The Right to Root: Constructing a Claim to Control Devices from the Right to Privacy

by **Ot van Daalen** *

Abstract: Empowering people with digital tools has been an enduring ideal throughout the history of computing. In some of the earlier visions, this was not only a matter of making life easier, it was also a matter of people gaining control over their digital tools. One solution to this problem which has been suggested is to provide users with a manual override to gain full control over a device, something called gaining 'root' – hence the 'Right to Root'. Yet, there are no policymakers who have seriously treated this as a possibility. For people pushing this right at a policy level, it would therefore be helpful to know whether this Right to Root can be constructed from human rights. In this article, I explore the European human rights-based arguments for a Right to Root, focusing on the right to privacy under the European Convention for Human Rights and the Charter of Fundamental Rights. I first discuss the origins of this ideal of gaining control over your own devices. I then show how users over the years have gained less control and how the Right to Root could enable them to regain control. I then explore how the Right to Root could be constructed from the right to privacy under the Convention and the Charter, by understanding it as a way to protect the values of autonomy, self-determination and seclusion. I conclude that a Right to Root can be grounded in the human right to privacy, but that further research is necessary to balance it with other interests, such as cybersecurity, traffic safety, health and intellectual property.

Keywords: Privacy; Self-Determination; Smart Devices; The Right to Root

Recommended citation: Ot van Daalen, The Right to Root: Constructing a Claim to Control Devices from the Right to Privacy 14 (2023) JIPITEC 580 para 1.

A. Introduction [1] [2]

1 Empowering people with digital tools has been an enduring ideal throughout the history of computing. In some of the earlier visions, this was not only a matter of making life easier, it was also a matter of people gaining *control* over their digital tools. But this vision never really materialised. Most of the devices we currently use, from smartphones to cars, are locked down, often collecting private data, while being controlled remotely. This locking down, data collection and remote control is enforced through information security measures – measures which are often difficult, and sometimes illegal to circumvent. As a result, although most people currently own their devices, only few actually control them.

2 One solution to this problem which has been suggested is to provide users with a manual override

1 * Ot van Daalen is assistant professor at the Institute for Information Law of the University of Amsterdam and founder of law firm Root Legal. He can be reached at o.l.vandaalen@uva.nl.

2 This work was supported by the Netherlands Organisation for Scientific Research (NWO), as part of the Quantum Software Consortium programme (project number 024.003.037 / 3368). Elements of this work are part of a PhD which was defended in October 2022: O.L. van Daalen, Making and Breaking with Science and Conscience: The Human Rights-Compatibility of Information Security Governance in the Context of Quantum Computing and Encryption (Van Daalen Press 2022).

to gain full control over a device, something called gaining "root" – hence the "Right to Root."[3] Yet, there are no policymakers who have seriously entertained this as a possibility. For people pushing this right at a policy level, it would therefore be helpful to know whether this Right to Root can be constructed from human rights.

3 This question, however, has received little scholarly attention to date, and most scholars which analysed this topic have done so from a US perspective. US-based Joshua Fairfield suggested in 2017 a "right to hack", based on the concept of ownership, which would also entail giving users the possibility of gaining root, but his analysis is grounded in US law.[4] Ido Kilovaty has argued that people should have the freedom to hack their devices, but this should be so in order to fix vulnerabilities found in these devices.[5] Pam Samuelson has argued that limitations on the "freedom to tinker" hamper competition, innovation and tinkererers' interests, and that this calls for restrictive interpretation of IP rules – but she does not ground this in human rights, and does not explicitly call for a Right to Root.[6] The right to repair, recently gaining traction in US and the EU, is somewhat related to the Right to Root, but it is primarily based on sustainability considerations, not human rights.[7] Finally, Ohm and Kim suggest the right to turn off the "smart" functions of devices; while Hoofnagle, Kesari and Perzanowski analyse some of the issues with "tethered devices" and suggest a "kill switch" – solutions which point in the direction, but fall short of gaining full control over a device.[8]

4 In this article, I explore the European human rights-based arguments for a Right to Root, focusing on the right to privacy under the European Convention for Human Rights (the Convention) and the Charter of Fundamental Rights (the Charter).[9] This exploration involves clearing two significant hurdles. First, it requires connecting the idea of control over devices with the right to privacy – a link which is not necessarily intuitive. Then, it requires support for the claim that freedom requires gaining *full* control, or "root".

5 I attempt to clear these hurdles by first discussing the origins of this ideal of gaining control over

3 See Cory Doctorow, "The Coming Civil War over General Purpose Computing" (August 23, 2012) <https://memex.craphound.com/2012/08/23/the-coming-civil-war-over-general-purpose-computing/> accessed May 28, 2021; Erica Portnoy and Peter Eckersley, "Intel's Management Engine Is a Security Hazard, and Users Need a Way to Disable It" (May 8, 2017) <https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it> accessed December 28, 2021.

4 Joshua A. T. Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (Cambridge University Press 2017), in particular ch. 8.

5 Ido Kilovaty, "Freedom to Hack" (2019) 80 Ohio State Law Journal 455 <https://kb.osu.edu/bitstream/handle/1811/88006/1/OSLJ_V80N3_0455.pdf> accessed March 24, 2023.

6 Pamela Samuelson, "Freedom to Tinker" (2016) 17 Theoretical Inquiries in Law 563.

7 See for example Anthony D Rosborough, Leanne Wiseman and Taina Pihlajarinne, "Achieving a (Copy)Right to Repair for the EU's Green Economy" [2023] Journal of Intellectual Property Law and Practice <https://academic.oup.com/jiplp/advance-article/doi/10.1093/jiplp/jpad034/7147057> accessed May 7, 2023; Aaron Perzanowski, *The Right to Repair: Reclaiming the Things We Own* (Cambridge University Press 2022).

8 See Paul Ohm and Nathaniel Kim, "Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things" (2023) 84 Ohio State Law Journal 59; Chris Jay Hoofnagle, Aniket Kesari and Aaron Perzanowski, "The Tethered Economy" (2019) 87 The George Washington Law Review 783 <https://papers.ssrn.com/abstract=3318712> accessed November 19, 2020; and Christoph B Graber, "Tethered Technologies, Cloud Strategies and the Future of the First Sale/Exhaustion Defence in Copyright Law" (2015) 5 Queen Mary Journal of Intellectual Property 389 <http://www.elgaronline.com/abstract/journals/qmjip/5-4/qmjip.2015.04.02.xml> accessed February 24, 2022. See further Jonathan Zittrain, *The Future of the Internet - and How to Stop It* (Online edition 2009) for an earlier analysis; Rebecca Crootof, "The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference" 69 Duke Law Journal 583 on US civil law responses to "remote interference" with the "Internet of Things"; Margot E. Kaminski and others, "Averting Robot Eyes" (2017) 76 Maryland Law Review 983 <https://papers.ssrn.com/abstract=3002576> accessed March 24, 2023 for an analysis of design responses to deal with privacy risks associated with devices in the home; see Christina Mulligan, "Personal Property Servitudes on the Internet of Things" (2016) 50 Georgia Law Review 1121 <https://papers.ssrn.com/abstract=2465651> accessed March 24, 2023 for an analysis of potential responses to contractual and licensing restrictions on these devices; and Scott R Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Review 85 for an analysis of risks relating to discrimination, privacy, security and consent and potential responses.

