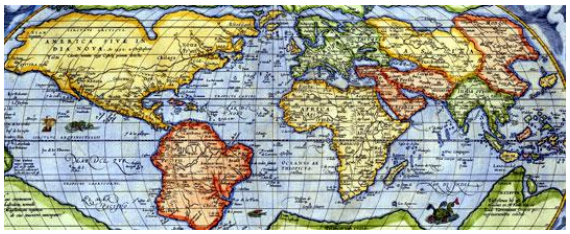
Rethinking Privacy Online and Human Rights

Rachovitsa, Adamantia

Published in:
European Society of International Law Conference Papers Series



European Society of International Law

Conference Paper Series

Conference Paper No. 5/2016

2016 ESIL Research Forum, Istanbul, 21-22 April 2016

Rethinking Privacy Online and Human Rights: The Internet's Standardisation Bodies as the Guardians of Privacy Online in the Face of Mass Surveillance

Adamantia Rachovitsa

Rethinking Privacy Online and Human Rights: The Internet's Standardisation Bodies as the Guardians of Privacy Online in the Face of Mass Surveillance

Adamantia Rachovitsa

Abstract:

There is a growing literature revolving around the role of non-State actors in the international law-making process. The starting point of this article is that although informal international law-making may not be legally binding, it would be unwise to dismiss it as legally irrelevant. Informal law-making can be relevant with respect to conceptualising and applying existing law, as well as guiding future regulation. The present discussion is placed in the context of cyberspace and, more specifically, the Internet standardisation bodies' informal law-making functions when creating Internet protocols by setting Internet standards. The article addresses the legitimacy and the ongoing work of the Internet Advisory Board and Internet Engineering Task Force in setting Internet standards with the aim to protect Internet users from mass surveillance and serious threats to privacy online. The article makes two main arguments. First, the effective protection of online privacy cannot be understood only in terms of compliance with legal frameworks but– in practice - that also needs to be secured through technological means. Second, in the area of online privacy informal law-making and international law converge in a distinctive way. Internet standards should not necessarily be seen as "living a parallel life" to law or as displacing or merely complementing the law. Technical standards and international law can actively inform one another and converge in their application. The analysis explores the implications of the Internet's technical features to policy-making and legal reasoning by discussing State and judicial practice. The article demonstrates how the technical perspective on privacy informs and enriches the manner in which the legal advisor argues about privacy, the legislator articulates the interests at stake and the judge and practitioner interpret and apply international human rights law.

Keywords: Internet standards; Internet protocols; online privacy; privacy by design; human rights; international informal law-making; mass surveillance; Internet Engineering Task Force; technology

Author Information:

Assistant Professor of Public International Law, Department of International Law, Faculty of Law, University of Groningen, NL; 2015-2016 Fellow at UC Berkeley - Center for Technology, Society & Policy. I would like to thank Mark Nottingham, Eva Kassoti, Thomas Skouteris and Mary Footer for useful feedback. Comments are welcome (a.rachovitsa@rug.nl).

Table of Contents

1. Introduction

There is a growing literature revolving around the role of non-State actors in the international law-making process. The starting point of this article is that, although informal international law-making may not be legally binding, it would be unwise to dismiss it as legally irrelevant. Informal law-making can be relevant with respect to conceptualising and applying existing law as well as guiding future regulation. The present discussion is placed in the context of cyberspace and, more specifically, the Internet standardisation bodies' informal law-making functions when creating Internet protocols (by setting Internet standards). Despite the emerging interest in the informal law-making activities of standardisation bodies,[1] the work of the Internet Architecture Board (IAB) and Internet Engineering Task Force (IETF) has escaped the attention of international

[1] For example, A von Bogdandy and others (eds), *The Exercise of Public Authority in International Institutions* (Springer 2010); A Peters and others (eds), *Non-State Actors as Standard Setters* (CUP 2009); J Pauwelyn, R Wessel, J Wouters (eds), *Informal International Lawmaking* (OUP 2012); 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.

lawyers. This is not the first time that novel international bodies appear, at first, insignificant or irrelevant in the eyes of international lawyers.[2]

The article addresses in particular how the Internet standardisation bodies create informal law-making (Internet standards) with the aim to protect Internet users from mass surveillance and serious threats to privacy online. 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".[3] The consequences of pervasive monitoring[4] cannot be duly appreciated unless one underlines that the exercise of the right to privacy is also a prerequisite for realizing other human rights – both online and offline[5] - and that serious and systematic attacks on online privacy further undermine relations among States, confidence of the citizens in the rule of law, and trust in the digital economy.[6] Despite the serious interests at stake, we are far from comprehending fully 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,[7] but international lawyers and courts as well as policy makers have just started to explore the

2 Anne Peters, Simone Peter, 'International Organizations: Between Technocracy and Democracy' in B Fassbender and others (eds), *The Oxford Handbook of the History of International Law* (OUP 2012) 170-197, 174-175 discussing how international law scholarship ignored, at first, the legal significance of the creation of the 19th-century international unions.

3 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).

4 For a definition of pervasive monitoring S Farrell, H Tschofenig (May 2014) 'Pervasive Monitoring Is an Attack', 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.

5 UN Report on the Right to Privacy (n 3) [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].

6 European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Program, 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, 111-112.

7 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 UN HRC Res 26/13, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', UN Doc A/HRC/RES/26/13 (26 June 2014) (adopted without a vote as orally revised), [1], [5]; UN HRC Res 20/8, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', UN Doc A/HRC/RES/20/8 (5 July 2012) (adopted without a vote); UN HRC Res 32/13, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (1 July 2016) (adopted without a vote as orally revised).

implications of the Internet's technical features to policy-making and legal reasoning.[8] 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, with a view to protect privacy online.[9] The article makes two main arguments. First, it argues that the effective protection of online privacy cannot be understood only in terms of compliance with legal frameworks but that – in practice - it also needs to be secured through technological means. Second, the article argues that, in the area of online privacy, informal law-making and international law converge in a distinctive way. Technical (Internet) standards should not necessarily be seen as "living a parallel life" to law or as displacing or merely complementing the law. The article shows how technical standards and international law can actively inform one another and converge in their application.

