Engineering and lawyering privacy by design

Rachovitsa, Adamantia

Published in:
International Journal of Law and Information Technology

DOI:
10.1093/ijlit/eaw012

International Journal of Law and Information Technology, 2016, 24, 374–399
doi: 10.1093/ijlit/eaw012
Advance Access Publication Date: 4 September 2016
Article

OXFORD

Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue

Adamantia Rachovitsa*

ABSTRACT

There is already evidence that 'governmental mass surveillance emerges as a dangerous habit'. Despite the serious interests at stake, we are far from fully comprehending the ramifications of the systematic and pervasive violation of privacy online. This article underscores the reasons that policy-makers and lawyers must comprehend and value privacy not only as a human rights issue, but also as a fundamental technical property for the well-functioning of the Internet. The analysis makes two main arguments. Firstly, it argues that the effective protection of online privacy cannot be thought of only in terms of compliance with legal frameworks but that—in practice—it also needs to be secured through technological means, such as privacy enhancing technologies and, most importantly, Privacy by Design. Recent developments in the standardization work of the Internet Advisory Board and the Internet Engineering Task Force suggest a paradigm shift with respect to integrating Privacy by Design into the core Internet protocols. The consideration of privacy as a requirement in the design of the Internet will have a significant impact on reducing states' capability to conduct mass surveillance and on protecting the privacy of global end-users. Secondly, the article argues that Internet standards should not be seen as 'living a parallel life' to, or as displacing or merely complementing, international human rights law. Technical standards and international law can actively inform one another. The analysis and findings demonstrate how the technical perspective on privacy can inform and enrich policy-making and legal reasoning.

KEYWORDS: internet standards, internet protocols, online privacy, privacy by design, human rights, pervasive monitoring, surveillance, internet engineering task force

INTRODUCTION

Recent revelations that states conduct mass and indiscriminate surveillance and eavesdrop on digital communications demonstrate that 'governmental mass surveillance emerges as a dangerous habit rather than an exceptional measure'.[1] The right

* Assistant Professor of Public International Law, Department of International Law – Faculty of Law, University of Groningen; 2015-2016 Fellow at UC Berkeley – Center for Technology, Society & Policy. I would like to thank the participants to Amsterdam Privacy Conference – APC 2015 and the anonymous reviews for their useful feedback. E-mail: a.rachovitsa@rug.nl.

1 Report of the Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' 30 June 2014, UN Doc A/HRC/27/37, [3] (UN Report on the Right to Privacy). For

to privacy is seriously and extensively threatened online without users being aware of. The consequences of pervasive monitoring[2] cannot be duly appreciated unless one underlines that the exercise of the right to privacy is also a prerequisite for realizing other human rights—online and offline.[3] Furthermore, serious and systematic attacks on online privacy undermine relations among states, confidence of the citizens in the rule of law and trust in the digital economy.[4] Despite the serious interests at stake, we are far from fully comprehending the ramifications of the violation and abuse of privacy by means of pervasive monitoring. Affirming that human rights apply equally offline and online is an invaluable and timely pronouncement,[5] but international lawyers and courts as well as policy makers, have just started to explore the implications of the Internet's technical features to policy-making and legal reasoning.[6] The article underscores the reasons that policy-makers and lawyers must value privacy not only as a human rights issue, but also as a fundamental technical property for the well-functioning of the Internet.

The article makes two main arguments. First, it argues that the effective protection of online privacy cannot be thought of only in terms of compliance with legal frameworks but that—in practice—it also needs to be secured through technological means, such as privacy enhancing technologies and, most importantly, Privacy by Design.[7]

example, NSA's programme 'PRISM' allows to access a wide range of Internet communication content and metadata from US corporations. NSA also runs the 'UPSTREAM' programme which provided access to nearly all the traffic passing through fibre optic cables owned by US service providers such as AT&T and Verizon. The UK surveillance programme 'TEMPORA' operated by the GCHQ included access to traffic passing along fibre optic cables running between UK and North America—the data collected are both Internet and telephone communications.

2 For a definition of pervasive monitoring S Farrell and H Tschofenig, 'Pervasive Monitoring Is an Attack' (May 2014) RFC 7258, Best Current Practice 188, 2, <http://www.rfc-editor.org/rfc/rfc7258.txt> accessed 1 May 2016. 'Pervasive monitoring' and 'surveillance' will be used interchangeable herein.

3 UN Report on the Right to Privacy (n 1) [14]; Franck La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' 12 April 2014, UN Doc A/HRC/23/40 [24]–[26]; Human Rights Council, Decision 25/117, 'Panel on the Right to Privacy in the Digital Age' 15 April 2014, UN Doc A/HRC/DEC/25/117 (adopted with no vote) rec 9; Council of Europe Parliamentary Assembly, 'Report on Mass Surveillance' 18 March 2015, Doc 13734, [97].

4 European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, 2013/2188(INI) BO, BT, BV, 72, 111–12.

5 UNGA Res 68/167, 'The Right to Privacy in the Digital Age' 21 January 2014, UN Doc A/RES/68/167 (adopted with no vote) [3], [4]; UNGA Res 69/166, 'The Right to Privacy in the Digital Age' 10 February 2015, UN Doc A/RES/69/166 (adopted with no vote). See also Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' 20 June 2014, UN Doc A/HRC/26/L.24, [1], [5]. See also Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' 29 June 2012, UN Doc A/HRC/20/L.13.

6 Global Multi-stakeholder Meeting on the Future of Internet Governance, 'NETmundial Multi-stakeholder Statement' São Paulo, 24 April 2014, 9, <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> accessed 1 May 2016.

7 The term 'privacy by design' was coined by Dr Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada: A Cavoukian, 'Privacy by Design in Law, Policy and Practice – A White Paper for Regulators, Decision-makers and Policy-makers' (2011) 19–24, <http://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 1 May 2016. Privacy by design is different from privacy enhancing technologies in that the former is a general requirement of the core architecture of a system or product, whereas the latter are employed to strengthen privacy-related components of the system, as a second stage, when the architecture is already implemented.

The article addresses how privacy is hardwired into the core Internet protocols that form the Internet's basic architecture,[8] by introducing the privacy-related work of the Internet's technical bodies. The Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF) are the most prominent and influential standardization bodies in this area. The design of the network[9] and Internet protocols (as engineered via technical standards) by default encapsulate regulation and, therefore, prescribe a certain level of privacy protection for Internet users. The analysis looks at recent developments in the standardization work of the IETF and IAB and provides evidence of a paradigm shift with respect to integrating 'privacy by design' requirements in the Internet protocols. The consideration of privacy as a requirement in the design of the Internet will have a significant impact on reducing states' capability to conduct mass surveillance and on protecting the privacy of global end-users. Secondly, the article argues that Internet standards and the technical point of view on privacy should not be seen as 'living a parallel life' to, or as displacing or merely complementing, international human rights law. Technical standards and international law can actively inform one another and converge in their application with respect to protecting privacy online. In fact, the technical perspective reinforces human rights arguments concerning the protection of privacy. The analysis and findings come to reinforce the point of the UN Special Rapporteur on privacy with regard to fully exploring the potential of international law including binding and non-binding instruments.[10]

The discussion is structured into four parts. The second part briefly explains the role of the IAB and IETF and it shows that protecting privacy online falls within the remit of the IETF's standardisation work. However, the IETF does not value privacy as a human right per se, or as a legal consideration, but rather as an instrumental value that must be understood as a necessary condition for restoring and maintaining users' trust in the Internet. The work in progress of these bodies with regard to integrating Privacy by Design into the core Internet protocols[11] qualifies as a technical 'solution'/response to mass surveillance. This solution includes the creation of a privacy threat vocabulary, the introduction of encryption in the Internet traffic and implementation of privacy into all the layers of the network. The analysis demonstrates how Internet standards are being informed by, and in turn shape and nurture, legal standards and business practices. At the same time, however, the overall impact of Privacy by Design incorporated into the Internet's architecture is subject to Privacy by Design policies by service providers and states' practices. The third part proceeds to explore how the technical perspective on privacy can inform the manner in which the legal advisor argues about privacy, the legislator articulates the interests at stake and the academic and practitioner interpret international human rights law. Pressing questions, such as the relevance of the location and nationality of individuals in the digital environment or the interrelation of privacy, freedom of expression and

8 For the definition of the core Internet protocols see discussion in the subsection 'Internet standards and standard-setting process'.

9 The Internet is composed of a great number of networks. 'Internet' and 'network' will be used interchangeably herein.

10 Report of the Special Rapporteur on the Right to Privacy, JA Cannataci, 8 March 2016, UN Doc A/HRC/31/64, [46 (j)].

11 L Lessig, *The Future of Ideas: The Fate of the Commons on a Connected World* (Vintage Books 2001) 36.

security, require us to revisit our take on interpreting and applying international human rights law. The fourth part concludes.

DEVELOPING INTERNET STANDARDS TO SECURE PRIVACY ONLINE

Internet governance is highly fragmented in terms of the distribution of authority, reflecting the decentralized nature of the network itself. The creation and evolution of the Internet are shaped by standards, principles, norms, rules and business practices, which are developed in a multi-stakeholder ecosystem. States, the technical community, industry, civil society, academia and global users participate to varying degrees to formal and informal governance arrangements.[12] Despite this fragmentation and lack of formal authority, a limited de facto hierarchy exists in the day-to-day management of the Internet.[13] The Internet's engineers and, in particular, the IETF and the IAB are responsible for making the Internet work better and managing the technical aspects of the Internet by creating Internet Protocols.[14]

Internet standards and standard-setting process

Internet protocols are engineered on the basis of technical standards, known as Internet standards, set by the IETF and the IAB.[15] Internet protocols constitute the backbone of the Internet upon which all the layers of the network are created.[16] As such, they define—to a significant extent—how the Internet functions and they frame the context of its legal regulation.[17] The core architecture of the Internet is a strong mode of regulation itself: technological capabilities and design choices impose rules/constraints on the online user regarding access and use of information.[18] The default settings—from the design of the Internet protocols to a particular application or a browser—shape the user's choices Consequently, Internet protocols are a 'hidden' yet powerful regulatory force complementing the law, the market and social

12 NETmundial Statement (n 6) 6; World Summit on the Information Society, 'Tunis Agenda for the Information Society', 18 November 2005, WSIS-05/TUNIS/DOC/6(Rev.1)-E, [34]; Lee Bygrave and Terje Michaelsen, 'Governors of the Internet' in L-A Bygrave and J Bing (eds), *Internet Governance – Infrastructure and Institutions* (OUP 2009) 92–125.