9 This article will not focus on other human rights, such as the right to property and the right to freedom of expression, because they seem less likely candidates for grounding a Right to Root. The principles developed here are, however, also useful when applying those rights.

your own devices, an ideal which visionaries in the seventies of the past century considered to be closely connected to individual freedom. I then show how users over the years have gained less control and how the Right to Root could enable them to regain control. I then explore how the Right to Root could be constructed from the right to privacy under the Convention and the Charter, by understanding it as a way to protect the values of autonomy, self-determination and seclusion. I conclude that a Right to Root can be grounded in the human right to privacy, but that further research would be necessary to balance the Right to Root with other interests, such as cybersecurity, traffic safety, health and intellectual property.

B. The Right to Root: how it started...

6 The story of the Right to Root starts in the sixties and seventies of the past century, around Silicon Valley. Most of the computers at that time were being used in business, the military and academia.[10] There were, however, a number of computer pioneers who focused on what these machines could do to empower ordinary people. One of the people to develop this vision was Douglas Engelbart. Engelbart, born in 1929, decided early in his career that he would focus on augmenting the human intellect in order to enable humanity to cope with the increasing number of complex, yet urgent problems.[11] Computers could play an important role in this; he envisioned these devices as "giving the man maximum facility for directing all [computing] power to his individual task", and as a "very fast symbol-manipulating slave."[12] Another influential visionary from that time, Alan Kay, in 1972 sketched a similar vision for a "Personal Computer for Children of All Ages", which was supposed to also "augment" the learning process.[13]

7 Parallel to this, some people were underlining how computers could be a tool for liberation, not mere augmentation. One magazine for computer hobbyists, called the People's Computer Company, in their first issue of 1972 already suggested that computers have something to do with personal freedom: "Computers are mostly used against people instead of for people, used to control people instead of to *free* them, time to change all that – we need a People's Computer Company."[14] And in 1974, a computer enthusiast named Ted Nelson self-published *Computer Lib/Dream Machines*, a pamphlet which echoed the same vision: "I want to see computers useful to individuals, and the sooner the better, without necessary complication or human servility being required."[15] He wrote the pamphlet "for personal freedom and against restriction and coercion" and concludes with the rallying cry: "Computer power to the people!".

8 The first person, however, to clearly articulate how this freedom also required full control over software and hardware, was Richard Stallman. In the seventies, Stallman was working with one of the few computers in existence at MIT. When he tried to fix an issue with a jamming printer, he discovered that the printer driver was available only in compiled, binary code. This made it difficult for him to solve the jamming problem. The experience set him on a path which eventually resulted in a movement built around the ideal that people should have the *freedom* to run, share, study and change the software they use, because, in Stallman's words:[16]

> Freedom means having control over your own life. If you use a program to carry out activities in your life, your freedom depends on your having control over the program. You deserve to have control over the programs you use, and all the more so when you use them for something important in your life.

9 This idea kickstarted what is now known as the Free Software movement from mid-eighties onward, a movement centered around the vision that

10 See for example on business: James W. Cortada, *IBM: The Rise and Fall and Reinvention of a Global Icon* (The MIT Press 2019); see on academia Steven Levy, *Hackers* (1st ed, O'Reilly Media 2010)

11 Thierry Bardini, *Bootstrapping : Douglas Engelbart, Coevolution, and the Origins of Personal Computing* (Stanford, Calif : Stanford University Press 2000) 10–11 <http://archive.org/details/bootstrapping00thie> accessed May 31, 2022.

12 Ibid 18–19.

13 Alan C. Kay, "A Personal Computer for Children of All Ages" (Xerox Palo Alto Research Center 1972) <https://www.mprove.de/visionreality/media/Kay72a.pdf> accessed June 3, 2022.

14 Bob Albrecht and others, "Epilogue" (1972) 1 People's Computer Company <https://archive.computerhistory.org/resources/access/text/2017/09/102661095/102661095-05-v1-n1-acc.pdf> accessed June 3, 2022.

15 Ted Nelson, *Computer Lib/Dream Machines. New Freedoms Through Computer Screens.* (1974) <https://ia802805.us.archive.org/8/items/computer-lib-dream-machines/Computer%20Lib%2C%20Dream%20Machines%20%E2%80%93%20Ted%20Nelson%20%281974%29.pdf> accessed June 2, 2022.

16 Richard Stallman, "Why Free Software Is More Important Now Than Ever Before" [2013] *Wired* <https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before/> accessed December 1, 2022.

software should be free as in free speech, not as in free beer. And although the movement initially was concerned with software, it has since then also extended its scope to hardware, because freedom in an information society requires full control over *all* aspects of digital tools.[17] So, what has become of this idea since?

C. ...How it's going

10 Fifty years later, little of this vision has become reality. There was a short period, in the early eighties, when people had a semblance of control. At that time, computers had just become *personal* computers, instead of centrally administered mainframes, to be used also in homes, not yet connected to the internet.[18] These personal computers combined keyboard, processing, storage and screen all in one device – no part of the machine was outside the house. And not only were all these components on one desktop, they could usually be fully administered by the owner. *In theory*: most personal computer users at that time were unable to exploit this power, because they didn't have the necessary expertise, because most of the software was not Free Software as described above, and because some computers also limited what hardware you could connect to it.

11 This temporary semblance of control changed for the worse when personal computers were outfitted with network technologies at some point in the late eighties. People soon started hooking up their personal computers to outside networks, first bulletin board systems, later public networks, eventually resulting in the internet as we know it. This advent of the internet heralded a profound shift in control over digital devices: it not only provided a way for people to connect *to* the outside world, but also provided the outside world with a direct path *into* people's computers.

12 And the outside world made good use of this. This direct path to users' computers enabled two things: collecting data on users, and controlling their devices. As to the collection of data: one of the earliest and still most relevant examples of this is the use of cookies, originally intended to allow a server to recognise a browser when doing things like online shopping, it was quickly repurposed to track people's surfing habits.[19] That, however, was only the beginning. Since then, many more devices have become a computer, and collecting data through these devices has not only became ubiquitous, it has also become much more detailed. If we focus on devices which everyone uses: both dominant smartphone platforms Android and iOS provide fine-grained access to smartphone sensors, enabling them to read information such as the location, camera, files and battery level of the phone.[20] The same with cars: for example, Tesla remotely collects data related to the usage, operation and condition of a vehicle – even using this once to track the whereabouts of a critical journalist.[21] Same for bikes: eBike manufacturers collect information on the speed limit, total distance and battery level of the bike (if you use their app).[22] And the same for fridges, lamps, watches – the list is endless.