The analysis is structured into three main parts. The first part introduces the informal law-making work of the Internet's technical standardisation bodies – the IAB and IETF. The Internet is regulated and managed by technical standards which are developed by private bodies. The design of the network and Internet protocols by default encapsulate regulation and, therefore, international informal law-making is instrumental to how, and to what extent, the right to online privacy can be protected. The discussion explains the legal value of Internet standards from an international informal law-making point of view and assesses the legitimacy of the standards and the standard-setting process. The second part argues that protecting privacy online falls within the remit of the IETF's standardisation work. The IETF, however, 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 bodies focus on adopting a series of technical solutions, which will have a significant impact on the protection of end users from surveillance and serious threats to their privacy online. Work in progress includes the integration of Privacy by Design[10] into the core Internet protocols that form

[8] 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.

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

[10] 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 in place. The term 'privacy by design' was coined by Dr Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada. For a quick overview of different approaches see Ann 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.

the Internet's basic architecture,[11] the creation of a privacy vocabulary and encrypting the web. Interestingly, Internet standards are being informed by, and in turn shape and nurture, legal standards and business practices. The technical community employs legal definitions and texts in order to address the issue of the right to privacy. Conversely, its work on studying the implications of, and dangers posed by, mass surveillance not only assists in understanding the value of online privacy but also provides insights to much-debated legal questions, such as whether metadata fall within the protective scope of privacy, what constitutes an interference with privacy and how we legally conceptualise privacy harms in the online environment. Finally, 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. The relevance of the location and nationality of individuals in the digital environment and the interrelation of privacy and freedom of expression are questions that require us to revisit our take on interpreting and applying international human rights law to privacy online.

2. Internet Standards as Informal Law-making

Internet governance is highly fragmented in terms of the distribution of authority, reflecting the decentralised nature of the Internet 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 in formal and informal governance arrangements.[12] Despite this fragmentation and the absence 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 managing the technical aspects of the Internet. The IETF's goal is 'to make the Internet work better'[14] and its mission is to identify and suggest solutions to technical problems. The IAB, in turn, is responsible for reviewing the overall technical and

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

12 NETmundial Statement (n 8); 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, 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 (October 2004) 'A Mission Statement for the IETF', RFC 3935, Best Current Practice 95, 1 <http://tools.ietf.org/html/rfc3935> accessed 1 May 2016.

engineering development of the Internet.[15] These two bodies are the most important global standard-setters in the field and, therefore, their privacy-related work merits careful study.[16] This section explains the function of the Internet protocols and proceeds to address the protocols' value as informal law-making. The discussion also assesses the legitimacy of the standards and the standard-setting process.

2.1 The Function and Normative Value of Internet Standards

Internet protocols constitute the backbone of the Internet upon which all the layers of the network are created.[17] As such, they define - to a significant extent - how the Internet functions, and they frame the context of its legal regulation.[18] 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.[19] The default settings – from the design of the Internet protocols to a particular application or browser - shape the user's choices. Consequently, Internet protocols are a "hidden" yet powerful regulatory force complementing the law, the market and the social norms developed online.[20]

An (international) lawyer may perhaps struggle to identify the normative value of these protocols. Internet protocols are engineered on the basis of technical standards, known as Internet standards, set by the IETF and the IAB.[21] The Internet was created and is evolving by voluntary adherence

15 B Carpenter (ed), 'Charter of the Internet Architecture Board (IAB)' (May 2000) IAB, RFC 2850, Best Current Practice 39, 2-3 <http://www.ietf.org/rfc/rfc3710.txt> accessed 1 May 2016.

16 ML Rustad, *Global Internet Law* (West Academic Publishing 2014) 69-70.

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

18 Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Texas Law Review 553-593, 582; Steven Wheatley, 'Democratic Governance Beyond the State: The Legitimacy of Non-State Actors as Standard-Setters' in A Peters and others (n 1) 215-240, 220.

19 Seda Gürses, 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) 301-322, 317.

20 In Lessig's words "code is law" in Lessig (n 11) 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 Law Journal 593-622, 608-617; Benjamin Farrand, 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 357-368, 362; Daniel Benoliel, 'Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology' (2004) 92 California Law Review 1069-1116.

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

to these standards. Industry, organisations, Internet users and States adhere to these non-binding technical standards and, therefore, acknowledge the regulation of the Internet by informal law-making. It has been highlighted that 'there is no question […] of [the Internet] standards being legally binding or not. They are simply implemented by public and private actors'.[22]

2.2 The Internet Standard-setting Process and its Legitimacy

The Internet standard-setting process does not observe formalities traditionally associated with the production of domestic or international law in terms of the processes followed, the actors involved or the final output.[23] This informality, however, does not necessarily mean that these bodies and the respective standardisation process lack legitimacy.[24] On the contrary, there is strong evidence to suggest that the IETF meets high standards of transparency and inclusiveness.

A. Stakeholder Participation and Involvement in the Standard-setting Process

The establishment of the Internet's standardisation bodies is informal. The IETF emerged from a *quasi*-academic group of people who created the Internet. It was established as a body in 1986 and today it is still organised as an activity of the Internet Society (ISOC) - a US non-profit entity. The IAB, the members of which are selected from and by the IETF participants, is chartered both as a committee of the IETF and as an advisory body of ISOC.[25] The IETF is financially independent, funding its operations from conference fees and ISOC's membership fees.[26] Its informality extends also to the internal structure of the two bodies. The IETF does not have an elected board. There is no official membership and participation is open to all interested individuals on a voluntary basis. Anyone can attend its in-person meetings (held three times per

22 Duquet and others (n 1) 90; Liv Coleman, '"We Reject: Kings, Presidents and Voting": Internet Community Autonomy in Managing the Growth of the Internet' (2013) 10 Journal of Information Technology & Politics 171-189, 179; DG Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (OUP 2009) 134-142; Joost Pauwelyn, Ramses Wessel, Jan Wouters, 'Informal International Lawmaking: An Assessment and Template to Keep it Both Effective and Accountable' in Pauwelyn, Wessel, Wouters (n 1) 500-538, 512.

23 Joost Pauwelyn, 'Informal International Lawmaking: Framing the Concept and Research Questions' in Pauwelyn, Wessel, Wouters (n 1) 13-34, 17.