13 Roger Clarke and others, 'A Primer on Internet Technology' (1998) <http://www.rogerclarke.com/II/IPrimer.html> accessed 1 May 2016.

14 H Alvestrand, 'A Mission Statement for the IETF' (October 2004) Best Current Practice 95, RFC 3935, 1 <http://tools.ietf.org/html/rfc3935> accessed 1 May 2016; B Carpenter (ed), 'Charter of the Internet Architecture Board (IAB)' (May 2000) Best Current Practice 39, IAB, RFC 2850, 2-3 <http://www.ietf.org/rfc/rfc3710.txt> accessed 1 May 2016.

15 S Bradner, 'The Internet Standards Process – Revision 3' (October 1996) RFC 2026, Best Current Practice 9, 2 <http://ftp://www.ietf.org/rfc/rfc2026.txt> accessed 1 May 2016.

16 L Lessig, *Code 2.0* (Basic Books 2006) 145. For an illustrative account of the role of the protocols see 143–45.

17 Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Texas L Rev 553–93, 582; Steven Wheatley, 'Democratic Governance Beyond the State: The Legitimacy of Non-state Actors as Standard-Setters' in A Peters and others (eds), *Non-State Actors as Standard Setters* (CUP 2009) 215–40, 220.

18 Seda Gürses and Bettina Berendt, 'PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm' in S Gutwirth, Y Poullet and P de Hert (eds), *Data Protection in a Profiled World* (Springer Science 2010) 301–22, 317.

norms developed online.[19] Although Internet standards are not legally binding, industry, organizations, Internet users and states adhere to and implement them.[20]

The Internet standard-setting does not observe formalities traditionally associated with the production of domestic or international law in terms of the processes followed, the actors involved and the final output.[21] This informality, however, does not necessarily mean that these bodies and the respective standardization process lack legitimacy. On the contrary, there is strong evidence to suggest that the IETF meets high standards of transparency and inclusiveness.[22] Much has been written about the legitimacy of the IETF's standardization work. Froomkin, in his seminal study, found that the IETF standard process 'harbors an environment capable of providing the "practical discourse" that Habermas suggests is a prerequisite to the creation of morally acceptable norms'.[23]

The establishment of the Internet's standardization bodies is informal. The IETF is organized as an activity of the Internet Society (ISOC)—a US non-profit entity—and the IAB is chartered both as a committee of the IETF and an advisory body of ISOC.[24] Informality extends to the internal structure of the two bodies. The IETF does not have an elected board and it enjoys financial independence.[25] Participation is free and open to all interested individuals and on an equal footing for all stakeholders (including States).[26]

19 In Lessig's words 'code is law' in Lessig (n 16) 223. Vinton Gray Cerf, 'Foreword: Who Rules the Net?' in A Thierer and CW Crews (eds), *Who Rules the Net?* (Cato Institute 2003) vii–xiii, vii; Graham Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21 University New South Wales L J 593–22, 608–17; Benjamin Farrand and Helena Carrapico, 'Guest Editorial: Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators' (2013) 10 Journal of Information Technology & Politics 357–68, 362; Daniel Benoliel, 'Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology' (2004) 92 California L Rev 1069–116.

20 Sanderijn Duquet and others, 'Upholding the Rule of Law in Informal International Lawmaking Processes' (2014) 6 Hague Journal on the Rule of Law 75–95, 90; Liv Coleman, '"We Reject: Kings, Presidents and Voting": Internet Community Autonomy in Managing the Growth of the Internet' (2013) 10 J Information Technol & Pol 171–89, 179; DG Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (OUP 2009) 134–42; Joost Pauwelyn, Ramses Wessel and Jan Wouters, 'Informal International Lawmaking: An Assessment and Template to Keep it Both Effective and Accountable' in J Pauwelyn, R Wessel and J Wouters (eds), *Informal International Lawmaking* (OUP 2012) 500–38, 512.

21 Joost Pauwelyn, 'Informal International Lawmaking: Framing the Concept and Research Questions' in Pauwelyn, Wessel and Wouters (n 20) 13–34, 17.

22 See, eg Duquet and others (n 20); Joost Pauwelyn, Ramses Wessel and Jan Wouters, 'Informal International Law as Presumptive Law: Exploring New Modes of Lawmaking' in R Liivoja and J Petman (eds), *International Law-making – Essays in Honour of Jan Klabbers* (Routledge Research in International Law 2014) 75; Pauwelyn, Wessel and Wouters (n 20) 521; Pauwelyn, ibid 18; Dan Burk, 'Legal and Technical Standards in Digital Rights Management Technology' (2005) 74 Fordham L Rev 537–73, 554.

23 Michael Froomkin, 'Habermas@discourse.net: Toward a Critical Theory of Cyberspace' (2003) 116 Harvard L Rev 749–73, 871.

24 Bygrave and Michaelsen (n 12) 96–97.

25 Harald Alvestrand and Hakon Wium Lie, 'Development of Core Internet Standards: the Work of the IETF and W3C' in Bygrave and Bing (n 12) 126–46, 128, 135.

26 Timothy Simcoe, 'Governing the Anti-commons: Institutional Design for Standard Setting Organizations' 6–7 <http://www.nber.org/chapters/c12944.pdf> accessed 1 May 2016. cf Pauwelyn (n 31) 19, 21, 33 and P Dann, M Engelhardt, 'Legal Approaches to Global Governance and Accountability: Informal Lawmaking, International Public Authority, and Global Administrative Law Compared' in Pauwelyn, Wessel and Wouters (n 20) 106, 112, 114.

Turning to the outputs of the informal law-making process, Internet standards and other deliverables, such as guidelines, or best current practices,[27] are adopted by consensus-making mechanisms. Each new proposal for a specification undergoes a period of review and revision and is initially published as a 'Request for Comment' (RFC) until (if) it reaches a certain level of maturity and turns into an Internet standard.[28] There are no formal voting rules and new standards are approved by 'rough consensus and running code', which means that the value of the ideas is assessed by the empirical proof of their feasibility and the combined engineering judgment of the participants.[29] For an Internet standard to be adopted the specifications needs to be of the highest technical quality and it needs to be supported by widespread community consensus. Of particular interest is the fact that a third requirement needs to be met, namely that the IETF must assess the interests of all affected parties as well as the specification's contribution to the Internet.[30] Consequently, the standard-setting process is porous to external concerns. The IETF can value and accommodate in its assessment specific societal interests and considerations, including arguably the impact of Internet protocols on the users' privacy.

States and other stakeholders underlined in the Tunis Agenda the immense contribution of the technical community to the shaping and evolution of the Internet, hence, acknowledging the legitimacy of the IETF and IAB to regulate the Internet.[31] Moreover, the positive and widespread reception of the standards by their addresses is a significant indicator of the bodies' legitimacy.[32] The industry sector and Internet users think 'the courts and politicians are so naïve [and] the only way to retain the ability to communicate privately is to come up with a long-term *technical solution*'.[33] Even though the perception of the technical solution as replacing or displacing the law could lead to a technocratic government of experts,[34] standardization, in the present context, does not necessarily have a negative connotation. 'The geeks will save the Internet and privacy' is a prevalent narrative among the Internet users.[35] The Internet's technical community is, or at least is perceived as being, the legitimate guardian of the network and the respective values it carries within it.

27 The Best Current Practice (BCP) is a subseries of the RFCs. BCP aims at defining and ratifying the IETF's best current thinking on specific issues. BCPs may vary in style and content but are subject to the same consensus-building and review process as all proposed standards. See Bradner (n 15) 15–16.

28 R Housley, D Crocker and E Burger, 'Reducing the Standards Track to Two Maturity Levels' (October 2011) RFC 6410, Best Current Practice 2, <http://tools.ietf.org/html/rfc6410> accessed 1 May 2016.

29 Alvestrand and Lie (n 25) 132; Milton L Mueller, *Ruling the Root* (MIT Press 2002) 91. Interestingly, see how Berners-Lee, the inventor of the World Wide Web, describes his experience with engaging with the IETF in Tim Berners-Lee, *Weaving the Web* (Harper Collins Publishers 2000) 53–63.

30 Bradner (n 15) 2–3.

31 World Summit on the Information Society (n 12) [35 (e)], [36].

32 Pauwelyn, Wessel and Wouters (n 22) 86–87.

33 Statement by L Levison owner of Lavabit - Snowden's email service - in 'Snowden Email Service Lavabit Loses Contempt Appeal' *BBC News* (17 April 2014) <http://www.bbc.com/news/technology-27063369> accessed 1 May 2016.

34 Pauwelyn, Wessel and Wouters (n 22) 90–91.

35 R Brandom, 'Snowden Calls on the Geeks to Save Us from the NSA' *The Verge* (12 March 2014) <http://www.theverge.com/2014/3/12/5500290/snowden-calls-on-the-geeks-to-save-us-from-the-nsa> accessed 1 May 2016.