13 As noted above, companies are using these remote connections to not only collect data, but also for remote control: to restrict functionality, remove material and in some cases even shut off devices from afar. Lenders in the US have been known to disable the ignition of a car if the owner is late in payments.[23] Similarly, a Ukranian dealer of John

17 See the *Respects your Freedom*-certification programme of the Free Software Foundation which certifies hardware which implements these ideals in hardware: *https://ryf.fsf.org*.

18 See on the history of personal computing Michael Swaine, Paul Freiberger and Brian P. Hogan, *Fire in the Valley: The Birth and Death of the Personal Computer* (Third edition, The Pragmatic Bookshelf 2014).

19 See John Schwartz, "Giving Web a Memory Cost Its Users Privacy" *The New York Times: Business* (September 4, 2001) <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> accessed December 2, 2022; Lou Montulli, "The Irregular Musings of Lou Montulli: The Reasoning Behind Web Cookies" (May 14, 2013) <https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html> accessed December 2, 2022.

20 See Google, "Android Documentation" (2021) <https://developer.android.com/guide/topics/sensors/sensors_overview> accessed January 5, 2021, sections on Sensors, Location and Performance; Apple, "SRSensor. The Sensors an App Can Read" <https://developer.apple.com/documentation/sensorkit/srsensor#3681604> accessed June 22, 2021

21 Tesla, "Privacy Notice" (2022) <https://www.tesla.com/en_eu/legal/privacy> accessed December 2, 2022; Elon Musk, "A Most Peculiar Test Drive" (February 13, 2013) <https://www.tesla.com/blog/most-peculiar-test-drive> accessed November 18, 2020.

22 VanMoof, "VanMoof Privacy Statement" (2022) <https://www.vanmoof.com/en-NL/privacy> accessed December 2, 2022.

23 Michael Corkery and Jessica Silver-Greenberg, "Miss a Payment? Good Luck Moving That Car" (September 24, 2019) <https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/> accessed November

Deere used this functionality to shut down farming equipment stolen by Russia.[24] Tesla disables features of the car remotely, for example when a car changes hands.[25] BMW and Audi announced they can enable certain options, such as seat heating or parking assistance, over the internet – thus also giving them power to disable functionality.[26] And in 2009, Amazon removed copies of Orwell's *1984* remotely from the e-readers of its customers over a copyright claim.[27]

14 While manufacturers gained control over these devices, many of these devices simultaneously are often designed to limit control by the user. All phones from Apple, and most Android phones, only allow the user to access the functionality provided through the default operating system, and install apps via the already provided app stores.[28] Google Nest devices only run approved software through a feature called "verified boot."[29] What's more, attempts to circumvent these restrictions are often actively prevented. iOS updates from Apple have long been designed to block methods to circumvent these restrictions.[30] HP installed a "security update" which started rejecting all third-party ink cartridges five months after installation.[31] Philips has released an update to its smart lamps which blocked lamps not approved by Philips from working.[32] And Tesla detects and centrally logs when people try to upgrade their car themselves without paying for it.[33]

15 Finally, not only are attempts to circumvent these restrictions made more complex: the act of circumvention, and the tools used for circumvention, may also under certain circumstances be unlawful. The European Copyright Directive requires member states to restrict the circumvention of "effective technological measures" and the offering of circumvention tools; US laws contain a similar provision.[34] Most of the technological restrictions

18, 2020.

24 Emma Roth, "Remote Lockouts Reportedly Stop Russian Troops from Using Stolen Ukrainian Farm Equipment" (May 2, 2022) <https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere> accessed May 3, 2022.

25 Aaron Gordon, "People Are Jailbreaking Used Teslas to Get the Features They Expect" (February 1, 2020) <https://www.vice.com/en/article/y3mb3w/people-are-jailbreaking-used-teslas-to-get-the-features-they-expect> accessed November 18, 2020.

26 Tim Stevens, "Your Next BMW Might Only Have Heated Seats for 3 Months" (July 1, 2020) <https://www.cnet.com/roadshow/news/bmw-vehicle-as-a-platform/> accessed November 18, 2020; Audi, "Consistently Connected: Audi Introduces Functions on Demand" (October 7, 2020) <https://www.audi.com/en/company/investor-relations/talking-business/audi-functions-on-demand.html> accessed November 24, 2020.

27 Bobbie Johnson and San Francisco, "Amazon Kindle Users Surprised by 'Big Brother' Move" *The Guardian: Technology* (July 17, 2009) <https://www.theguardian.com/technology/2009/jul/17/amazon-kindle-1984> accessed November 18, 2020. Amazon in response said that it would change the systems so that this could not happen again.

28 It has been reported that Apple is preparing to allow for sideloading, e.g. installling apps via other app store than Apple's: Mark Gurman, "Apple to Allow Outside App Stores in Overhaul Spurred by EU Laws" *Bloomberg.com* (December 13, 2022) <https://www.bloomberg.com/news/articles/2022-12-13/will-apple-allow-users-to-install-third-party-app-stores-sideload-in-europe> accessed December 15, 2022.

29 Google Safety Center, "Google Nest Security & Privacy Features" (2022) <https://safety.google/nest/> accessed December 2, 2022.

30 Chaim Gartenberg, "Apple Releases iOS 13.5.1, Patching Out the Unc0ver Jailbreak" (June 1, 2020) <https://www.theverge.com/2020/6/1/21277281/apple-ios-13-5-1-patch-unc0ver-jailbreak-update-software-install> accessed January 5, 2021; Jenna Wortham, "Unofficial Software Incurs Apple's Wrath" *The New York Times: Technology* (May 13, 2009) <https://www.nytimes.com/2009/05/13/technology/13jailbreak.html> accessed January 5, 2021

31 Cory Doctorow, "Ink-Stained Wretches: The Battle for the Soul of Digital Freedom Taking Place Inside Your Printer" (November 5, 2020) <https://www.eff.org/deeplinks/2020/11/ink-stained-wretches-battle-soul-digital-freedom-taking-place-inside-your-printer> accessed November 18, 2020.

32 Joel Ward, "Philips Hue Excludes 3rd Party Bulbs with Firmware Update" (December 11, 2015) <https://zatznotfunny.com/2015-12/philips-hue-excludes-3rd-party-bulbs/> accessed November 18, 2020.

33 Rob Stumpf, "Tesla Can Detect Aftermarket Hacks Designed to Defeat EV Performance Paywalls" (September 7, 2020) <https://www.thedrive.com/tech/35946/tesla-can-detect-aftermarket-hacks-designed-to-defeat-ev-performance-paywalls> accessed November 18, 2020.