24 See, for example, Duquet and others (n 1); Joost Pauwelyn, Ramses Wessel, Jan Wouters, 'Informal International Law as Presumptive Law: Exploring New Modes of Lawmaking' in R Liivoja, J Petman (eds), *International Law-making – Essays in Honour of Jan Klabbers* (Routledge Research in International Law 2014) 75; Pauwelyn, Wessel, Wouters (n 22) 521; Pauwelyn (n 23) 18; Dan Burk, 'Legal and Technical Standards in Digital Rights Management Technology' (2005) 74 Fordham Law Review 537-573, 554.

25 Bygrave and Michaelsen (n 12) 96-97.

26 Harald Alvestrand, Hakon Wium Lie, 'Development of Core Internet Standards: the Work of the IETF and W3C' in Bygrave, Bing (n 12) 126-146, 128, 135.

year) or get involved via its email lists. Participants reflect the multi-stakeholder model and include primarily protocol designers, software developers and industry representatives as well as government officials, civil society and legal/privacy experts. It should be highlighted that public officials participate in the proceedings on an equal footing with other stakeholders. Transparency and inclusiveness are in many respects an integral part of the working culture of these bodies and their standard-making process.

That being said, there is scope for improving the participation of stakeholders in the IETF community (input legitimacy). There are two key issues in this regard: first, whether the relevant stakeholders are engaged in the decision-making process and, second, the quality of these stakeholders' involvement in, and impact on, the process.[27] Starting with the first question, in theory, anybody can participate in the standard-setting process. In practice, however, this is not the case, given the fact that the IETF discussions are highly technical. Indeed, the IETF has been accused of "technical elitism".[28] On the one hand, experienced contributors are needed to come up with the best technical solutions in order to avoid the risk of 'having good consensus about a bad design'.[29] On the other hand, one cannot deny the importance of having stakeholders on board who bring different perspectives on the impact and implications of the IETF's work. Ideally, these should be stakeholders directly affected by the Internet standards or the absence thereof.[30] Take the example of whether and, if so, to what extent, a journalist in Turkey or a young gay man in Uganda can benefit from secure email communications by using Internet protocols that support encryption.[31] Few end users actually have the ability to follow the technical discussions. One way to mitigate the absence of end users from the IETF is to include stakeholders who can mediate for them (clearly, not on their behalf) and for their interests.[32] The Centre for Democracy and

27 Wolfgang Benedek, 'Multi-Stakeholderism in the Development of International Law' in U Fastenrath and others (eds), *From Bilateralism to Community Interest – Essays in Honour of Judge Simma* (OUP 2011) 201-210, 204-205.

28 Joel Reidenberg, 'Yahoo and Democracy on the Internet', 42 (2002) Jurimetrics 261-280. See discussion in Michael Froomkin, 'Habermas@discourse.net: Toward a Critical Theory of Cyberspace' (2003) 116 Harvard Law Review 749-873, 795.

29 D Crocker, 'Making Standards the IETF Way' (1993) <http://www.isoc.org/internet/standards/papers/crocker-on-standards.shtml> accessed 1 May 2016.

30 Wheatley (n 18) 231.

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

32 Eric J. Iversen, Thierry Vedel, Raymund Werle, 'Standardisation and the Democratic Design of Information and Communication Technology' (2004) 17 Knowledge, Technology & Policy 104-126, 114, 121.

Technology (CDT)[33] is one such public-interest advocacy group actively participating in the IETF.

Turning to the quality of stakeholders' participation in the decision-making process, this is an issue that can be assessed only empirically. To give an example, the IETF's working culture consists of creative, highly opinionated scientists who debate over their ideas and proposals. This has led to the nurturing of a confrontational environment in which all parties must argue strongly for their positions in order to be heard and to persuade others. Yet many people find such an environment to be rather inaccessible, or even professionally inappropriate, especially if they come from an entirely different cultural background (e.g. Asia).[34] The IETF community seems to have acknowledged the matter and steps are being taken toward promoting greater diversity and establishing norms of professional conduct.[35]

B. Setting the Standards and Navigating the "Tussles"

In day-to-day work, technical standards are developed by working groups, which are set up to address specific operational and technical problems. The groups publish technical standards as well as other deliverables, such as guidelines or current best practice.[36] The standard-setting process is stipulated by a detailed set of procedural rules, which includes an appeal mechanism. Each new proposal for a specification is initially published as a "Request for Comment" (RFC) and it undergoes a period of review and revision, reflecting the strongly collaborative nature of the standards' development.[37] The proposed standard is a draft under discussion until (if) it reaches a certain level of maturity and becomes an Internet standard.[38] 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 evidence for their feasibility and the combined

---

33 The Centre is a US-based, non-profit organisation, which aims to preserve the user-controlled nature of the Internet and champions freedom of expression <https://cdt.org> accessed 1 May 2016.

34 Jorge L. Contreras, 'Divergent Patterns of Engagement on Internet Standardization: Japan, Korea and China' 38 (2014) Telecommunications Policy 916-934, 929-930.

35 D Crocker, Clark (November 2015) 'An IETF with Much Diversity and Professional Conduct', RFC 7704, Informational <https://www.rfc-editor.org/rfc/rfc7704.txt accessed 1 May 2016.

36 The Best Current Practice (BCP) is a subseries of the RFCs. BCP aims to define and ratify 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 The Internet Standards Process – Revision 3 (n 21) 15-16.

37 *Ibid*; R Housley, D Crocker, E Burger (October 2011) 'Reducing the Standards Track to Two Maturity Levels', RFC 6410, Best Current Practice 9 <http://tools.ietf.org/html/rfc6410> accessed 1 May 2016. See also G-P Calliess, P Zumbansen, *Rough Consensus and Running Code* (Hart Publishing 2012) discussing the concept of "rough consensus" in contexts other than Internet standardisation.