The mandate of the internet standardization bodies to protect online privacy against mass surveillance

Even though privacy has always been a peripheral issue in the work of the IETF and IAB, the recent disclosures on mass surveillance by states[36] have forced the engineering community to face one of their major concerns, namely, the need to avoid exceeding their technical mandates or getting involved in politics. This section argues that the protection of online privacy falls within the remit of the standardization bodies' work. The IETF and IAB have, in fact, decided to defend the network against (mass) surveillance. The IETF, however, does not value privacy as a human right per se or as a legal consideration; privacy is an instrumental value and it is viewed as a necessary condition for restoring and maintaining users' trust in the Internet.[37]

It should be clarified that the work of the IETF, although technical, is not neutral or value-free.[38] Since Internet protocols are a form of regulation by default, standardization bodies also make choices by default.[39] Furthermore, the IETF's mission statement clearly states that 'the Internet isn't value-free and neither is the IETF'.[40] The IETF chooses to create *certain* technology by embracing *specific* technical concepts and ideas (decentralized control, edge-user empowerment and sharing resources).[41] The IAB, for its part, is entrusted with protecting the reliable operation of the Internet and the free flow of information, which is a broadly defined responsibility.[42]

The mandate of these bodies is not static: as the function and scope of the Internet evolves, so too will the role of the expert bodies entrusted with a public policy role in Internet governance. Protocol designers are more than familiar with the evolutionary nature of the Internet. In their view, the only principle of the Internet that will survive indefinitely is the principle of constant change: the architectural structure of the Internet is aimed at providing a set of rules (protocols) that generates a continuously evolving space of technology.[43] This is clear both in how the Internet is envisioned and how Internet standards develop.[44] Therefore, although these bodies are bound by their technical mandates, these mandates have to be read in the light of the needs of the users in whose name they act.[45] The protection of users' privacy is a serious and legitimate concern when designing and updating

36 UN Report on the Right to Privacy (n 1) [2]–[4].

37 See Helen Nissenbaum, 'Securing Trust Online: Wisdom or Oxymoron?' 81 (2001) BUL Rev 635–64 on the different meanings and nuances regarding the users' trust in the network.

38 Froomkin (n 23) 808–12; Sandra Braman, 'The Interpenetration of Technical and Legal Decision-Making for the Internet' (2010) 13 Information, Communication & Society 309–24, 313; ML Mueller, *Networks and States* (MIT Press 2010) 240–42. See also Pauwelyn, Wessel Wouters (n 20) 503–09.

39 Lessig (n 11) 79; Greenleaf (n 19) 608–17; Farrand and Carrapico (n 19) 362.

40 Alvestrand (n 14) 3.

41 L Denardis, *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009) 61, 71–77.

42 'Ethics and the Internet' (January 1989) Internet Activities Board, RFC 1087, 1–2, <http://www.ietf.org/rfc/rfc1087.txt> accessed 1 May 2016.

43 B Carpenter (ed), 'Architectural Principles of the Internet' (June 1996) RFC 1958, Informational, 1 <http://www.ietf.org/rfc/rfc1958.txt> accessed 1 May 2016.

44 Bradner (n 15) 3.

45 Alvestrand (n 14) 2–3. See also 2009 ICANN's Affirmation of Commitments, section 8 <http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm> accessed 1 May 2016.

protocols. As discussed earlier, the affected parties' interests[46] and the specification's contribution to the Internet's evolution are requirements to be addressed in the standardization process. Even though the engineers' ability to anticipate threats to privacy is limited,[47] the choices made in designing Internet protocols have profound implications for identifying and mitigating these threats.[48]

The IETF and IAB have accepted that their mandates encompass privacy issues by their recent acknowledgment that serious and systematic violations of users' privacy pose significant risks to the reliable operation of the Internet. The IETF Chair proclaimed that pervasive monitoring is a *threat* against which the Internet's engineers should defend.[49] Many strong voices from within the technical community took the position that engineers should reconsider the impact of protocol and system design choices in light of the serious issues involved in the protection of privacy.[50] In 2014, the IETF asserted its strong consensus that '[pervasive monitoring] is *an attack on the privacy of Internet users* and organizations'.[51] The pervasive nature of monitoring by specific states in collaboration with non-state actors is considered to constitute a breakdown in trust: the capabilities and activities of the attackers are greater; monitoring is highly indiscriminate and on a very large scale; and the surveillance is pervasive in terms of content.[52] In response to this attack on the network the technical bodies decided to expand their work by integrating privacy as a design requirement for the Internet standards (Privacy by Design).

Nonetheless, one should not lose sight of the fact that the IETF does not regard privacy as a human rights issue, but rather as a technical matter related to the functioning of the network.[53] Due to the unique features of the Internet's architecture, any threats to users' privacy equally qualify as threats to the fundamental value of the network: trust among its users. The core architecture of the network is its end-to-end design; this design, however, is based upon the presumption of trust.[54] Threats and risks to privacy, and especially pervasive monitoring, directly impact the level of trust placed by users in the network: compromising users' privacy undermines the

46 Froomkin (n 23) 808–12.

47 This is because Internet protocols are deployed within larger systems and are not always used in ways envisioned at the time of design. A Cooper and others, 'Privacy Considerations for Internet Protocols' (July 2013) IAB, RFC 6973, Informational, 5–6 <https://tools.ietf.org/html/rfc6973> accessed 1 May 2016.

48 Reidenberg (n 17) 570; Ann Cavoukian, Stuart Shapiro and R Jason Cronk, 'Privacy Engineering: Proactively Embedding Privacy by Design' (2014) 10–11 <http://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf> accessed 1 May 2016.

49 J Arkko, 'Message from the IETF Chair' (2014) 9 IETF Journal <http://www.internetsociety.org/publications/ietf-journal-march-2014/message-from-the-ietf-chair> accessed 1 May 2016.

50 T Hardie, 'A Personal Touchstone for Discussions of Pervasive Passive Monitoring' IETF, Internet-Draft (expired 22 April 2014) 3 <https://datatracker.ietf.org/doc/draft-hardie-perpass-touchstone/> accessed 1 May 2016.

51 Farrell and Tschofenig (n 2) 2 (emphases added).

52 'IAB Statement on Internet Confidentiality' (14 November 2014) <https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/> accessed 1 May 2016.

53 cf Fabrizio Cafaggi, 'Transnational Private Regulation and the Protection of Global Public Goods and Private "Bads"' (2012) 23 EJIL 695–718, 706 arguing that a human rights assessment should be considered relevant.

54 Carpenter (n 43) 1; R Bush and D Meyer, 'Some Internet Architectural Guidelines and Philosophy' (December 2002) RFC 3439, Informational, 3 <https://www.ietf.org/rfc/rfc3439.txt> accessed 1 May 2016; Dan L Burk, 'Federalism in Cyberspace Revisited' in Thierer and Crews (n 19) 119–57, 127.

network because the network *is* its end users. According to the engineering community's mindset, pervasive monitoring is an attack because users' participation in the network is adversely affected, the free flow of information is inhibited and the integrity and confidentiality of information are endangered. Threats to users' privacy undermine the reliable operation and the responsible use of the network as a whole.

Engineering privacy by design into the internet protocols

This section discusses how the IETF and IAB embed Privacy by Design requirements into the Internet protocols with the aim to protect end users from surveillance and serious threats to their privacy. Three specific threads of the ongoing standardization work have been selected: the introduction of a privacy vocabulary, encryption and the implementation of Privacy by Design in all layers of the network. It is argued that the development of Internet standards takes into consideration and, in turn, informs legal aspects of, the right to privacy as well as business practices.

It needs to be stressed from the outset that Privacy by Design affects the way the Internet is designed as well as the IETF's philosophy. The foundational end-to-end design principle encapsulates the choice made in the early development of the Internet to leave security and privacy issues to be addressed by the end users. This choice served the purpose of keeping the core communication Internet protocols as simple as possible.[55] It is for this reason that the Internet's engineers did not deem privacy to be a requirement when designing the Internet but rather something to be addressed by the end users.[56] This essential design principle, however, rests upon the fact that the Internet was originally built by a community of like-minded professionals who trusted each other.[57] In light of the unprecedented expansion of the Internet, and the recent revelations about state surveillance, the IETF re-examined its decision to leave privacy and security issues to the end users. In this sense, the integration of privacy requirements into the Internet standards signifies a rearrangement of the IETF's standardization philosophy and it indicates that privacy will be considered prior to designing new protocols or updating existing ones.[58] The consequence of shifting from the approach of leaving privacy to the end user to introducing Privacy by Design into the Internet protocols is that the core architecture of the Internet will encapsulate a higher level of privacy-protection features on a global level. This level of protection ensures stronger privacy protection than the (additional) measures taken by the individual user. The global interoperability of the network also ensures that privacy protection is ensured regardless of national borders, thereby mitigating threats to privacy and weakening the technical feasibility of conducting mass surveillance. The protection embedded in the technology of the Internet standards is, however, subject to any restrictions imposed by states. Similarly, the extent to which Privacy by Design features in the Internet protocols

55 Bush and Meyer, ibid 3.

56 Carpenter (n 43) 1, 2, 5.

57 J Kempf and R Austein (eds), 'The Rise of the Middle and the Future of the End-to-End: Reflections on the Evolution of the Internet Architecture' (March 2004) IAB, RFC 3724, Informational, 5 <https://www.ietf.org/rfc/rfc3724.txt> accessed 1 May 2016.

58 ibid 5, 8; New Security and Privacy Program established by the IAB in May 2014 <https://www.iab.org/activities/programs/privacy-and-security-program/> accessed 1 May 2016.

will impact end users depends on whether other stakeholders in the Internet's ecosystem, such as service providers, implement these protocols in all layers of the network, as it will be discussed below.

Developing a privacy vocabulary

In 2012 the IAB issued a report proposing, for the first time, a privacy-threat model with a specific focus on pervasive monitoring.[59] The model addresses the question of how surveillance can be countered on a technical level.[60] A notable contribution of this model is the creation of a privacy vocabulary, which defines privacy threats and establishes relevant terminology.[61] The main aim of this vocabulary is to introduce privacy-related concepts to the engineering community. Protocol designers need to be aware of specific engineering choices that can impact on privacy when crafting standards.[62] Just as the legal community is struggling to comprehend the technical aspects of privacy, the technical community is also in the process of realizing the value of privacy as a consideration in its work.[63]

What is particularly interesting about the development of a privacy vocabulary is its interrelation with privacy from a legal point of view. On the one hand, the technical community uses legal standards to inform its guidelines. The IETF not only documents the technical means employed to conduct mass surveillance, but also draws upon existing legal and policy privacy frameworks, such as texts by the Council of Europe, the Fair Information Practices, the Organization for Economic Co-operation and Development (OECD) guidelines concerning the collection and use of personal data and the Privacy by Design concept.[64] On the other hand, the technical community's work makes a relevant contribution to the legal community regarding the conceptualization of privacy in cases of (mass) surveillance.[65] A user-centric approach to privacy risks focuses on the ways in which end users feel threatened or suffer harm. The different types of privacy harm, including harm to financial standing, reputation, autonomy and safety, are discussed at length.[66] The IETF notes that 'when individuals or their activities are monitored, exposed, or at risk of exposure, those individuals may be stifled from expressing themselves, associating with others, and generally conducting their lives freely. They may also feel a general sense of unease'.[67] '[T]he effects of surveillance on the individual can range from anxiety and discomfort to behavioral changes such as inhibition and self-censorship. . . The *possibility* of surveillance may be

59 A Cooper, 'Report from the Internet Privacy Workshop' (January 2012) IAB, RFC 6462, Informational, 4–5 and 6–9, respectively <http://tools.ietf.org/html/rfc6462> accessed 1 May 2016.