34 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society 2001 (2001 OJ L 167/10), Art. 6; the new Copyright in the Digital Single Market Directive has retained this provision; Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives

limiting what people can do with their devices should be considered such "effective technological measures", because they restrict access to information or the copying of information without authorisation.[35] There have also been a number of cases where this provision has been used to restrict the sale of devices which remove copy protection measures.[36] Given how broadly these provisions have been interpreted in the past, this could mean that for example an exploit which allows for gaining full control over a phone is considered a product or service intended to circumvent an "effective technological measure" (but may profit from an exemption, see below). And while these rules may have been driven primarily by the desire to protect entertainment material, it is argued that the scope of these rules extends to fields far beyond movies and songs, such as the verification of printer cartridges and keycard systems for locks.[37] That is because it is argued that such systems restrict access to software, and software is protected by copyright as well.

16 Not only do the rules apply to virtually every kind of information with some security measure around it – the rules have a hard time distinguishing between legitimate and illegitimate circumvention. Whether you are breaking encryption to start your illicit filesharing empire, or doing it to share an out-of-copy version of a Shakespeare sonnet with your English teacher, rules prohibiting circumventions and related tools only partly take this into account. To be clear: there is some room for exceptions built into these laws, but it's limited. In the US, explicit exceptions to the circumvention prohibition have been adopted for certain uses in the public interest, such as *jailbreaking* (gaining full control over a device) and information security research, but these are narrowly defined.[38] The EU takes a different route: it prohibits all circumvention, but at the same time obliges member states to ensure that rightsholders under certain circumstances make available to users the means of benefiting from copyright exceptions.[39] This approach has made these exceptions depend on their national implementation, and more importantly, the carve-out is limited in its scope. Take *jailbreaking*: it is by no means certain whether this has a "commercially significant purpose or use."[40]

17 In short, the ideal of users gaining full control over their devices remained just that: an ideal, something which only very few people actually manage to have in practice, and sometimes even involves breaking the law.

96/9/EC and 2001/29/EC 2019 (2019 OJ L 139/92), rec. 7. A similar, but somewhat narrower provision can be found in the Software Directive; Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs 2009 (2009 L 111/16). These follow from Article 11 of the WIPO Copyright Treaty; WIPO Copyright Treaty 1996. Article 18 of the WIPO Performances and Phonograms Treaty contains a similar obligation; WIPO Performances and Phonograms Treaty 1996. These rules have been transposed in the United States in section 1201 of the Digital Millennium Copyright Act (); Digital Millennium Copyright Act 1998.

35 The Court of Justice in *Nintendo* (2014) has ruled that "the concept of 'effective technological measures' is defined broadly", which also complies with the principal objective of the directive, which is to establish a high level of protection in favour authors; *Nintendo / PC Box* [2014], par. 27.

36 See for example ibid; *Nintendo modchips* [2010]; *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball (Application for Summary Judgment)* (2004) [2004] EWHC 1738 (Ch); *Nintendo Co Ltd v Playables Ltd* [2010] [2010] EWHC 1932; *TubeBox* [2012].

37 In its litigation against the disclosure of vulnerabilities regarding the Mifare-chip in the Netherlands also relied on this provision, but the district court did not consider it proven that the algorithm in question was protected by copyright; *NXP / RUN (Mifare-chip)* [2008]; see Samuelson (n 5) for a discussion of US case law.

38 See U. S. Copyright Office, "Joint Study of Section 1201(g) of the Digital Millennium Copyright Act" (May 2000) <https://www.copyright.gov/reports/studies/dmca_report.html> accessed October 30, 2019 where it was concluded at that time that particular language to protect encryption research was premature; and Joseph P Liu, "The DMCA and the Regulation of Scientific Research" 18 38 where it was argued that encryption research needed better protection. The US Library of Congress in 2015, 2018 and 2021 provided for an exemption on the circumvention prohibition for "good-faith security research"; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 2021 201.40. The US Library of Congress also provided for exceptions protecting other public interests, such as circumvention for assistive technologies for blind people and for educational use.

39 Copyright Directive, Art. 6(4); see for the impact of these provisions on information security research Ot van Daalen, "In Defense of Offense: Information Security Research Under the Right to Science" (2022) 46 Computer Law & Security Review 105706 <https://linkinghub.elsevier.com/retrieve/pii/S026736492200053X> accessed July 11, 2022.

40 For example, the wording "commercially significant purpose or use other than to circumvent the technical protection" can be found in section 1201(a)(2) and 1201(b) of the as well, and the legislative history of those provisions suggests that "purpose or use" should be read together; Register of Copyrights, "Section 1201 of Title 17 A Report of the Register of Copyrights" (United States Copyright Office 2017), p. 14.

D. Enter the Right to Root

18 As a result, there have been a few calls for allowing users to gain root over the devices. In the beginning of this millenium, the first seeds for such an idea were planted in the context of a debate around the human rights implications of "trusted computing" infrastructure. At that time, Microsoft was working on hardware which could be used to approve software to run on a computer, ostensibly to improve user security. But security-expert Ross Anderson in 2002 suggested that this infrastructure could be used for removing or blocking software and other kinds of information on a computer remotely for all kinds of reasons.[41] The Free Software Foundation for the same reason was worried that it would affect the freedom of users to run the software they chose.[42] This discussion eventually died down, probably because of the pushback Microsoft received.

19 However, digital rights activist Cory Doctorow rekindled the discussion in 2012, when he gave a speech on the "coming civil war over general purpose computing."[43] This was at a time when "Trusted Party Modules" (TPMs) were starting to be installed in computers – in essence the same technology Microsoft was working on almost a decade earlier. TPMs are hardware chips which generate, store and process cryptographic keys "securely", that is, in line with the security policy set out by the designer of the system.[44] One application of TPMs is to check whether the software booting up the computer, the bootloader, has not been tampered with. If the TPM can confirm that the bootloader is intact, this provides a foundation of trust, which allows other software started up by the bootloader to be trusted as well. This means that whoever controls the TPM, also controls the computer.

20 TPM's as such are not problematic – the question is who gets to control the TPM. If this is, for example, the hardware manufacturer, or the operating system supplier, there is a risk that this control will be used to restrict user freedom, by prohibiting certain software from running on your device. If, on the other hand, the user controls the TPM, they can decide which software to trust.

21 This is not a purely technical question – as Doctorow points out, it has significant human rights implications. If the Chinese government through the use of TPMs can force Apple to block encrypted messaging apps on a phone, this directly affects activists in China, as they would have to move to communications means which are easier to surveil. Similarly, if the European Union can force Google to install software monitoring your conversations, the potential for abuse, chilling effects and wrongful accusations is enormous. And the human rights impact is even more profound when these devices are worn in, or around your body (think of cochlear implants, insulin pumps, bionic eyes and pacemakers).