38 Reducing the Standards Track to Two Maturity Levels (n 37) 2.

engineering judgment of the participants.[39] Therefore, the process and the final outcome are supported by a strong and broad consensus, which is built and reinforced by the voluntary adherence of Internet users and the industry to these standards.[40] The IETF sets a high standard for legitimacy among standardisation and informal law-making bodies. 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'.[41] Internet standards are not only developed in a collaborative, multi-stakeholder environment,[42] but they are also open standards. This means that they are non-proprietary and no one has exclusive control of a protocol or its implementation, which in turn encourages experimentation and innovation.[43] Open standards encapsulate and, at the same time, reinforce the special features of the network in terms of its open, decentralised and interoperable architecture.[44] If it were not for the use of open standards, the interoperability of the network on a global scale would not have been feasible.[45] Finally, Internet drafts and standards are freely available on the IETF website, making the informal law-making process transparent, as opposed to, for example, ISO standards.[46]

Despite the fact that the creation of Internet standards seems to demonstrate a high level of legitimacy, the present discussion raises the question of whether broader, societal concerns can be taken into account when drafting a standard.[47] It is clear that for a specification to be adopted it needs to be of the highest technical quality and it must be supported by widespread consensus. In addition to these criteria, the standardisation process indicates that a third requirement should be met: the IETF needs to make an assessment of the interests of all affected parties as well as the specification's contribution to the Internet.[48] Consequently, the standard-setting process is, in principle, receptive to external concerns. Does this mean, however, that the IETF will

39 P. Resnick (June 2014) 'On Consensus and Humming in the IETF' RFC 7282, Informational <https://tools.ietf.org/html/rfc7282> accessed 31 August 2016; Alvestrand and Lie (n 26) 132; ML Mueller, *Ruling the Root* (MIT Press 2002) 91. Interestingly, see how Berners-Lee, the inventor of the World Wide Web, describes his experience of engaging with the IETF in T Berners-Lee, *Weaving the Web* (Harper Collins Publishers 2000) 53-63.

40 Post (n 22) 134-142; Pauwelyn, Wessel, Wouters (n 22) 512.

41 Froomkin (n 28) 871.

42 Greenleaf (n 20) 606.

43 Lessig (n 11) 145; Mueller (n 39) 91.

44 NETmundial Statement (n 8) 5, 7; Council of Europe, 'Declaration by the Committee of Ministers on Internet Governance Principles', 21 September 2011 [8].

45 Berners-Lee (n 39) 16, 163-164, 186; Coleman (n 22) 178.

46 <https://datatracker.ietf.org> accessed 1 May 2016. See 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.

47 Pauwelyn, Wessel, Wouters (n 22) 521; Pauwelyn (n 23) 18.

48 The Internet Standards Process – Revision 3 (n 21) 2-3.

acknowledge and consider other values and interests outside its technical mandate? For instance, will the IETF take freedom of expression or the privacy of the end users into account? The answer seems to be in the negative.

A careful reading of the IETF's mandate suggests that it must assess how a specification affects the interests of all relevant parties. The IETF will not take privacy into account as a value in itself, but instead will consider how an Internet protocol (or the absence thereof) impacts users' expectations of privacy and, therefore, their trust in the network. This point is further illustrated by an Internet-Draft that is currently being discussed in the IETF community. The 'representing stakeholder rights in Internet protocols' draft was a response to the mass surveillance revelations and it is an attempt to explore how the IETF encompasses stakeholder rights in Internet protocols and how it should address ethical, societal and legal judgments in protocol design.[49] Yet the draft was dropped and, almost a year later, a new draft was submitted to discussion ('The Internet is for End Users'). The new draft frames the main issues in an entirely different way; it focuses on identifying the different constituencies within the Internet community and evaluating the impact of Internet standards on those constituencies' interests. This removes from the equation any discussion of stakeholder rights/interests or of making societal/legal judgments when designing technology: the question rather revolves around the assessment of the impact of technology on the users' interests. In this way, the IETF remains committed to its technical mandate while still considering non-technical issues in the standard-setting process, albeit in a narrow framework. The Internet-Draft aims to set guidelines for computer engineers on how to identify different sub communities within the Internet community and how to assess the impact of Internet standards on them in a more systematic and open fashion.[50] The draft also stresses that end users should take priority over other sub communities (e.g. network operators, equipment vendors, service providers), even though sometimes a protocol design decision will need to strike a balance between the benefits to two or more sub communities. In such a case, any trade-offs must be documented and justified. If this Internet-Draft matures into an Internet standard, it will both enhance the clarity of the decision-making process (input legitimacy) and aid external parties when engaging with the results of the standards process (output legitimacy).[51] In a similar vein, the ongoing work of the recently established 'Human Rights Protocols Considerations' Research

49 M Nottingham (27 October 2014) 'Representing Stakeholder Rights in Internet Protocols', Internet-draft (expired 30 April 2015) <https://tools.ietf.org/id/draft-nottingham-stakeholder-rights-00.txt> accessed 1 May 2016.

50 M Nottingham (7 August 2015) 'The Internet is for End Users', Internet-Draft (work-in-progress, expires 21 April 2016) <https://datatracker.ietf.org/doc/draft-nottingham-for-the-users/> accessed 1 May 2016.

51 The Internet Standards Process – Revision 3 (n 21) 4. Also, Wheatley (n 18) 230.

Group explores how Internet standards can enable, strengthen or threaten human rights.[52] The Group's frame of reference is confined to examining how protocols impact other external values (human rights). It will be of interest to see whether the Group will discuss in more substantive terms the interrelation between Internet standards and human rights.

Consequently, the standard-setting process is receptive/open to external considerations as far as the impact of the IETF's work on the Internet community is concerned. Societal and broader interests, other values or public interest considerations are not examined in themselves;[53] what is examined is how Internet standards affect different communities and stakeholders with regard to such broader interests and concerns. What the IETF thinks that it is mandated to do is to navigate through the "tussles": different stakeholders have interests that may be opposed to each other and the standard-setting process aims to accommodate the existing tussles in a constructive fashion by making sure that the plurality of stakeholders' interests is duly acknowledged and, if need be, that a balance is struck in the course of the decision-making process.[54]

C. The Reception of Internet Standards: "The Geeks Will Save the Internet"?

Besides the fact that relevant stakeholders systematically implement the IETF standards, a strong indicator of the IETF's legitimacy is the positive and widespread reception of the standards by their addressees.[55] In this instance, the addressees of these standards include every Internet user as well as a number of stakeholders with specific interests, including States, network operators, equipment vendors and specification implementers. States and other stakeholders underlined in the Tunis Agenda the immense contribution of the technical community to the shaping and evolution of the Internet.[56] Furthermore, the industry sector and Internet users believe that '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.'[57] Even though technical solutions can lead to a technocratic government of experts,[58] standardisation, in the present context, does

52 Chartered Human Rights Protocol Considerations Research Group <https://irtf.org/hrpc> accessed 1 May 2016.

53 For example, see the Internet Draft co-sponsored by CDT J Morris and others (18 October 2010) 'Policy Considerations for Internet Standards' (expired 21 April 2011).