60 R Barnes and others, 'Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement' (August 2015) RFC 7624, Informational, 1<https://tools.ietf.org/html/rfc7624> accessed 1 May 2016.

61 Cooper (n 59) 14.

62 Cooper and others (n 47) 4.

63 New Security and Privacy program established by the IAB in May 2014, <https://www.iab.org/activities/programs/privacy-and-security-program/> accessed 1 May 2016.

64 Cooper and others (n 47) 4, 18.

65 J Schiller, 'Strong Security Requirements for Internet Engineering Task Force Standard Protocols' (August 2002) RFC 3365, Best Current Practice 61, 2 <https://tools.ietf.org/html/rfc3365> accessed 1 May 2016; Daniel Le Métayer, 'Privacy by Design: A Matter of Choice' in Gutwirth, Poullet and de Hert (n 18) 323–34, 331.

66 Cooper and others (n 47) 12.

67 ibid.

enough to harm individual autonomy.'[68] The impact of surveillance, or the possibility of surveillance, on the autonomy and behaviour of Internet users is crucial from a technical point of view in assessing the erosion of trust placed in the network. From a legal standpoint, the Court of Justice of the European Union (ECJ) aligns with this perspective as far as the meaning of interference with the right to privacy is concerned. The ECJ found that mass and indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the EU Charter on the right to privacy and data protection, respectively.[69] More specifically, the ECJ held that the retention of traffic and location data without users being informed is likely to generate in the minds of the persons concerned the sense that their private lives are the subject of constant surveillance.[70] The collection of such data constitutes an interference with the right to privacy and it 'does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way'.[71] An interference with the right to privacy takes place regardless of whether the data has been subsequently processed, used or accessed by state authorities; these acts qualify as separate interferences.[72] There is already empirical evidence supporting the chilling effects of mass surveillance on the trust placed in the network and the exercise of freedom of expression online.[73]

Moreover, according to the IETF the *possibility* of covert surveillance suffices to threaten and adversely impact one's privacy. A similar nexus between the possibility of secret (mass) surveillance and the rights of personal autonomy and privacy is reflected in the approach of the European Court of Human Rights (ECtHR). In the recent *Zakharov* case the applicant claimed that there had been an interference with his privacy as a result of the mere existence of legislation permitting covert interception of mobile telephone communications and *the risk* of having been subjected to interception measures. The applicant was not in a position to furnish evidence that specific interception measures had been ordered against him. The ECtHR, by taking a rather flexible approach to the applicant's victim status and standing, accepted his arguments: when it comes to cases in which the secrecy of measures renders them effectively unchallengeable at the domestic level, the individual does not have to demonstrate the existence of a risk that surveillance measures were actually taken against him.[74] This position was reaffirmed in the *Szabó and Vissy* case.[75] It remains to be

68 ibid 13 (emphasis added).

69 Opinion of the Advocate General Bot in *Maximillian Schrems v Data Protection Commissioner*, C-362/14, 23 September 2015 [200].

70 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014 (Grand Chamber) [37].

71 ibid [33].

72 ibid [37]; UN Report on the Right to Privacy (n 1) [20].

73 Eg Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93 Journalism & Mass Communication Quarterly 296–311; Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645> accessed 1 May 2016.

74 *Roman Zakharov v Russia*, 4 December 2015 (Grand Chamber) [167]–[172].

75 *Szabó and Vissy v Hungary*, 12 January 2016 [37]–[41].

seen whether the ECtHR will reinstate this approach in the high-profile pending case brought by Big Brother Watch, Open Right Group, English Pen and Constanze Kurz against the UK Government Communications Headquarters (GCHQ). In a similar vein, the applicants argue that GCHQ conducted generic surveillance and that it is *likely* that they have been subjected to such interference. The applicants also contend that the generic interception of communications is an inherently disproportionate interference with the right to privacy of thousands, perhaps millions, of people.[76] If the ECtHR leans towards the *Zakharov* line of reasoning, it will be at variance with the *Clapper* judgment of the US Supreme Court. The Supreme Court dismissed by a slim 5–4 majority the applicants' claims as highly speculative fears and found that they had no standing.[77] In an unpersuasive judgment the Supreme Court held that there was no real likelihood that the government will at some point intercept some of the applicants' communications, and consequently that there was no actual or imminent injury (no injury-in-fact).[78]

Creating an encrypted web

The IETF is currently focusing on security and encryption as one of the means to mitigate privacy threats.[79] The Internet's engineers classify online surveillance as a combined security and privacy threat, underpinning the fact that security and privacy are interrelated.[80] In November 2014, the IAB issued a Statement on Internet Confidentiality in which it reaffirmed that the growth of the Internet depends on users having confidence that their private information is protected in the network.[81] The IAB underscored the importance that protocol designers, developers and operators should make encryption the norm for Internet traffic. The ongoing standardization work on 'opportunistic security' is aimed at ensuring some security, even when full end-to-end security is not possible.[82] A few new working groups have been set up, focusing on areas within the Internet protocols that have been neglected from a privacy point of view, such as Internet traffic and metadata. The working group on using transport layer security (TLS) in applications was established to increase the

76 *Big Brother Watch and Others v United Kingdom* (communicated case on 9 January 2014) Application No 58170/13. See also the pending *Bureau of Investigative Journalism and Alice Ross v United Kingdom* (communicated case on 5 January 2015) Application No 62322/14.

77 US Supreme Court, *Clapper v Amnesty International USA* 133 S Ct 1138 (2013).

78 ibid; cf Justice Breyer, with whom Justice Ginsburg, Justice Sotomayor, and Justice Kagan joint dissenting, 6.

79 The IETF's work to mitigate privacy threats revolves around (i) data minimization; (ii) user participation and empowerment; and (iii) security. These three areas can be loosely mapped to existing privacy principles, such as the Fair Information Practices, but they have been adapted to the aims and mindset of the engineers. See Cooper and others (n 47) 18.

80 The IAB created the Security and Privacy Program in May 2014 by merging two separate programmes on security and privacy respectively. Farrell and Tschofenig (n 2) 3; Cooper and others (n 47) 13.

81 IAB Statement on Internet Confidentiality (n 52).

82 See, for example, V Dukhovni, 'Opportunistic Security: Some Protection Most of the Time' (December 2014) RFC 7435, Informational, 3 <http://www.rfc-editor.org/rfc/rfc7435.txt> accessed 1 May 2016; Cooper and others (n 47) 10. D Meyer, 'How the Internet's Engineers are Fighting Mass Surveillance' (30 December 2014) <https://gigaom.com/2014/12/30/how-the-internets-engineers-are-fighting-mass-surveillance/> accessed 1 May 2016.

security of transmissions over the Internet, including email communications.[83] The Group has identified best practices in using TLS and unauthenticated encryption in future application definitions.[84] Furthermore, the working group on domain name system privacy considerations is developing a private exchange mechanism so that Domain Name System (DNS) transactions and queries become more private.[85]

The Article 29 Data Protection Working Party, in its Opinion 8/2014, and the European Data Protection Supervisor also acknowledge the interconnection between security concerns and privacy risks and violations.[86] In general, however, policy-makers and lawyers have not digested the complex interrelation between network/national/individual security and privacy online: privacy and security are in many cases in a symbiotic rather than an antithetical relationship, and privacy can be a pre-requisite for ensuring security.[87] Moreover, the emphasis placed by the IETF on increasing security and anonymity regarding Internet traffic and metadata mirrors the serious concerns over the (illusive) distinction between the content of communications and metadata (other non-content information). The UN High Commissioner on Human Rights has stressed that the distinction between content and metadata of communications is not persuasive, since metadata effectively reveal an individual's behaviour, social relationships, private preferences and identity.[88] The ECJ in the *Digital Rights* case has held that traffic and location data, taken as a whole, may allow very precise conclusions to be drawn concerning private lives.[89] Nonetheless, US courts have not (yet, at least) extended the Fourth Amendment protections on privacy to metadata used to route internet communications, including sender and recipient addresses on an email, or IP addresses.[90] In November 2015 the US Supreme Court rejected an appeal to the *USA v Davis* case to determine whether it is necessary to obtain a search warrant when law enforcement requests access to cell phone location data.[91] Although the introduction of encryption as the norm on the Internet is a necessary condition for ensuring secure and private online

83 <https://datatracker.ietf.org/wg/uta/documents/> accessed 1 May 2016.

84 Y Sheffer, R Holz and P Saint-Andre, 'Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)' (February 2015) RFC 7457, Informational <https://tools.ietf.org/rfc/rfc7457.txt> accessed 1 May 2016; Y Sheffer, R Holz and P Saint-Andre, 'Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)' (May 2015) RFC 7525, Best Current Practice 195 <https://tools.ietf.org/id/draft-ietf-uta-tls-bcp-11.txt> accessed 1 May 2016.

85 S Bortzmeyer, 'DNS Privacy Considerations' (August 2015) RFC 7626, Informational <https://www.rfc-editor.org/rfc/pdfrfc/rfc7626.txt.pdf> accessed 1 May 2016.

86 Art 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 16 September 2014, 4; Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, March 2010, [59].

87 For further discussion, see the subsection 'The Triptych of privacy, freedom of expression and security'.

88 UN Report on the Right to Privacy (n 1) [19]–[20].

89 *Digital Rights* case (n 70) [27].