22 Still, there are also potentially persuasive reasons for not letting owners or users determine what they can do with their devices. Doctorow gives the example of changing the software on self-driving cars, removing speed limits or overriding traffic rules – which could significantly affect traffic safety. And although self-driving cars are not common yet, manually removing speed restrictions from e-bikes is already happening. Another example where it could be problematic to grant users the freedom to run their own software, would be in a corporate environment, where this could lead to security risks.

23 The Electronic Frontier Foundation in 2017 suggested that users should be offered the ability to disable a certain security measure imposed by Intel chips which had the effect of blocking users from patching vulnerabilities.[45] The authors at the same time recognize that there are situations where this may impossible, or where this may pose a security problem in itself – in those cases they would require the possibility to audit, and control which services run on the chip to enable administrators to mitigate security risks. Similarly, US-based academic Joshua Fairfield advocates for a "right to hack."[46] This would entail at a minimum removing tracking devices from things people own, being able to repair these, controlling or stopping forced updates. More generally, it would entail the right to "modify [a device], improve it, sell it, back it up, switch formats or devices, or simply have it accept the owner's commands over those of the manufacturer or rightsholder."[47] This would also

41 Ross Anderson, "Trusted Computing FAQ" (August 2003) <https://www.cl.cam.ac.uk/~rja14/tcpa-faq.html> accessed March 24, 2023.

42 Richard Stallman, "Can You Trust Your Computer?" (2015) <https://www.gnu.org/philosophy/can-you-trust.en.html> accessed March 24, 2023.

43 Doctorow, "The Coming Civil War over General Purpose Computing" (n 2)

44 Microsoft, "Trusted Platform Module Technology Overview (Windows)" (February 17, 2023) <https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview> accessed February 24, 2023.

45 Portnoy and Eckersley, (n 2)

46 Fairfield (n 3) ch 8.

47 Ibid 198.

entail permitting users "root access in the device as shipped, and to stop removing root access via over-the-air update". Fairfield does ecognize the tensions with, for example, safety and security, but does not work this out further.[48]

24 Ido Kilovaty has also argued that people should have the freedom to hack their devices, but does not advocate for the possibility to gain root.[49] Pam Samuelson defends the "freedom to tinker", but also does not translate this in a Right to Root.[50] Ohm and Kim's proposal of a "legacy switch" would merely reduce the functionality.[51] The right to repair, recently gaining traction in US and the EU, is somewhat related to the Right to Root, but it is primarily based on sustainability considerations, not human rights.[52] Finally, Ohm and Kim suggest the right to turn off the "smart" functions of devices; while Hoofnagle, Kesari and Perzanowski analyse some of the issues with "tethered devices" and suggest a "kill switch" – solutions which point in the direction, but fall short of gaining full control over a device.[53]

25 Meanwhile, this development is becoming ever more urgent – if only because Windows 11 can only run on computers with a certain TPM.[54] Furthermore, some have recently been ringing the alarm bell about remote attestation, which is a check by an online service provider whether you're running trusted operating system (or software) on your computer, something which also requires TPMs to function.[55]

26 So, an important question is whether you can argue that the Right to Root follows from human rights.

E. How this relates to the right to privacy

27 There are many human rights angles to this question, but I discuss only one: the right to privacy (and data protection). I chose privacy primarily because it is closely related to autonomy, the central concern of those arguing for full control over devices. Other rights could also be useful for supporting a Right to Root – in particular the rights to property and the right to freedom of expression. But the right to property can be restricted through contractual means, and it is questionable to what extent positive obligations can limit such restrictions.[56] The right to freedom of expression is furthermore only applicable to the extent that these devices play a role in freedom of expression, something which is less clear in the case of devices such as thermostats and cars. Nevertheless, I expect the framework developed in this context to be also useful in the context of construction of a Right to Root from the foundation of other human rights.

I. Conceptual frameworks around privacy

28 Before trying to locate the Right to Root in the case law on the right to privacy under the Convention and the Charter, it is useful to consider where the Right to Root fits more generally in the *concept* of privacy. For our purposes, the typology of privacy presented by Koops and others is useful as a location device.[57] The following diagram summarizes their findings:

48 Ibid 225.

49 Kilovaty (n 4).

50 Samuelson (n 5).

51 Ohm and Kim (n 50).

52 See for example Rosborough, Wiseman and Pihlajarinne, (n 0); Perzanowski, (n 0).

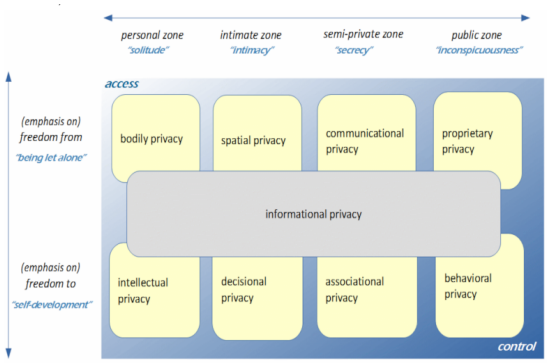
53 See Ohm and Kim, (n 50); Hoofnagle, Kesari and Perzanowski, (n 0); and Graber, (n 0). See further Zittrain, (n 0) for an earlier analysis; Crootof, (n 0) on US civil law responses to "remote interference" with the "Internet of Things"; Kaminski and others, (n 0) for an analysis of design responses to deal with privacy risks associated with devices in the home; see Mulligan, (n 0) for an analysis of potential responses to contractual and licensing restrictions on these devices; and Peppet, (n 0) for an analysis of risks relating to discrimination, privacy, security and consent and potential responses.

54 Microsoft, "Windows 11 Specs and System Requirements | Microsoft" <https://www.microsoft.com/en-us/windows/windows-11-specifications> accessed March 29, 2023.

55 Gabriel Sieben, "Remote Attestation Is Coming Back. How Much Freedom Will It Take?" (July 29, 2022) <https://gabrielsieben.tech/2022/07/29/remote-assertion-is-coming-back-how-much-freedom-will-it-take/> accessed March 24, 2023.

56 See ECHR, "Guide on Article 1 of Protocol No. 1 - Protection of Property" (ECHR 2022), sec. II.C.1.

57 Bert-Jaap Koops and others, "A Typology of Privacy" (2017) 38 University of Pennsylvania Journal of International Law 483 <https://scholarship.law.upenn.edu/jil/vol38/iss2/4>.



29 In their overview, Koops et. al. distinguish two axes. On one axis, they contrast the framing of privacy in negative and positive terms: the right to privacy can be understood to encompass a spectrum, ranging from emphasis on the right to be left alone (negative aspects), to emphasis on self-development (positive aspects).[58] On the other axis, Koops et. al. describe the different domains in which privacy operates, ranging from the private to the public: privacy not only protects activities in private, but also increasingly protects things we do in public.