54 David D. Clark and others, 'Tussle in Cyberspace: Defining Tomorrow's Internet', Proceedings of ACM Special Interest Group on Data Communications (2002) <http://conferences.sigcomm.org/sigcomm/2002/papers/tussle.pdf> accessed 1 May 2016.

55 Pauwelyn, Wessel, Wouters (n 24) 86-87.

56 Tunis Agenda (n 12) [35 (e)] [36].

57 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.

58 Pauwelyn, Wessel, Wouters (n 24) 90-91; Peters and Peter (n 2) 195.

not necessarily have negative connotations. "The geeks will save the Internet and privacy" is a prevalent narrative among Internet users.[59] This strong social legitimacy seems to do justice to the values that this transnational community serves, and to its readiness to protect these values against external interference. One should recall that, when in 1992 the IETF participants thought that there was an attempt to interfere politically with its technical work and to establish internal hierarchies within the community, they declared that 'We reject: kings, presidents and voting. We believe in: rough consensus and working code'.[60] The Internet's technical community is, or at least is perceived to be, the legitimate guardian of the network and the values it carries within it.

3. Creating Informal Law-making for Protecting Privacy Online

3.1 Appreciating Online Privacy as a Technical Issue

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[61] 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 standardisation 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.[62]

It needs to be clarified from the outset that the work of the IETF, although technical, is not neutral or value-free.[63] Since Internet protocols are a form of regulation by default, standardisation bodies also make choices by default.[64] Furthermore, the IETF's mission statement clearly States that 'the Internet isn't value-free and neither is the IETF'.[65] The IETF chooses to create certain technology by embracing specific technical concepts and ideas (decentralized control, edge-user

59 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.

60 For further discussion, see Coleman (n 22) 180-183.

61 UN Report on the Right to Privacy (n 3) [2]-[4].

62 See Helen Nissenbaum, 'Securing Trust Online: Wisdom or Oxymoron?' 81 (2001) B.U.L.Rev. 635-664 on the different meanings and nuances regarding the users' trust in the network.

63 Froomkin (n 28) 808-812; Sandra Braman, 'The Interpenetration of Technical and Legal Decision-Making for the Internet' (2010) 13 Information, Communication & Society 309-324, 313; ML Mueller, *Networks and States* (MIT Press 2010) 240-242. See also Pauwelyn, Wessel, Wouters (n 22) 503-509.

64 Lessig (n 11) 79; Greenleaf (n 20) 608-617; Farrand and Carrapico (n 20) 362.

65 A Mission Statement for the IETF (n 14) 3.

empowerment and sharing resources).[66] 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.[67]

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.[68] This is clear both in how the Internet is envisioned and how Internet standards develop.[69] 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.[70] The protection of users' privacy is a serious and legitimate concern when designing and updating protocols. As discussed earlier, the affected parties' interests[71] and the specification's contribution to the Internet's evolution are requirements to be addressed in the standardisation process. Even though the engineers' ability to anticipate threats to privacy is limited,[72] the choices made in designing Internet protocols have profound implications for identifying and mitigating these threats.[73]

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

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

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

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

69 The Internet Standards Process – Revision 3 (n 21) 3.

70 A Mission Statement for the IETF (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.

71 Froomkin (n 28) 808-812.

72 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, H Tschofenig, B Aboba, J Peterson, J Morris, M Hansen, R Smith (July 2013) 'Privacy Considerations for Internet Protocols', IAB, RFC 6973, Informational, 5-6 <https://tools.ietf.org/html/rfc6973> accessed 1 May 2016.

73 Reidenberg (n 18) 570; Ann Cavoukian, Stuart Shapiro, 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.

threat against which the Internet's engineers should defend.[74] 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.[75] In 2014, the IETF asserted its strong consensus that '[pervasive monitoring] is an attack on the privacy of Internet users and organizations'.[76] 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.[77] 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.[78] 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.[79] 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 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.

3.2 The Technical "Solution" to Serious Threats to Privacy Online and its Relevance to International Human Rights Law

74 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.

75 A Personal Touchstone for Discussions of Pervasive Passive Monitoring (n 31) 3.

76 Pervasive Monitoring is an Attack (n 4) 2 (emphases added).

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

78 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.

79 Architectural Principles of the Internet (n 68) 1; R Bush, D Meyer (December 2002) 'Some Internet Architectural Guidelines and Philosophy', RFC 3439, Informational, 3 <https://www.ietf.org/rfc/rfc3439.txt> accessed 1 May 2016; Dan L. Burk, 'Federalism in Cyberspace Revisited' in Thierer, Crews (n 20) 119-157, 127.

The technical "solution" to serious threats to privacy online comprises of integrating Privacy by Design requirements into the Internet protocols. The first section discusses two specific threads of the IETF's ongoing standardisation work, namely, the introduction of a privacy vocabulary and encrypting the Web. The analysis shows that informal law-making in this area is relevant to business practices and legal regulation. The technical community takes into consideration and, in turn, informs legal aspects of, the right to privacy. In this sense, Internet standards can nurture and shape privacy-protection practices in business practices,[80] and they have the potential to guide future regulation.[81] At the same time, however, the protection embedded in the technology of the Internet standards is subject to any restrictions imposed by States. Similarly, the extent to which Privacy by Design features in the Internet protocols 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.

A. Integrating Privacy by Design into Internet Protocols

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.[82] 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.[83] 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.[84] 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 standardisation philosophy and it indicates that privacy will be considered prior to

80 Privacy Considerations for Internet Protocols (n 72).

81 Pauwelyn, Wessel, Wouters (n 24) 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) 331-346, 332-334; Joy Liddicoat, 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.

82 Some Internet Architectural Guidelines and Philosophy (n 79) 3.

83 Architectural Principles of the Internet (n 68) 1, 2, 5.

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

designing new protocols or updating existing ones.[85] 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.

i. 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.[86] The model addresses the question of how surveillance can be countered on a technical level.[87] The IAB also established a privacy directorate to ensure that privacy considerations are considered and incorporated accordingly when drafting Internet standards.[88] This is an example of how the bodies' remain vigilant with regard to shaping their working culture and adapting their internal organisational structure. Furthermore, a notable contribution of this model is the creation of a privacy vocabulary, which defines privacy threats and establishes relevant terminology.[89] 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.[90] Just as the legal community is struggling to comprehend the technical aspects of privacy, the technical community is also in the process of realising the value of privacy as a consideration in its work.[91]

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,

85 *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.