90 In June 2014, the US Supreme Court unanimously ruled that the police must obtain a warrant from a court before searching a cellphone, explaining that an individual's email account is an electronic 'cache of sensitive personal information' that is entitled to the highest level of *Constitutional privacy protection Riley v California* 573 US _(2014).

91 See US Court of Appeals for the Eleventh Circuit, *United States v Quartavious Davis*, 5 May 2015; *United States v Jones*, 132 S.Ct 945, 950 (2012) and the very recent US Court of Appeals for the Sixth Circuit, *USA v Timothy Ivory Carpenter & Timothy Michael Sanders*, 13 April 2016.

communications, it is not sufficient notwithstanding that the impact of Internet Protocols is subject to their implementation by other stakeholders in Internet governance, as the next section will discuss.

Implementing and mainstreaming privacy by design

An innovative feature of the IETF's ongoing work is that it encourages the implementation of Privacy by Design into all layers of the Internet—and not only in the core (low-layer) Internet protocols.[92] The IETF has thus far focused mostly on the design and update of Internet protocols since it is difficult for protocol designers to foresee all pertinent privacy risks when browsers and web services implement standards. Privacy by Design, entrenched in the Internet's architecture, should ideally be implemented by Privacy by Design policies set by service providers and Privacy by Design legal/regulatory obligations prescribed by states. In this sense, Internet standards can nurture and shape privacy-protection practices in business practices,[93] and they have the potential to guide future regulation.[94] At the same time, the precise impact of the IETF's work on the end user is *dependent on* Privacy by Design policies and Privacy by Design legal regulation.

Many states have taken certain steps towards Privacy by Design policies. Privacy by Design is now prescribed as a legal standard in the EU General Data Protection Regulation which replaced the EU Data Protection Directive.[95] More specifically, Privacy by Design is a requirement that must be implemented by any person or organization controlling the collection, processing, holding or use of personal information.[96] It is the first document to define Privacy by Design as a legal obligation. Article 25 provides that 'the controller shall [. . .] implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing [. . .]'. Despite the high hopes invested in this provision, its concrete implementation remains unclear due to the vague caveats to the scope of the obligations of the data controller.[97] In addition, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework provides for the principle of preventing harm. The principle recognises that all means of regulating

92 Cooper and others (n 47) 5–6; Cooper (n 59) 9–11.

93 Cooper and others (n 47); Cooper (n 59).

94 Pauwelyn, Wessel and Wouters (n 20) 81; Ugo Pagallo, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in S Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer 2012) 331–46, 332–34; Joy Liddicoat and Avri Doria, 'Human Rights and Internet Protocols: Comparing Processes and Principles' 16 <http://www.internetsociety.org/sites/default/files/Human%20Rights%20and%20Internet%20Protocols-%20Comparing%20Processes%20and%20Principles.pdf> accessed 1 May 2016.

95 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 4 May 2016, L119/1.

96 Gehan Gunasekara, 'Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law' (2014) 22 Int J Law Info Tech 141–77, 161.

97 Opinion of the European Data Protection Supervisor (n 94) [39]–[45]; Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 Int J Law Info Tech 151–75, 159–60; European Union Agency for Network and Information Security, 'Privacy and Data Protection by Design – From Policy to Engineering' (December 2014) iii.

privacy—including technology, self-regulation and the law—must be designed to prevent privacy harm to individuals.[98] In a similar vein to the new EU Regulation, the principle affords no specific rights to individuals and no concrete obligations are imposed on data controllers.[99] It remains, therefore, to be seen how these principles will be formulated and implemented in the national context of EU and APEC member states. The APEC Privacy Framework retains its importance, if one bears in mind that APEC member states' economies are located on four continents and account for one-third of the world's population and almost half of world trade.

Privacy by Design policies cannot be effectively implemented and mainstreamed unless they are supported by appropriate technological security measures. Despite the business sector's chronic reluctance to increase privacy-protection features,[100] the post-Snowden arena provided a greater incentive, by transforming privacy into a business advantage. Silicon Valley's leading companies (eg Apple, Google, Twitter, Facebook and Snapchat) concentrate their efforts on introducing device encryption and incorporating end-to-end encryption into online services.[101] Google now tracks the encryption efforts—both at Google and on other popular websites by monitoring the progress made towards implementing HTTPS by default.[102] Interesting synergies between human rights organizations, such as the Electronic Frontier Foundation (EFF), companies and other stakeholders in Internet governance are also forged with respect to transport encryption in the form of HTTPS: 'Let's Encrypt' is an initiative that aims at setting up an HTTPS server and running a certificate management agent on the web server. Hewlett Packard, Facebook, the Internet Society, Cisco, Mozilla and Gelmato are some of the stakeholders involved.[103]

These initiatives have been received by states in an ambiguous fashion and one could say that state practice is in flux. On the one hand, data protection and other national authorities align with the need for security measures in order to ensure users' privacy. For instance, Article 29 of the Data Protection Working Party strongly recommends the application of Privacy by Design and Security by Design, including cryptography, when designing and manufacturing technology.[104] Moreover, states impose specific obligations on data controllers to ensure data security in order to avoid privacy breaches. The US Federal Trade Commission has sanctioned companies for having insufficient data security.[105] The French Data Protection Authority has imposed fines on companies for violations of the security and confidentiality of

98 Asia-Pacific Economic Cooperation, Privacy Framework (2005) 11 <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> accessed 1 May 2016.

99 G Greenleaf, *Asian Data Privacy Laws* (OUP 2014) 33–35.

100 See, in general, Ira S Rubinstein, 'Regulating Privacy by Design' 26 (2011) Berkeley Tech L J 1409–56; European Parliament Resolution on Surveillance (n 4) [62] [63] [110].

101 Danny Yadron, 'Facebook, Google and WhatsApp Plan to increase Encryption of User Data' *The Guardian* (14 March 2016) <http://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple> accessed 1 May 2016.

102 'Google Launches Project to Track Encryption Efforts - Both Internally and at Other Popular Sites' 15 March 2016, <http://www.circleid.com/posts/20160315_google_launches_project_to_track_encryption_efforts/> accessed 1 May 2016.

103 <https://letsencrypt.org/> accessed 1 May 2016.

104 Art 29, Opinion 8/2014 (n 86) 19, 22, 24.

105 For details see <https://www.ftc.gov/search/site/Wyndham%20Hotels> accessed 1 May 2016.

their customers' personal data, on the basis that they did not provide secure access to the Internet or had not implemented HTTPS (encrypted) or other security protocols.[106] Recently, the UK Information Commissioner Office has released updated guidance on the use of encryption stressing that encryption software should be used and that if data breaches occur where encryption was not used regulatory action may be pursued.[107]

On the other hand, and in contradiction to the aforementioned, states are divided as to whether they should regulate encryption and anonymity tools. The current, highly politicized debate in the US nencrypted iPhones or the issue of accessing WhatsApp encrypted instant messaging in Brazil[108] are the tip of the iceberg. States, including Russia, Morocco, Pakistan and Iran, have banned the use of encrypted communications altogether.[109] Against this backdrop, Germany and the Netherlands are two of the few states strongly supporting end-to-end encryption.[110] Interestingly, Germany has released the 'Charta for Strengthening Confidential Communication' stressing that encryption should become a standard for the masses in their private communication.[111] It seems that for the majority of states adopting a position is work-in-progress, which could be a positive indicator of subjecting possible changes to debate. The US after many back and forths decided (for now) that it will not regulate encryption; the Indian government withdrew a draft encryption policy after public uproar over the proposed measures;[112] and France seems to have abandoned its plans on banning Tor and other anonymity mechanisms.[113] Encryption in communications is unlikely to be banned. Similarly, suggestions to build 'backdoors' into systems or purposeful weaknesses that can be exploited to gain access have been officially dropped, although informal discussions with the private sector are on the table regarding granting access to unencrypted data or undermining data security and privacy. Most states, including

106 'Défaut de Sécurité de Données Clients: Sanction de 50 000 €à l' Encontre d'Optical Center' (13 November 2015) <http://www.cnil.fr/linstitution/missions/controler/actualite-controles/article/defaut-de-securite-de-donnees-clients-sanction-de-50-000-EUR-a-lencontre-doptical-cente/> accessed 1 May 2016.

107 <https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/> accessed 1 May 2016.

108 D Phillips and E. Nakashima, 'Senior Facebook Executive Arrested in Brazil After Police Are Denied Access to Data', The Washington Post, 1 March 2016 <https://www.washingtonpost.com/world/national-security/senior-facebook-executive-arrested-in-brazil-after-police-denied-access-to-data/2016/03/01/f66d114c-dfe5-11e5-9c36-e1902f6b6571_story.html> accessed 1 May 2016.

109 For state practice see Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, on the use of encryption and anonymity in digital communications, UN Doc A/HRC/29/32, 22 May 2015, [36]–[52]; Amnesty International, 'Encryption - A Matter of Human Rights', March 2016, 12, 25.

110 ibid. The Dutch government has granted a fund of 500.000 euros to OpenSSL, a project developing the widely used open-source encryption software library <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015> accessed 1 May 2016.

111 <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2015/charta-vertrauenswuerdige-kommunikation.html> accessed 1 May 2016.

112 <http://www.bbc.com/news/world-asia-india-34322118> accessed 1 May 2016.

113 <http://www.wired.co.uk/news/archive/2015-12/11/france-wont-ban-tor-or-wi-fi> accessed 1 May 2016.

China, France, the UK and the USA, opt out for the 'moderate' position of introducing targeted decryption orders.[114]

From a human rights law point of view, restrictions to encryption and anonymity as enablers of the right to privacy and freedom of expression must meet the well-known human rights three-part test: any limitations need to be provided by law, serve a legitimate aim and conform to the necessity and proportionality requirements.[115] Moreover, when states request disclosure of encrypted information procedural and judicial safeguards should be in place, including a judicial warrant. There is also merit in the argument that states have the *positive obligation* under the right to freedom of expression and the right to privacy to actively promote and facilitate security of online communications.[116] If such an obligation is read into the scope of these rights, the scrutiny of states' regulation of encryption and anonymity could be raised to a higher standard. Overall, the relevance of the *international* human rights law framework is noteworthy so that a clear point of reference is provided for policy-makers and judges on a universal level. Relying solely upon domestic law guarantees ignores the existing international safeguards and hinders their progressive development. Threats to privacy online are not anymore a matter to be framed and discussed in terms of (western) democratic *and* non-democratic states, as it is being presented.[117] Such distinctions are informative but they do not accurately reflect state practice and, therefore, they are meaningful to a certain extent.

