no. 3 (2012): 40–41.