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

87 R Barnes, B Schneier, C Jennings, T Hardie, B Trammell, C Huitema, D Borkmann (August 2015) 'Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement', RFC 7624, Informational, 1<https://tools.ietf.org/html/rfc7624>.

88 Report from the Internet Privacy Workshop (n 86) 14.

89 *Ibid*.

90 Privacy Considerations for Internet Protocols (n 72) 4.

91 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.

such as texts by the Council of Europe, the Fair Information Practices, and the OECD guidelines concerning the collection and use of personal data and the Privacy by Design concept.[92] On the other hand, the technical community's work makes a relevant contribution to the legal community regarding the conceptualisation of privacy in cases of (mass) surveillance.[93] 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.[94] 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'.[95] '[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 enough to harm individual autonomy'.[96] 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.[97] 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.[98] 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.'[99] An interference with the right to privacy takes place regardless of whether the data has subsequently been processed, used, or

92 Privacy Considerations for Internet Protocols (n 72) 4, 18.

93 J Schiller (August 2002) 'Strong Security Requirements for Internet Engineering Task Force Standard Protocols', 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, de Hert (n 19) 323-334, 331.

94 Privacy Considerations for Internet Protocols (n 72) 12.

95 *Ibid*.

96 *Ibid*, 13 (emphasis added).

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

98 *Digital Rights* case [37].

99 *Ibid* [33].

accessed by State authorities; these acts qualify as separate interferences.[100] There is already evidence supporting the chilling effects of mass surveillance on the trust placed in the network and the exercise of freedom of expression online.[101]

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 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.[102] This position was reaffirmed in the *Szabó* and *Vissy* cases.[103] It remains to be 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.[104] If the ECtHR leans toward 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.[105] 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

100 *Ibid* [37]; UN Report on the Right to Privacy (n 3) [20].

101 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.

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

103 *Szabó and Vissy v Hungary*, 12 January 2016 [37]-[41].

104 *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.

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

applicants' communications, and consequently that there was no actual or imminent injury (no injury-in-fact).[106]

ii. Creating an Encrypted Web

The IETF is currently focusing on security and encryption as one of the means to mitigate privacy threats.107 The Internet's engineers classify online surveillance as a combined security and privacy threat, underpinning the fact that security and privacy are interrelated.[108] 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.[109] The IAB underscored the importance that protocol designers, developers and operators should make encryption the norm for Internet traffic. The on-going standardisation work on "opportunistic security" is aimed at ensuring some security, even when full end-to-end security is not possible.[110] 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 security of transmissions over the Internet, including email communications.[111] The Group has identified best practices in using TLS and unauthenticated encryption in future application definitions.[112] Further, the working group on domain name system privacy considerations is developing a private exchange mechanism so that

106 *Ibid*; cf Justice Breyer, with whom Justice Ginsburg, Justice Sotomayor, and Justice Kagan join, dissenting, 6.

107 The IETF's work to mitigate privacy threats revolves around 1) data minimisation; 2) user participation and empowerment; and 3) 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 Privacy Considerations for Internet Protocols (n 72) 18.

108 The IAB created the Security and Privacy Program in May 2014 by merging two separate programmes on security and privacy respectively. Pervasive Monitoring is an Attack (n 4) 3; Privacy Considerations for Internet Protocols (n 72) 13.

109 IAB Statement on Internet Confidentiality (n 77).

110 See, for example, V Dukhovni (December 2014) 'Opportunistic Security: Some Protection Most of the Time', RFC 7435, Informational, 3 <http://www.rfc-editor.org/rfc/rfc7435.txt> accessed 1 May 2016; Privacy Considerations for Internet Protocols (n 72) 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.

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

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

DNS transactions and queries become more private.[113]

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.[114] 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 prerequisite for ensuring security.[115] 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.[116] 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.[117] 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.[118] 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.[119] Although the introduction of encryption as the norm on the Internet is a necessary condition for ensuring secure and private online 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.

---

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

114 Article 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].

115 For further discussion, see 3.1.

116 UN Report on the Right to Privacy (n 3) [19]-[20].

117 *Digital Rights* case [27].

118 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 U.S _(2014).

119 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.

B. Privacy by Design Subject to Law and Business Practices

Privacy by Design as a technological/informal law-making standard embedded into Internet protocols is yet subject to law as well as business practices. To be accurate, it is the precise impact of the Internet standards to the Internet user's privacy that depends on how the Privacy by Design is implemented into all layers of the network. The IETF has thus far focused mostly on the design and update of core (low-layer) Internet protocols since it is difficult for protocol designers to foresee all pertinent privacy risks when browsers and web services implement standards. 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.[120] 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.

Many States have taken certain steps toward 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.[121] More specifically, Privacy by Design is a requirement that must be implemented by any person or organisation controlling the collection, processing, holding or use of personal information.[122] 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.[123] 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 privacy - including technology, self-regulation and the law

120 Privacy Considerations for Internet Protocols (n 72) 5-6; Report from the Internet Privacy Workshop (n 86) 9-11.

121 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.

122 Gehan Gunasekara, 'Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law' (2014) 22 Int J Law Info Tech 141-177, 161.

123 Opinion of the European Data Protection Supervisor (n 114) [39]-[45]; Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 Int J Law Info Tech 151-175, 159-160; European Union Agency for Network and Information Security, 'Privacy and Data Protection by Design – From Policy to Engineering' (December 2014) iii.

- must be designed to prevent privacy harm to individuals.[124] 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.[125] 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,[126] the post-Snowden era provided a greater incentive, by transforming privacy into a business advantage. Silicon Valley's leading companies (e.g. Apple, Google, Twitter, Facebook and Snapchat) concentrate their efforts on introducing device encryption and incorporating end-to-end encryption into online services.[127] Google now tracks the encryption efforts - both at Google and on other popular websites by monitoring the progress made toward implementing HTTPS by default.[128] Interesting synergies between human rights organisations, 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, Gelmato are some of the stakeholders involved.[129]

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

---

[124] 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.

[125] G Greenleaf, *Asian Data Privacy Laws* (OUP 2014) 33-35.

[126] See, in general, Ira S. Rubinstein, 'Regulating Privacy by Design' 26 (2011) Berkeley Tech. L. J. 1409-1456; European Parliament Resolution on Surveillance (n 6) [62] [63] [110].