To sum up, from a technical point of view, privacy protection is no longer a mere concern, but is now a guiding, structural principle of protocol design embedded into the DNA of the Internet and further disseminated to the deployment of Internet protocols. Privacy protection has become a thread running through the fundamental fabric of the Internet tapestry.[118] Following IETF's emphatic 2014 statement describing pervasive monitoring as an attack, and having demonstrated in this article the rigorous and systematic technical work in progress, it is reasonable to expect that the efforts to support Privacy by Design in the Internet standards will be further intensified.[119] Internet standardization is not, however, watertight and compartmentalized

114 China: Provisions on Decryption of Communications in Anti-Terrorism Law, Global Legal Monitor – Library of Congress, 17 February 2016 <http://www.loc.gov/law/foreign-news/article/china-provisions-on-decryption-of-communications-in-anti-terrorism-law/> accessed 1 May 2016; the French parliament seems to be in the final stages of approving legislation to penalise companies for refusing to decrypt messages see G Moody, 'France Votes to Penalise Companies for Refusing to Decrypt Devices, Messages', Ars Technica, 9 March 2016 <http://arstechnica.com/tech-policy/2016/03/france-votes-to-penalise-companies-for-refusing-to-decrypt-devices-messages/> accessed 1 May 2016; as far as the developments underway in the UK are concerned <http://www.dailydot.com/politics/encryption-uk-investigatory-powers-bill-nca-director-backdoors/> accessed 1 May 2016. Finally, there is a pending bill brought before the US Senate forcing companies to comply with court orders seeking locked communications.

115 UN Report on the use of encryption and anonymity in digital communications (n 109) [31]–[35], [58]; Report on 'Encryption - A Matter of Human Rights' (n 109) 15.

116 Report on 'Encryption - A Matter of Human Rights' (n 109) 37.

117 Stephen J Schulhofer, 'An International Right to Privacy? Be Careful What You Wish for' (2016) 14 I•CON 238–61.

118 Greenleaf (n 19) 606–07.

119 See the W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring, London (28 February–1 March 2014) <https://www.w3.org/2014/strint/Overview.html> accessed 1 May 2016.

from legal and regulatory developments. The development of Internet standards towards protecting privacy online and enhancing security of communications is in a symbiotic relationship with international human rights law and business practices.[120] This also involves that Privacy by Design entrenched into the Internet's technology and its impact to the Internet user is conditioned to how states will regulate Privacy by Design in law and how they will receive encryption and anonymity online.[121]

INTERNATIONAL HUMAN RIGHTS LAW 2.0: HOW THE TECHNICAL PERSPECTIVE ON PRIVACY INFORMS INTERNATIONAL HUMAN RIGHTS LAW

One of the main aspects of the international law discussion on privacy (vis-à-vis either the domestic protection of privacy or other international angles on privacy) is privacy's status as an international human right. The added value that the international human rights paradigm brings is that it 'provides the *universal framework* against which any interference in individual privacy rights must be assessed'.[122] Online privacy as a human right concerns first the applicability and second the application of international human rights law to the digital environment. A series of recent developments in the United Nations has formally acknowledged that human rights apply online. The UN General Assembly, in its 2014 Resolution, affirmed for the first time that the right to privacy applies in digital communications and called upon states to respect their associated obligations.[123] Similarly, the UN Human Rights Council has confirmed that the same rights that people enjoy offline must also be protected online, and has stressed that all states must address security concerns on the Internet in accordance with their human rights obligations.[124] The Human Rights Council also established the mandate for the UN Special Rapporteur on Privacy.[125] Turning to the application of the right to privacy online, the United Nations Office of the High Commissioner on Human Rights (OHCHR), the UN Special Rapporteur on the Freedom of Expression and the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism have made important contributions in setting out the human rights law framework applicable to recent practices of states and other actors.[126]

120 Reidenberg (n 17) 583. cf Cafaggi (n 53) 716 and Philip J Weiser, 'Internet Governance, Standard-Setting, and Self-Regulation' (2001) 28 Northern Kentucky L Rev 822–46.

121 NETmundial Statement (n 6) 9; 2013; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 3) [98]; Filippo Novario, 'Cyberspace, Surveillance and Law: A Legal Informatics Perspective' (2013) 4 Eur J L & Technol. Also Prasad Boradkar, 'Design as Problem Solving' in R Frodeman, J Thompson Klein and C Mitcham (eds), *The Oxford Handbook on Interdisciplinarity* (OUP 2010) 273.

122 UN Report on the Right to Privacy (n 1) [12] (emphasis added).

123 UNGA Res 68/167 (n 5); UNGA Res 69/166 (n 5).

124 Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' UN Doc A/HRC/26/L.24 (n 5) [1] [5]; See also Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', UN Doc A/HRC/20/L.13 (n 5).

125 'Human Rights Council Creates Mandate of Special Rapporteur on the Right to Privacy' Press Statement, 26 March 2015 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15763&LangID=E> accessed 1 May 2016.

126 Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/69/397, 23 September 2014.

They have underlined, in this respect, that mass or indiscriminate surveillance may be deemed arbitrary[127] or even an inherently disproportionate interference with the right to privacy.[128]

Yet the discussion is flux. It is not clear whether the international framework needs to be updated in order to accommodate technological advancements or whether a dynamic interpretation of the existing body of law will suffice. Suggestions at the UN level include the adoption of a new Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR) with regard to protecting privacy in the digital sphere,[129] or that the Human Rights Committee revisit General Comments 16 and 31.[130] Despite the possible usefulness of all the aforementioned ideas, one cannot fail to note that international law struggles to grasp and accommodate the concept and function of privacy in the online environment. This part argues that not only does the standardization work of the IETF operationalize privacy by design and enrich our perception of privacy; it also provides an opportunity to inform the mindset of the international lawyer. Few international and/or human rights bodies and international lawyers have substantially engaged with the legal implications of the Internet's design principles and special features.[131] The technical perspective on privacy, and the technical solutions to threats to privacy, should expand our legal imagination in terms of how the legal advisor argues on privacy, how the legislator articulates the interests at stake and how the academic and practitioner interpret existing law. The discussion that follows builds upon three examples which

127 Report on the Right to Privacy (n 2) [25]; 2013 UN Report on Freedom of Expression (n 3) [81]–[83].

128 'Joint Declaration on Freedom of Expression and Responses to Conflict Situation by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information', 4 May 2015, [8 (a)] <http://www.osce.org/fom/154846> accessed 1 May 2016.

129 The UN Special Rapporteur on Privacy recently called for a Geneva Convention for the Internet in A Alexander, *The Guardian*, 24 August 2015 <http://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief> accessed 1 May 2016 Germany advocated negotiations within the EU on this matter; see 'Measures for Better Privacy Protection - Progress Report', 14 August 2013 <http://www.scribd.com/doc/171155043/Measures-for-Better-Privacy-Protection> accessed 1 May 2016; European Parliament Resolution (n 4) [129]; 35th International Conference of Data Protection and Privacy Commissioners – Privacy: A Compass in Turbulent World, 'Resolution on Anchoring Data Protection and the Protection of Privacy in International Law', 23–26 September 2013 <https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf> accessed 1 May 2016.

130 'Common response of Austria, Liechtenstein, Slovenia and Switzerland to the OHCHR request regarding the right to privacy in the digital age', 26 February 2014, 3 <http://www.ohchr.org/Documents/Issues/Privacy/CommonResponse.pdf> accessed 1 May 2016.

131 The Annual Report of the Office of the Special Rapporteur for Freedom of Expression, in Annual Report of the Inter-American Commission on Human Rights, 31 December 2013, vol II, OEA/Ser.L/V/II.149 [523] and the Council of Europe Committee of Ministers in Council of Europe, 'Declaration by the Committee of Ministers on Internet Governance Principles' 21 September 2011, [8] are the only bodies discussing this issue. The UN Special Rapporteur on Freedom of Expression (n 3) [30]) and the Human Rights Council in its 2014 Resolution (n 5, rec 6) merely referred to the need to preserve people's confidence and trust in the network. The UN Report on the Right to Privacy (n 1) the Human Rights Council in its 2012 Resolution (n 5) and the UN General Assembly in its Resolution on the Right to Privacy in the Digital Age (n 5) do not make any reference to the special features of the Internet.

demonstrate the ways in which we could rethink our take on interpreting and applying international human rights law to privacy online. The first concerns the interrelation between privacy on the one hand and freedom of information and freedom of expression on the other, and how courts and legislators alike could take this interrelation into consideration. The second example addresses how the technical perspective could inform the policy-maker's mindset with regard to certain values invoked as limitations to privacy. Finally, the third case study attempts to revisit the relevance of the location and nationality of individuals and/or data in the digital environment.

The Triptych of privacy, freedom of expression and security

Recent developments demonstrate that many states are openly subjecting the free flow of information and the Internet's global reach to their national jurisdictions.[132] These policies frequently take the form of introducing restrictions regarding data location and data export. The motivations driving such policies vary, but privacy is the primary justification put forward. States—ranging from Russia and Saudi Arabia to Brazil, Germany and France—argue for their right to 'digital sovereignty', invoking their citizens'/residents' right to privacy, national security or even the development of the local economy.[133]

Addressing privacy as an intrinsic value for the integrity of the network provides informative insights on the human rights analysis. Protecting users' privacy, and their trust in the network, is tightly interconnected to freedom of information and the interoperability of the Internet at a global level. In other words, within the context of 'privacy as a technical issue', freedom of information and privacy are interlinked, and states are not able to easily invoke privacy as a possible limitation to freedom of information and transborder data flows. In addition, a rigorous understanding of the value of privacy and trust from the technical point of view updates our comprehension of the complex relationship between privacy, security and freedom of expression. In the online environment, these interests are interconnected in a distinctive fashion when compared to the offline environment. In many instances, the effective protection of privacy is a precondition for ensuring network, national and

132 See the Government of India in Press Information Bureau – Government of India – Ministry of External Affairs, 'Spy Program by the USA' 16 July 2014 <http://pib.nic.in/newsite/PrintRelease.aspx?relid=106792> accessed 1 May 2016; and the Sixth BRICS Summit – Fortaleza Declaration, 15 July 2014 [49] <http://brics6.itamaraty.gov.br/media2/press-releases/214-sixth-brics-summit-fortaleza-declaration> accessed 1 May 2016.