30 Along the first axis, the Right to Root is located mostly under self-development: it is a way to gain control over devices, a way to extend what you can do with your machines. Logically, if digital tools play an important role in our life, then full control over those tools can further our possibilities for development, and thus our freedom: it enables you to share a book (if you disable digital rights management), to use an alternative app (if you circumvent the official app store), or to drive faster with your bike (if you override speed settings). In other words; of all the goals which privacy aims to protect, the Right to Root is related primarily to the principles of autonomy and self-determination (below I'll discuss case law on this).

31 But if you look more closely, the Right to Root arguably spans this entire axis, not only the self-development aspect of it: it also has a relationship with the right to be let alone – or seclusion – because of the control *others* have over these devices. This control, as discussed above, is about limiting the functionality of devices, disabling them and collecting data via these devices. And gaining full user control over these devices is an important condition for removing the control of others: you can only replace Google's operating system on your smartphone with a version without all the Googly bits, if you first gain control over your device, if you gain "root".

58 See the diagram on p. 482 of ibid.

32 On the second axis, distinguishing between the private and the public domain, the Right to Root is located in the private realm. First, it is about *your* personal devices. Many of these devices are in the *home*, traditionally considered one of the most private places and often explicitly protected in national constitutions. Some of these we take with us continuously – they are in effect an extension of the body, a domain which could be considered even more private. Some are even worn *in* the body – think of digital pacemakers, cochlear implants and insulin pumps. Furthermore, the *information* on the devices is intended to be accessed by the user, not by others: the books you read on your e-reader are part of a private activity, and the smart thermostat in your house displays its readings for your benefit, not for the outside world. Some devices contain your most intimate thoughts – when you keep a diary on your computer for example. And while some of it may be intended for others – for example the email conversation stored on your phone which you were having with your friend – even then: private communications are also considered at the core of the right to privacy.

33 So, to recap: the Right to Root is strongly connected to the values of autonomy, self-development and seclusion as protected under the concept of privacy, and it is located primarily in the private domain. Given this understanding of the Right to Root, the question then is whether the existing case law on the right to privacy under the Convention and the Charter provides support for such a right.

II. The right to integrity and confidentiality of IT systems

34 One intuitive starting point for this inquiry is not found in case law of the Convention and the Charter, but instead in the decision on the right to integrity and confidentiality of IT systems of the German constitutional court. In 2008, the German Constitutional Court reviewed a German law allowing the state to enter computers remotely, and in the context of this law clarified how devices are protected under the right to privacy.[59]

59 See *Online-Durchsuchung* [2008]; Wiebke Abel and Burkhard Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a Case Report on BVerfG, NJW 2008, 822" (2009) 6 SCRIPT-ed 106 <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp> accessed November 23, 2018; Karavas Vaios, "Das Computer-Grundrecht. Persönlichtkeitsschutz Unter Informationstechnischen Bedingungen" (2010) 7 Neue Zeitschrift für Sozialforschung 95; see also Mirja Gutheil and others, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of

35 In its decision, the Court observed that the fundamental rights to confidential communication, inviolability of the home and informational self-determination currently recognised under the German constitution do not provide sufficient protection against the state searching an IT-system remotely. This is because of the potentially wide-ranging nature of such a search. The Court in response discerned a new fundamental right which protects against "access by the state in the area of information technology also insofar as the state has access to the information technology system as a *whole*, and not only to individual communication events or stored data" (emphasis mine).[60] In other words, it argued that integrity and confidentiality of the *device* is protected under the right to privacy. The German court based this new right under the general "right of personality" under the German Constitution, which serves as a backstop when other rights cannot provide protection. It came to this conclusion firstly because personal computers and other computerised devices have become central to the *development* of personality, especially when they are part of a network.[61] It further argues that these devices also *endanger* personality, partly because of the amount of personal information being processed by them, partly because of how outsiders can gain access to this data.[62]

36 As we will see below, the reasoning of the German court – emphasising how these devices both further individual freedom through their possibilities and restrict freedom through the amount of control they afford to others – can also be found in Convention and Charter case law.

III. The right to privacy under the Convention

37 Of the four distinct concepts protected by the right to privacy under the Convention, private life, correspondence, family life and the home, private life and correspondence are most relevant for this article. The concept of "family life" relates to issues such as marriages and family reunification.[63] The notion of the "home" revolves mostly around themes such as housing, the protection of homes of journalists and lawyers and the environment surrounding a home.[64]

38 As to the notion of "private life": the Court has repeatedly emphasised that it is a broad term not susceptible to exhaustive definition.[65] This is relevant, as it demonstrates that this concept lends itself well to the dynamic interpretation the Court has developed over the years. And the Court has, through this dynamic interpretation, read into the Convention support for the concepts of seclusion, autonomy and self-determination.

39 As a starting point, the Court has in its case law repeatedly noted that the "very essence of the Convention is respect for human dignity and human freedom", also in the context of Article 8.[66] Zooming in on the value of seclusion, it has considered that Article 8 includes "the right to live privately, away from unwanted attention."[67] And it has emphasised

Practices" (Directorate-General for Internal Policies of the European Parliament 2017) Study for the LIBE Committee for an overview of similar laws.

60 *Online-Durchsuchung* (n 58), par. 201.

61 par. 172-174

62 par. 177-180

63 See ECHR, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Privacy and Family Life, Home and Correspondence* (Council of Europe 2022) ch III <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed October 17, 2018.

64 See ibid IV. Intuitively, one could argue that the fact that something is in the home, as most digital devices are, is a relevant consideration when applying Article 8 of the Convention. The case law does not provide support for this, however. Instead, privacy-related cases with regard to devices in the "home" have been handled under the header of private life and correspondence (see below for an overview). Koops and Hoepman explore how the home could be understood to not only protecting the space between physical walls, but also the space between digital walls, affording functionally equivalent protection to remote storage of private information; See Jaap-Henk Hoepman and Bert-Jaap Koops, "Offering 'Home' Protection to Private Digital Storage Spaces" (2020) 17 SCRIPTed 359 <https://research.tilburguniversity.edu/en/publications/offering-home-protection-to-private-digital-storage-spaces> accessed November 13, 2020.

65 *Niemietz v Germany* [1992], par. 29; *Pretty v The United Kingdom*, par. 61

66 *Christine Goodwin v The United Kingdom* [2002], par. 90; *Pretty v. The United Kingdom* (n 65), par. 65. See later for similar wording; *Bouyid v Belgium* [2015], par. 89; *Svinarenko and Slyadnev c Russia* [2014], par. 138; *El-Masri v The former Yugoslav Republic of Macedonia* [2012], par. 248. As follows from the wording of the Court, human dignity is a concept central to the *entire Convention*, but the above cases demonstrate that it is also central to informing the scope of the protection afforded under Article 8.