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

[128] '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.

[129] <https://letsencrypt.org/> accessed 1 May 2016.

Security by Design, including cryptography, when designing and manufacturing technology.[130] 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.[131] The French Data Protection Authority has imposed fines on companies for violations of the security and confidentiality of 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.[132] 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.[133]

On the other hand, and in contradiction to what was mentioned previously, States are divided as to whether they should regulate encryption and anonymity tools. The current, highly politicised debate in the US on encrypted iPhones or the issue of accessing WhatsApp encrypted instant messaging in Brazil[134] are the tip of the iceberg. States, including Russia, Morocco, Pakistan and Iran, have banned the use of encrypted communications altogether.[135] Against this backdrop, Germany and the Netherlands are two of the few States strongly supporting end-to-end encryption.[136] Interestingly, Germany has released the "Charta for Strengthening Confidential Communication" stressing that encryption should become a standard for the masses in their private communication.[137] It seems that for the majority of States adopting a position is work-in-

130 Article 29, Opinion 8/2014 (n 114) 19, 22, 24.

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

132 '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.

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

134 D Phillips, 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.

135 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.

136 *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.

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

progress, which could be a positive indicator of subjecting possible changes to debate. The US after many 'backs 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;[138] and France seems to have abandoned its plans on banning Tor and other anonymity mechanisms.[139] 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 China, France, the UK and the US, opt out for the "moderate" position of introducing targeted decryption orders.[140]

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.[141] 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.[142] 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

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

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

140 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.

141 UN Report on the use of encryption and anonymity in digital communications (n 135) [31]-[35], [58]; Report on 'Encryption - A Matter of Human Rights', (n 135) 15.

142 Report on 'Encryption - A Matter of Human Rights', (n 135) 37.

and discussed in terms of (western) democratic and non-democratic States, as it is being presented.[143] 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.[144] Following IETF's emphatic 2014 statement describing pervasive monitoring as an attack, and having demonstrated in this paper 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.[145] Internet standardisation is not, however, watertight and compartmentalised from legal and regulatory developments. The development of Internet standards toward protecting privacy online and enhancing security of communications is in a symbiotic relationship with international human rights law and business practices.[146] 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.[147]

4. Thinking Outside the "International Human Rights Law" Box

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.'[148] Online privacy as a human right concerns, first, the applicability and,

143 Stephen J. Schulhofer, 'An International Right to Privacy? Be Careful What You Wish for' (2016) 14 I•CON 238-261.

144 Greenleaf (n 20) 606-607.

145 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.

146 Reidenberg (n 18) 583. cf Cafaggi (n 78) 716 and Philip J. Weiser, 'Internet Governance, Standard-Setting, and Self-Regulation' (2001) 28 Northern Kentucky Law Review 822-846.

147 NETmundial Statement (n 8) 9; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 5) [98]; Filippo Novario, 'Cyberspace, Surveillance and Law: A Legal Informatics Perspective' (2013) 4 European Journal of Law & Technology. Also Prasad Boradkar, 'Design as Problem Solving' in R Frodeman, J Thompson Klein, C Mitcham (eds), *The Oxford Handbook on Interdisciplinarity* (OUP 2010) 273.

148 UN Report on the Right to Privacy (n 3) [12] (emphasis added).

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.[149] 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.[150] The Human Rights Council also established the mandate for the UN Special Rapporteur on Privacy.[151] Turning to the application of the right to privacy online, the 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.[152] They have underlined, in this respect, that mass or indiscriminate surveillance may be deemed arbitrary[153] or even an inherently disproportionate interference with the right to privacy.[154]

Yet the discussion is in 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 ICCPR with regard to protecting privacy in the digital sphere,[155] or that the Human Rights Committee revisit General Comments 16 and 31.[156] Despite

149 UNGA Res 68/167 (n 7); UNGA Res 69/166 (n 7).

150 Human Rights Council Resolution (n 7) [1] [5].

151 '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.

152 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.

153 UN Report on the Right to Privacy (n 3) [25]; 2013 UN Report on Freedom of Expression (n 141) [81]-[83].

154 '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.

155 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-

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 section argues that not only does the standardisation 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.[157] 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 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-makers mind-set 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 in the digital environment.

Privacy-Protection> accessed 1 May 2016; European Parliament Resolution on Surveillance (n 6) [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.

156 '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.

157 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 CoE Declaration on Internet Governance Principles (n 44) are the only bodies discussing this issue. The UN Special Rapporteur on Freedom of Expression (n 5 [30]) and the Human Rights Council in its 2014 Resolution (n 7, 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 3) the Human Rights Council in its 2012 Resolution (n 7) and the UN General Assembly in its Resolution on the Right to Privacy in the Digital Age (n 7) do not make any reference to the special features of the Internet. David Kaye and his Report on the use of encryption is a bright exception.

4.1 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.[158] 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.[159]

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 trans-border data flows. In addition, a rigorous understanding of the value of privacy and trust from the technical point of view updates our understanding 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 international security as well as safeguarding

158 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.

159 See, for example, Russian Federal Law No. 242-FZ 2014 which entered into force on the 1st September 2015 and establishes the requirement to localise personal data held on Russian citizens in Russia. The German Parliament approved on 16th of 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 & 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, Uyên P. Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677-739; Alexander Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?' (2016) 32 CLSR 128-145; Francis Augusto Medeiros, Lee A Bygrave, 'Brazil's Marco Civil da Internet: Does It Live up to the Hype?' (2015) 31 CLSR 120-130.

freedom of expression.[160] 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.[161]

International and domestic bodies and courts should explore how this perspective informs legal reasoning in two respects. First, 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 toward 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).[162] 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 technical developments.[163]

Second, domestic and international courts need to acknowledge and "translate" in legal and human rights law terms the symbiotic relationship between security, on the one hand, and privacy and freedom of expression on the other hand. Privacy and security can be mutually supportive goals and, therefore, courts need to appreciate their interrelation in a non-conflictual fashion.[164] Security measures that aim to strengthen the protection of privacy should be carefully assessed. Weakening encryption, for example, will have serious ramifications not only to undermining the effective exercise of the right to privacy and freedom of expression[165] but also to compromising

---

160 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.

161 UN Report on the Right to Privacy (n 3) [24]-[25].

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

163 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.