133 See, eg Russian Federal Law No 242-FZ 2014 which entered into force on the 1 September 2015 and establishes the requirement to localise personal data held on Russian citizens in Russia. The German Parliament approved on 16 October 2015 a new data retention law with localisation requirements; see <https://www.huntonprivacyblog.com/2015/10/16/german-parliament-adopts-data-retention-law-with-localization-requirement> accessed 1 May 2016. Also statement by Saudi Arabia arguing for each State's right to protect its citizens in the Third Committee of the General Assembly when discussing the right to privacy in the digital age; 69th Session, 73rd and 74th Meetings, UNGA – Meetings Coverage, 18 December 2014 <http://www.un.org/press/en/2014/ga11604.doc.htm> accessed 1 May 2016. For recent developments, see Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory L J 677–739; Alexander Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?' (2016) 32 CLSR 128–45; Francis Augusto Medeiros and Lee A Bygrave, 'Brazil's Marco Civil da Internet: Does It Live up to the Hype?' (2015) 31 CLSR 120–30.

international security as well as safeguarding freedom of expression.[134] The UN Rapporteur on Privacy has already underlined the critical role of privacy online both as complementary to security and as an enabling right to other human rights.[135]

International and domestic bodies and courts should explore how this perspective informs legal reasoning in two respects. Firstly, the strong interconnection between privacy and freedom of expression can be taken into account when freedom of expression is assessed as a proportionate and necessary restriction to the right to privacy, and vice versa. This is all the more the case since certain international courts—for instance, the ECtHR—seem to be predisposed towards protecting the right to privacy to the expense of acknowledging modern pronouncements of freedom of expression online (eg re-use of or turning data and databases to readable and searchable formats).[136] It would be also interesting to see how the ECtHR, in the *Bureau of Investigative Journalism* and the *10 Human Rights Organisations* cases, will discuss the allegation that the generic surveillance conducted by GCHQ violated *both* the right to privacy *and* freedom of expression and whether it will read the interests in accordance with international legal and technological developments.[137] Secondly, the symbiotic relationship between security on the one hand and privacy and freedom of expression on the other hand needs to be articulated in legal and human rights law terms. The fact that privacy and security can be mutually supportive goals entails that courts need to appreciate their interrelation in a non-conflictual fashion.[138] Security measures that aim to strengthen the protection of privacy, including encryption, ought to be carefully assessed. Weakening encryption will have serious ramifications not only to the right to privacy and freedom of expression,[139] but also to national and international security.[140] In this regard, the role of national and international courts will be instrumental in articulating and, if necessary, balancing the respective interests in ad hoc cases as well as pronouncing on the compatibility of

134 UN High Commissioner on Human Rights, 'Apple-FBI case could have serious global ramifications for Human Rights', Press Release, 4 March 2016 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E> accessed 1 May 2016.

135 Report of the Special Rapporteur on the Right to Privacy (n 10) [24]–[25].

136 *Satakunman Markkinapopsski and Satamedia OY v Finland*, 21 July 2015. The case was referred to and is currently pending before the Grand Chamber.

137 Pending cases: *Bureau of Investigative Journalism and Alice Ross v United Kingdom* (communicated case on 5 January 2015) Application No 62322/14; *10 Human Rights Organisations and Others v United Kingdom* (communicated case on 24 November 2015) Application No 24960/15.

138 Third party intervention to the *10 Human Rights Organisations and Others* case, 18 March 2016, 10, <https://epic.org/2016/03/epic-intervenes-in-privacy-cas.html> accessed 1 May 2016.

139 UN Report on the use of encryption and anonymity in digital communications (n 109); Letter addressed to the Hon. Sheri Pym in the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 ED No CM 16-10 (SP) <https://www.apple.com/pr/pdf/Letter_from_David_Kaye_UN_Special_Rapporteur_on_the_promotion_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf> accessed 1 May 2016.

140 UN High Commissioner on Human Rights, 'Apple-FBI Case Could Have Serious Global Ramifications for Human Rights', Press Release, 4 March 2016 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E> accessed 1 May 2016; UN Report on the use of encryption and anonymity in digital communications (n 109) [8], [56]; Susan Landau, Individual Statement, Berkman Centre for Internet & Society, 'Don't Panic. Making Progress on the "Going Dark" Debate', 1 February 2016.

recently introduced pieces of legislation regulating or banning encryption and/or anonymity (discussed earlier) or implementing domestic surveillance programmes.[141] The views of data protection authorities will also weight as Hamburg's data protection watchdog proved with respect to the right to use pseudonyms online and preserve anonymity.[142]

Privacy and bringing values and cultural considerations into play

Furthermore, the human rights perspective brings debates on values and cultural diversity to the surface. Certain states contended, in a draft resolution to the General Assembly, that respect for human rights online, including privacy, should be balanced against the cultural considerations and social systems of all countries.[143] Despite the fact that the HRC adopted the 2014 resolution on the right to privacy in the digital age without a vote, China, supported by South Africa, brought an oral amendment to the discussion of the draft resolution. The amendment concerned the inclusion of a paragraph in the resolution warning of the dangers that the Internet poses in terms of terrorism, extremism, racism and religious intolerance. Although the oral amendment was voted down,[144] 15 states supported the amendment, which makes it clear that there is no global consensus on Internet-related or privacy-related issues.[145] Therefore, even though the human rights angle puts pressure on states regarding the protection of online privacy, it also brings considerations which are invoked to place limitations on the effective exercise of privacy rights and which are usually construed very broadly. In this way, legal regulation undermines the interoperability of the Internet.[146]

At the other end of the spectrum, the technical approach to privacy lays the basis for a less heated cultural debate and promotes a language that certain states would

141 Eg although the French Constitutional Court validated the recent Law 912/2015, 24 July 2015 implementing a surveillance program, 13 complaints are currently pending before the ECtHR against this decision. <https://www.lexology.com/library/detail.aspx?g=2c230c55-43c6-4452-ad04-d6be99e15a2f> accessed 1 May 2016. Conversely, the English High court issued a landmark judgment in *David & Ors v Secretary of State for the Home Department* [2015] EWHC 2092 declaring the 2014 Data Retention and Investigatory Powers Act to be unlawful.

142 See, for instance, the current tension between Hamburg's data protection watchdog and Facebook over the use of fake names <http://arstechnica.co.uk/tech-policy/2016/03/pseudonym-ruling-facebook-claims-real-name-policy-protects-users/> accessed 1 May 2016.

143 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, 66th Session, UN Doc A/66/359, 14 September 2011, 4. The draft was subsequently co-sponsored by Kazakhstan and Kyrgyzstan.

144 The oral amendment was voted down by twenty-eight to fifteen votes. The states that voted in favour of the amendment were: Algeria, China, Congo, Cuba, Namibia, Russia, Pakistan, Saudi Arabia, South Africa, UAE, Venezuela and Vietnam. Four States abstained (Gabon, India, Indonesia and the Philippines).

145 cf C Bildt, Minister of Foreign Affairs of Sweden, who celebrated the existence of a 'global alliance for the freedom on the internet' when the Human Rights Council adopted its 2012 Resolution (n 5) on the freedom of information on the Internet in 'A Victory for the Internet', *New York Times*, 5 July 2012 <http://www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-internet.html?_r=3&> accessed 1 May 2016.

146 'The Rule of Law on the Internet and in the Wider Digital World', Issue Paper published by the Council of Europe Commissioner for Human Rights, December 2014, 40 <https://wcd.coe.int/ViewDoc.jsp?id=2268589> accessed 1 May 2016.

perhaps be more willing to accept. The technical perspective highlights the significance of users' privacy to the development of the digital economy. The growth of the Internet depends on users having confidence that their private information is secure and, consequently, privacy online is not only a human right, but also an enabler of public trust in the network.[147] Such a strategy can be persuasive when addressing policy-makers from specific regions of the world as well as when motivating lawmakers in general to enhance legal and technical privacy safeguards.[148] The International Conference of Data Protection, Privacy Commissioners and the European Data Protection Authorities as well as the APEC leaders have acknowledged the importance of safeguarding the integrity of the network as a value in itself.[149] There is, however, merit in arguing that the technical approach to privacy deprives the discussion of its socio-political dimensions.[150] It cannot go unnoticed that the human rights approach to cyberspace does not only refer to strictly speaking the applicability and application of human rights online but also introduces a 'humanisation' narrative of the Internet. This narrative brings in the mediation of power between State and individual and sets the parameters for defining the issues at stake or even prioritizing dissonant interests. Many state and non-state stakeholders endorse a rights-based approach to cyberspace. The NETmundial Multi-stakeholder Statement on the Future of Internet Governance devoted a section to 'Human Rights and Shared Values' and proceeded to proclaim that the Internet standards must be consistent with human rights.[151] The Council of Europe's Committee of Ministers has underlined (in the 2011 Declaration on Internet Governance Principles) the need for a '*rights-based approach* to the Internet'.[152] ISOC also employed human rights language and discourse by welcoming the 'formal endorsement of a *rights-based approach* for the Internet'. [153] To conclude, understanding and arguing for privacy could and should include different narratives and strategies highlighting different aspects of the discussion depending on the geographical/political context and the stakeholders involved.

147 IAB Statement on Internet Confidentiality (n 52).

148 See also Susan Shrink's comment, 'Should Internet Censorship be Considered a Trade Issue?' 12 April 2016 <https://www.chinafile.com/conversation/should-internet-censorship-be-considered-trade-issue> accessed 1 May 2016.