67 *Smirnova v Russia*, par. 95; later reiterated in *inter alia Couderc and Hachette Filipacchi Associés v France* [2015], par.

the importance of autonomy, in cases focusing on the right to self-determination (euthanasia, discrimination of transgender people).[68] More recently, the Court has even read into Article 8 "a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged."[69] And while these values cannot be connected as easily to the concept of "correspondence", the Court has also interpreted this notion broadly, covering a wide range of media, extending to real-time and stored interception, to content as well as metadata, to professional and personal communications, to interception as well as to the impeding of correspondence.[70]

40 Still, even if the right to privacy under the Convention may in theory protect the values underlying the Right to Root, this is only the beginning of the analysis. The next question is what this means for legal measures in this area: to what extent may the government impinge on the Right to Root, and does it have positive obligations in this regard? Answering these questions is not straightforward. This is because the developments described above are mostly the results of actions by non-state actors, such as device manufacturers and commercial service providers. Thus the case law on negative obligations cannot be applied directly, and instead functions more as inspiration for the development of state obligations under the case law on *positive* obligations under Article 8. I discuss both.

IV. The relevance of negative privacy obligations under the Convention

41 As to the negative obligations under Article 8 of the Convention, the gist of the case law of the Court centers around the risk of abuse of surveillance powers by states. This abuse, according to the Court, can be prevented by clear and proportionate laws, as well as oversight (for example by courts).[71] As to the proportionality, it is firstly important to note for purposes of this article that this hinges on the seriousness of the interference, which in turn has to do with criteria such as the sensitivity and richness of the data involved, the number of people affected, the amount of data processed and the duration of the surveillance.[72] Sometimes, the privacy impact is so great that it does not matter what the risk of abuse is: for example, the "blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences" was considered to be incompatible, regardless of the existence of safeguards against abuse.[73] This is relevant for the analysis under the positive obligations framework, because this case law suggest that when it comes to devices, any interference will quickly deemed to be serious.

42 The Court has also clarified how developing technology can further the risk of abuse. In *Szabó* (2016), the Court warned for example about the potential for abuse, given the "formidable technologies" at the disposal of governments and "the magnitude of the pool of information retrievable by the authorities."[74] It has also repeatedly underlined that the continuously advancing sophistication of surveillance technologies increases the risk of arbitrariness.[75] Furthermore, in *Zakharov* (2015), the

83; *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017], par 130; *Bărbulescu v Romania* [2017], par. 70.

68 *Pretty v. The United Kingdom* (n 65), par. 61; *Christine Goodwin v. The United Kingdom* (n 65), par. 90.

69 *Breyer v Germany* [2020], par. 75.

70 See for example *Buglov v Ukraine*; *X V The United Kingdom* [1978]; *Christie v The United Kingdom* [1994]; *Malone v The United Kingdom* [1984]; *Klass and others v Germany*; *Taylor-Sabori v The United Kingdom*; *X And Y V Belgium* [1982]; *Copland v The United Kingdom*; *Bărbulescu v. Romania* (n 66); *Niemietz v. Germany* (n 69); *Wieser and Bicos Beteiligungen GmbH v Austria*; *Iliya Stefanov v Bulgaria* [2008]; *Frérot v France*; *Mehmet Nuri* Özen *and others v Turkey*; *Halford v The United Kingdom* [1997]; See *Golder v United Kingdom* [1975], par. 43.

71 See e.g. , *Roman Zakharov v Russia* [2015]. for the development of these principles; and *Centrum för Rättvisa v Sweden (Grand Chamber)* [2021], par. 253; and *Big Brother Watch and others v United Kingdom (Grand Chamber)* [2021], par. 339 on proportionality.

72 See for example *S and Marper v United Kingdom* [2008], par. 104; *Breyer v. Germany* (n 68); *Uzun v Germany*; *Szabó and Vissy v Hungary* [2016]; *Weber and Saravia v Germany* [2006]; *Iordachi and others v Moldova*; *Roman Zakharov v. Russia* (n 71); *Uzun v. Germany* (n 71).

73 *S and Marper v. United Kingdom* (n 71), par. 125.

74 *Szabó and Vissy v. Hungary* (n 71), par. 73, 79.

75 *Catt v The United Kingdom* [2019], par. 114; *Big Brother Watch and others v. United Kingdom (Grand Chamber)* (n 74), par. 322; *Centrum för Rättvisa v. Sweden (Grand Chamber)* (n 74), par. 236; *Roman Zakharov v. Russia* (n 71), par. 229; *Szabó and Vissy v. Hungary* (n 71), par. 62; see also the Court in *S and Marper v. United Kingdom* (n 71), which observed that "the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential

Court examined one particular aspect of this: where the security services and the police have direct technical access to communications and are thus in theory able to circumvent the judicial authorisation procedure, this makes the system particularly prone to abuse, especially since this access is not logged.[76] This is relevant in the context of the Right to Root, because others such as device manufacturers and service providers, often have *direct* access to devices. Although these decisions have been taken in the context of state surveillance, this also gives us an idea on how to assess the far-reaching monitoring and control by others.

43 Technology – and in particular information security measures – can also *mitigate* the risk of abuse, according the Court. In *Big Brother Watch* (2021), the Court for example considered that a state, when transferring intelligence information to other states, must ensure that the receiving state, in handling the data, has "in place safeguards capable of preventing abuse and disproportionate interference.[77] And in *Centrum för Rättvisa* (2021), the Court concluded that, in order to minimize the risk of unlawful access, intelligence services should be obliged to retain logs and a detailed record of each step in bulk interception operations.[78] This is relevant, because it could be argued that the control afforded by the Right to Root is a security measure which could prevent such unlawful access – something which is also discussed in the context of positive obligations below.

V. Positive privacy obligations under the Convention

44 As is well-known, although the object of Article 8 of the Convention is "essentially" to protect the individual against arbitrary interference, the Court has also read into this provision a positive obligation to respect the rights therein.[79] In the context of Article 8, the question is whether member states are under circumstances obliged to take "measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."[80]

45 Generally speaking, the nature of a positive obligation (and the margin of appreciation) will depend on the particular aspect of the right to privacy which is at issue and the interests at stake.[81] In its case law, the Court has considered it firstly relevant whether "fundamental values" or "essential aspects" of private life are at stake.[82] There is a narrower margin of appreciation where "a particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life."[83]

46 Here, the case law discussed above on the seriousness of the interference in the context of negative obligations provides an idea of where we could look for such fundamental values or essential aspects – think of highly sensitive data, bulk data, continuous control and direct access. Most of the devices to which the Right to Root would extend tick those boxes.

47 Finally, two cases on positive obligations are particularly relevant to the questions discussed here: *I. v. Finland* and *K.U. v. Finland*, where the Court underlined that states have a positive obligation to protect private information against *unauthorised access* by others, by requiring the taking of information security measures.[84] As noted, there is an obvious connection to the Right to Root here, in the sense that one way to prevent data collection is to gain full control. Whether that connection is sufficient to support legislative intervention is something I discuss in the conclusion.

benefits of the extensive use of such techniques against important private-life interests." (par. 112).