164 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.

165 UN Report on the use of encryption and anonymity in digital communications (n 135); 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_promoti

national and international security.[166] In this regard, the courts' role will be instrumental in articulating and, if necessary, balancing the respective interests in ad hoc cases as well as pronouncing on the compatibility of recently introduced pieces of legislation regulating or banning encryption and/or anonymity (discussed earlier) or implementing domestic surveillance programs. For instance, although the French Constitutional Court validated a recent domestic law implementing a surveillance program, thirteen complaints are currently pending before the ECtHR against this decision.[167] Conversely, the English High court issued a landmark judgment in *David & Ors v. Secretary of State for the Home Department* declaring the 2014 Data Retention and Investigatory Powers Act to be unlawful.[168] The views of data protection authorities will also be informative judging from the strong stance of Hamburg's data protection watchdog on preserving anonymity and the right to use pseudonyms online.[169]

4.2 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.[170] 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,[171] fifteen States supported the amendment, which makes it clear that there is no

---

on_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf> accessed 1 May 2016.

166 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; Susan Landau, Individual Statement, Berkman Centre for Internet & Society, 'Don't Panic. Making Progress on the "Going Dark" Debate', 1 February 2016.

167 The French Constitutional Court validated the recent Law 912/2015 (24 July 2015) implementing a surveillance program <https://www.lexology.com/library/detail.aspx?g=2c230c55-43c6-4452-ad04-d6be99e15a2f> accessed 1 May 2016.

168 *David & Ors v Secretary of State for the Home Department* [2015] EWHC 2092.

169 <http://arstechnica.co.uk/tech-policy/2016/03/pseudonym-ruling-facebook-claims-real-name-policy-protects-users/> accessed 1 May 2016.

170 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.

171 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,

global consensus on Internet-related or privacy-related issues.[172] 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 may undermine the interoperability of the Internet.[173]

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 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.[174] Such a strategy can be persuasive when addressing policy-makers from specific regions of the world as well as when motivating all law-makers to enhance legal and technical privacy safeguards.[175] 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.[176] There is, however, merit in arguing that the technical approach to privacy deprives the discussion of its socio-political dimensions.[177] It cannot go unnoticed that the human rights approach to cyberspace does not only refer to strictly speaking the applicability and

South Africa, UAE, Venezuela, Vietnam. Four States abstained (Gabon, India, Indonesia and the Philippines).

172 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 7) 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.

173 '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.

174 IAB Statement on Internet Confidentiality (n 77).

175 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.

176 2013 Resolution (n 155); 'Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party', 25 November 2014, points 1 & 4 <http://europeandatagovernance-forum.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.

177 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.

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 prioritising 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.[178] 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".[179] ISOC also employed human rights language and discourse by welcoming the "formal endorsement of a rights-based approach for the Internet".[180] 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.

4.3 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.[181] 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 articulated as legal arguments raised before

178 NETmundial Statement (n 8) 7.

179 CoE Declaration on Internet Governance Principles (n 144) [5] (emphases added).

180 '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).

181 UN Report on the Right to Privacy (n 3) [31]-[36] [47]; 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 [62]; UNGA Res 69/166 (n 7). 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.

courts and other bodies, and 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 mind-set; 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" '.[182]

Access Now and the 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 FBI's request.[183] These arguments have become legally relevant because we are now exploring and conceptualising the legal implications of the nature of the Internet. The arguments underline the global implications of acts or omissions of state authorities even if they 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. Despite this, there are instances in which courts do not seem to properly apply basic concepts of international human rights law regarding the exercise of jurisdiction by a State let alone read the concept of jurisdiction under the technical perspective. In the Human Rights Watch *Inc & Ors* case the UK Investigatory Powers Tribunal curiously dismissed the claim that the United Kingdom could have the obligation to respect the right to privacy of an individual outside the country.[184]

---

182 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).

183 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.

184 *Human Rights Watch Inc & Ors v The Secretary for the Foreign & Commonwealth Office & Ors* [2016] UKIPTrib 15_165-CH, [58].

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.[185] 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.[186] Such a practice not only subverts legal safeguards of privacy in 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.[187] Similar suggestions for government hacking are being explored in the United Kingdom[188] and the Netherlands.[189] 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).[190] 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

185 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 favor by simple majority, the revisions will become law that same day.

186 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.

187 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.

188 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.

189 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.

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

international and national standards of online privacy. The use of means of transnational cooperation, such as Mutual Legal Assistance Treaties, is a preferable way of thinking the way forward in such instances.

5. Conclusions

The legal nature and effects of informal law-making are context-specific and should be assessed on a case-by-case basis, given the plurality of informal norms that may be taken into consideration. There is no doubt that Internet standards, set by the IETF and IAB, are not legally binding, nor do they have the potential to evolve into something binding. Internet standards, nonetheless, frame, and to a great extent shape, the user's choices online and therefore constitute a powerful regulatory force.

Even though the Internet standards-setting process does not observe traditional law-making formalities, there is strong evidence to suggest that the IETF meets high standards of transparency, inclusiveness and legitimacy. There is, however, scope for engaging a broader spectrum of stakeholders in the standardisation process, and for promoting greater diversity within the IETF community. Of particular interest for the present discussion was the question of whether the bodies' technical mandate allows broader societal interests to be taken into consideration. The analysis found that the standard-setting process is open to external considerations insofar as the impact of the IETF's work on the Internet community and its contribution to the evolution of the Internet is concerned. Societal and broader interests, other values or public interest considerations are not examined in themselves; what is examined is how Internet standards affect different communities and stakeholders with regard to such broader interests and concerns. The IETF needs to navigate through the "tussles" and constructively accommodate the - possibly competing - interests of different stakeholders and sub communities within the Internet community.

Building upon these findings, the discussion turned to examine 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 become a guardian of privacy online, and to integrate Privacy by Design into the core Internet architecture as a requirement when creating and updating

standards. This has a series of implications for the IETF's design philosophy, its organisational structure and the level of privacy protection contained within technology and afforded to global end users. 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 mass surveillance. Moreover, Internet standards operationalize a given level of privacy protection. 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.

Crucially, the technical community's approach to privacy 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. For instance, the distinctive interconnection between privacy and freedom of information/expression online, or the relevance of the users' location and nationality, are issues that we need to reconsider in legal reasoning and in balancing the relevant interests.