149 2013 Resolution (n 137); 'Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party' 25 November 2014, points 1 & 4 <http://europeandatagovernanceforum.com/pro/fiche/quest.jsp;jsessionid=oxBeuLGjbMbcy3ofZYYEunXT.gl2?surveyName=&main=&pg=&pg2=&pg3=&locale=1&_zz0_=&_zz1_=&_zz2_=&_zz3_=&_zz4_=&_zz5_=&_zz6_=&_zz7_=&_zz8_=&_zz9_=&_scrollX=0&_scrollY=0> accessed 1 May 2016; 23rd Leaders' Declaration, Building Inclusive Economies, Building a Better World: A Vision for an Asia-Pacific Community, 19 November 2015, point 3 (e) <http://www.apec.org/Meeting-Papers/Leaders-Declarations/2015/2015_aelm.aspx> accessed 1 May 2016.

150 For an excellent argument regarding the encryption debate see Sedra Gürses, Arun Kundnami, Joris Van Hoboken, 'Crypto and Empire: the Contradictions of Counter-surveillance Advocacy' (2016) Media, Culture & Society 1-15.

151 NETmundial Statement (n 6) 7.

152 CoE Declaration on Internet Governance Principles (n 131) [5] (emphases added).

153 'Internet Society Welcomes Adoption of Resolution on Human Rights and the Internet at 20th Human Rights Council', 9 July 2012 <http://www.internetsociety.org/news/internet-society-welcomes-adoption-resolution-human-rights-and-internet-20th-human-rights> accessed 1 May 2016 (emphases added).

The requirements of nationality and location of individuals (or data)

Safeguarding privacy as a *sine qua non* for the network's proper functioning casts a new light on the discussion of the nationality and location of individuals as requirements under international human rights law. These questions do not seem to be entirely settled in human rights law and practice, despite the recent strong pronouncements by the UN High Commissioner for Human Rights and the UN Special Rapporteur on Torture.[154] According to the technical viewpoint, neither the nationality nor the location of the individuals under surveillance is a critical—or even relevant—variable, since the Internet transcends national boundaries. A threat to users' privacy, and consequently to the network, exists regardless of nationality or the geographical particularities in question. It is of particular interest that claims that have been regarded until recently as policy considerations at best are now raised as legal arguments before courts and other bodies, and are given great weight by judges and policy-makers, respectively. The work of *Article 19*, an international NGO dedicated to the protection of freedom of expression, is noteworthy. *Article 19,* in its oral statement to the Human Rights Council Panel Discussion on Privacy, argued for the human right to online privacy by adopting the technical community's own mindset; it states that:

> '[w]here privacy online is threatened, *trust in the Internet* evaporates. Pervasive, untargeted and unchecked surveillance, including the interception, collection or retention of communications or meta-data, *is a systemic and structural attack on the Internet*, regardless of the nationality or location of the "target"'.[155]

Access Now and the Center for Democracy & Technology (CDT), in their amicus curiae briefs to US District Court of California regarding the matter of the search of an Apple iPhone seized during the execution of a search warrant, have devoted large sections of their arguments to the unintended detriment to end users, public trust in technology and digital security around the world, should the US Court decide to grant the Federal Bureau of Investigation's request.[156] These arguments have

154 UN Report on the Right to Privacy (n 1) [31]–[36] [47]; Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, (n 126) [62]; UNGA Res 69/166 (n 5). The Human Rights Committee has also emphasized the importance of 'measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, *regardless of the nationality or location of individuals whose communications are under direct surveillance*', Concluding Observations of the fourth Periodic Report of the United States of America, UN Doc CCPR/C/USA/CO/4, 23 April 2014, [22 (a)] (emphasis added). See Marco Milanović, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 86 Harv Intl'l L J 81–146.

155 UNHRC, 'Oral Statement on Freedom of Expression in the Digital Age', 12 September 2014 <http://www.article19.org/resources.php/resource/37686/en/unhrc:-oral-statement-on-freedom-of-expression-in-the-digital-age> accessed 1 May 2016 (emphases added).

156 Brief of *Amici Curiae* Access Now and Wickr Foundation in Support of Apple Inc.'s Motion to Vacate, in the Matter of the Search of An Apple iPhone Seized During the Execution of a Search Warrant, United States District Court for the Central District of California, Case No 5:16-cm-00010-SP-1 <http://images.apple.com/pr/pdf/Access_Now_and_Wickr_Foundation.pdf> accessed 1 May 2016; Brief of the Center for Democracy & Technology as Amicus Curiae in Support of Apple Inc.'s Motion to Vacate <http://images.apple.com/pr/pdf/Center_for_Democracy_and_Technology.pdf> accessed 1 May 2016.

become legally relevant because we are now exploring and conceptualizing the legal implications of the nature of the Internet. The arguments underline the global implications of acts of state authorities even if these acts take place within a state's territory. Clearly, although this does not entail that the nationality and location requirements under international human rights law became somewhat obsolete, such considerations and arguments inform a judge's approach.

Conversely, a state cannot extend its jurisdiction outside its national borders by way of circumventing privacy protection. The US Supreme Court has recently approved a rule change that could allow law enforcement to remotely search computers around the world.[157] Under the proposed change the government would be able to obtain a single warrant to access and search—essentially hack—any number of computers simultaneously regardless of their location or whether the users are a threat to national security or suspected of any crime.[158] Such a practice not only subverts legal safeguards of privacy both in the US and in third states but also compromises the functioning of the network. It is difficult to anticipate how the unpredictable nature of government malware to infiltrate user devices will perform in the real world. Government hacking also broadly undermines the security of the global Internet.[159] Similar suggestions for government hacking are being debated in the UK[160] and the Netherlands.[161] The execution of a US warrant to hand over a customer's email stored in a data centre in Ireland is also an attempt to evade human rights law safeguards in the territory of another state by putting pressure on a corporation (Microsoft).[162] It is true that data does not follow the predictable paths of the physical world and that the law and law enforcement need to keep up with the evolution of technology. The legal means to do so, however, need to serve transparency and respect international and national standards of online privacy. The use of means

157 Rule 41(b)(6) of Federal Rules of Criminal Procedure states that 'at the request of a federal law enforcement officer or an attorney for the government (. . .) a magistrate judge with authority in any district where activities related to a crime have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district' available at < https://www.documentcloud.org/documents/2819194-frcr16-8mad.html#document/p9/a291884> accessed 12 May 2016. The Supreme Court referred the change to US Congress, which will have until 1 December 2016 to modify, reject, or defer the proposal. If the House of Representatives and Senate do not pass a resolution in favour by simple majority, the revisions will become law that same day.

158 Danny Yadron, 'Supreme Court Grants FBI Massive Expansion of Powers to Hack Computers' 29 April 2016, <https://www.theguardian.com/technology/2016/apr/29/fbi-hacking-computers-warrants-supreme-court-congress> accessed 1 May 2016.

159 Brett Solomon, 'This Arcane Rule Change Would Give U.S. Law Enforcement New Power to Hack People Worldwide' Slate, 11 May 2016 <http://www.slate.com/blogs/future_tense/2016/05/11/the_rule_41_change_would_give_u_s_law_enforcement_power_to_hack_people_worldwide.html> accessed 12 May 2016.

160 David Connett and others, 'UK Government Rewrites Surveillance Law to Get Away with Hacking and Allow Cyber Attacks, Campaigners Claim' *The Independent* (15 May 2015) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-government-rewrites-surveillance-law-to-get-away-with-hacking-and-allow-cyber-attacks-campaigners-10253485.html> accessed 1 May 2016.

161 Tim Cushing, 'Dutch Government Moves To Let Intelligence Community Have More Hacking & Mass Surveillance Powers', 9 July 2015 <https://www.techdirt.com/articles/20150706/09575131559/dutch-government-moves-to-let-intelligence-community-have-more-hacking-mass-surveillance-powers.shtml> accessed 1 May 2016.

162 See <http://digitalconstitution.com/about-the-case/> accessed 1 May 2016.

of transnational cooperation, such as Mutual Legal Assistance Treaties, is a preferable way of thinking the way forward in such instances.

CONCLUSIONS

Internet standards, set by the IETF and IAB, are not legally binding nor do they have the potential to evolve into something binding. Nonetheless, Internet standards, constitute a powerful regulatory force by framing, and to a great extent shaping, the user's choices online. The discussion examined the computer engineers' approach to privacy online. The IETF has declared in the most emphatic terms that mass surveillance and serious threats to users' privacy are an attack on the reliable operation of the network. In this context, privacy online has an instrumental value as a necessary condition for retaining trust in the network. The IETF decided to integrate Privacy by Design into the core Internet architecture as a requirement when creating and updating standards. In this way, the level of privacy protection entrenched into technology is reinforced.

Three significant threads of the IETF's ongoing work are the development of a privacy vocabulary, the creation of an encrypted web and the renewed focus on implementing Privacy by Design in all layers of the network. It was argued that the technical discussion of many aspects of privacy interacts in manifold ways with the legal and human rights approaches to privacy: they enhance each other's understanding of the specificities of the online environment and they converge in their understanding of the meaning of interference in cases of surveillance or the protection of metadata to name a few examples. At the same time, the precise impact of Privacy by Design incorporated into protocols for the benefit of the end user is dependent on the practices of service providers on the application layer of the network and on state legislation. Currently, state practice is in flux regarding Privacy by Design as a legal obligation as well as the regulation (or the lack thereof) of encryption and anonymity tools that are indispensable to support privacy online.

Furthermore, the technical community's approach to privacy issues is an opportunity for international lawyers to rethink how we articulate, and argue for, privacy online from the point of view of international human rights law. This is a pressing need given the fact that national and international courts and bodies are expected to play a significant role in scrutinizing interferences with and restrictions to the right to privacy. The distinctive interconnection between privacy and freedom of information/expression online; the symbiotic relationship of privacy and security in many instances; or the relevance of the users' location and nationality, are issues that we need to consider seriously in legal reasoning and when conceptualizing and balancing the relevant interests.