76 *Roman Zakharov v. Russia* (n 71), par. 270, 272. On the other hand, in *Kennedy*, the Court considered the fact that there was no evidence of abuse of the powers a reason for considering the measures compatible with Article 8; *Kennedy v United Kingdom*, par. 168.

77 *Big Brother Watch and others v. United Kingdom (Grand Chamber)* (n 74), par. 362.

78 *Centrum för Rättvisa v. Sweden (Grand Chamber)* (n 74), par. 311-316.

79 See *Marckx v Belgium*, par. 31; see in the context of Art. 6 *Airey v Ireland* [1979], par. 25; see further *X and Y v The Netherlands* [1985], par. 23.

80 *X and Y v. The Netherlands* (n 78), par. 23; *Odièvre v France* [2003], par. 40; *Evans v The United Kingdom* [2007], par. 75.

81 See *Hämäläinen v Finland* [2014], par. 66-68.

82 See *X and Y v. The Netherlands* (n 78), par. 27; *MC V Bulgaria* [2003], par. 150 and 153; *KU V Finland* [2008], par. 43 and 46; *IC V Romania*, par. 51 and 52.

83 *Söderman v Sweden* [2013], par. 79; see *Evans v. The United Kingdom* (n 79), par. 77 regarding "a particularly important facet of an individual's existence or identity".

84 *I v Finland* [2008]; *Z v Finland* [1997]; see also *K.U. V. Finland* (n 81), par. 49.

VI. The rights to privacy and data protection under the Charter

48 Since the Charter has come into effect, the Court of Justice has also played a significant role in interpreting the scope of the right to privacy (and data protection). The Charter grants at least the same protection as the Convention, so the European Court of Justice was able to build on decades of case law when it started to apply the right to privacy under Charter. The Charter protects the right to privacy and the right to data protection in separate provisions, Articles 7 and 8 respectively. The Court, however, often discusses these together and the relevance of the right to data protection as an individual ground for constructing the Right to Root is limited, so case law on data protection will not be discussed separately.[85]

49 Similar to the Convention, the risk of abuse of state powers is central to the assessment of negative obligations in the context of surveillance, evaluated on the basis of the objective of an interference, the seriousness of the interference and measures to prevent abuse.[86] This assessment involves aspects such as the number of people affected, the nature of the data, the duration of the measure and whether automated processing is applied.[87] Again, these are all factors pointing to the protection of devices under the right to privacy.

50 In this context, the Court has also investigated the security measures prescribed by the legislature. In *Digital Rights Ireland*, it considered the required security measures insufficient, in particular because they permit providers to take into account economic considerations when determining the level of security they apply.[88] And in *Tele 2* it considered that, given "the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures."[89] This is relevant, because gaining root over devices is one way to ensure device security.

51 Finally, one aspect relevant in this context is that the European legislator explicitly extended protection to devices through the ePrivacy Directive (in 2002), which required member States to ensure that the storing or gaining access of information on connected devices requires consent.[90] The Directive clarified that these connected devices are "part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms". It further emphasises that "spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users". Later, the EU Court of Justice in *Planet49* also touched on this, acknowledging that it follows from recital 24 of the ePrivacy Directive, that any information stored in the terminal equipment of users of electronic communications networks are part of users' private sphere protected under the Convention, which "applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge."[91]

F. Conclusion

52 One important takeaway from the case law is that the values of autonomy, self-determination and seclusion which underpin a Right to Root can be found in the case law of the right to privacy under the Convention and the Charter, as well as the right to confidentiality and integrity of IT systems recognised by the German constitutional court. Many devices are considered to fall within the private sphere, regardless of the data tbat it

85 See for example *Bavarian Lager* [2007], par. 118; *Satamedia* [2008], par. 52; *Promusicae* [2008], par. 63; *Volker und Markus Schecke and Eifert* [2010], par. 47; later repeated in *ASNEF* [2011], par. 41; *Schwarz v Bochum* [2013], par. 25 and 26; *Schrems I* [2015], par. 91; *Tele2 Sverige and Watson and Others* [2016], par. 100.

86 See *Digital Rights Ireland and others* [2014]; *La Quadrature du Net* [2020]; *Tele2 Sverige and Watson and Others* (n 85); *Ministerio Fiscal* [2018]; *Opinion 1/15*, par. 149; *Privacy International v United Kingdom* [2020]; *Schrems II* [2020].

87 See for example *Digital Rights Ireland and others* (n 85); *Tele2 Sverige and Watson and Others* (n 85); *Schrems I* (n 86); *SABAM / Netlog* [2012]; *Scarlet / SABAM* [2011].

88 *Digital Rights Ireland and others* (n 85), par. 67.

89 See for similar consideration *Tele2 Sverige and Watson and Others* (n 85), par. 122.

90 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector as Amended by Directive 2006/24/EC and Directive 2009/136/EC 2002, Art. 5(3).

91 *Planet49* [2019], par. 70.

contains. Devices tick many of the boxes relevant to proportionality and necessity assessment under the right to privacy (and data protection), such as the sensitivity and amount of data, as well as whether there is continuous control and direct access to the device.

53 It is also recognised in the case law that security measures are an important way to prevent unlawful access to information in the private sphere, but the courts do not prescribe which measures are most appropriate to mitigate unlawful access – in particular the case law on security measures in the context of the right to privacy does not yet make the connection to the Right to Root.

54 So where does this leave the Right to Root? One conclusion is that the current situation, where rooting might in some cases be illegal, interferes with the right to privacy. One could perhaps even argue that the right to privacy protects anyone who would manually override their device – effectively creating immunity for criminal and civil liability for the act of circumvention. Such an argument would, however, also have to take into account the other interests at stake, including traffic safety (for cars), health (for medical devices) security (for example for company-managed devices) and intellectual property (for DRM).

55 The few policy proposals pointing in the direction of a mandatory Right to Root have not really developed this tension, and further research on resolving this is necessary. This involves, firstly, better understanding *the extent* to which gaining root supports autonomy, self-determination and seclusion in different domains; this may, for example, be less important with regard to a smart thermostats, given their limited functionality, but more important with regard to phones. It also involves identifying the role of restrictions in devices for safeguarding the different interests. For example, to what extent does a speed limit on bikes further traffic safety; to what extent does DRM prevent copyright infringement?

56 Conversely, it involves an understanding of the impact of on these interests when one removes restrictions in systems. One distinction which is probably relevant in this context is between single-user and multi-user systems. For single-user systems, security measures are often intended to protect the system against the user. This can be done for example to restrict the functionality of the device, usually for economic reasons – and these restrictions are usually imposed by a vendor or supplier of a device. This is different for multi-user systems. In multi-user systems, there are good reasons for security restrictions – to prevent people from snooping in files without authorisation, for example, or to prevent them from spending other peoples' money. In this instance, a manual override of security measures would only create a huge security hole, without much gain in individual freedom. These are not the places where the right to privacy should impose a manual override.