Engineering ‘Privacy by Design’ in the Internet Protocols:
Understanding Online Privacy both as a Technical and a Human Rights Issue in the Face of Pervasive Monitoring

Adamantia Rachovitsa*

Keywords: Technical standards; Internet standards; Internet protocols; privacy; privacy by design; human rights; international informal law-making; pervasive monitoring

A. Introduction

The Internet - like no other means of communication in the past - has allowed instant communication and at a low cost creating unprecedented opportunities for the exchange of ideas and information on a global level. It provides a platform for the realization of human rights and it is also a driving force in the acceleration of progress and international development. At the same time, however, information and communications technology and the Internet provide the technical capability for the capture, storage, administration and analysis of enormous quantities of data and information.¹ The right to privacy may be seriously and extensively threatened online without the awareness of its users. Tracking is passive and invisible to the users and it has become relatively easy for states, business actors and individuals to interfere with the privacy of communications. Recent revelations that states conduct, and that the private sector facilitates, extraterritorial surveillance, interception of digital communications and collection and retention of data give rise to alarming concerns.² The United Nations High Commissioner for Human Rights (OHCHR) warns that “governmental mass surveillance emerges as a dangerous habit rather than an

* Assistant Professor of International Law, College of Law, Qatar University; Founder and Secretary of the Qatari Branch of the International Law Association; Ph.D. (Nottingham).
exceptional measure”. Moreover, the exercise of the right to privacy is a prerequisite for realizing other human rights - online and offline. Respect for online privacy enables the exercise of the freedom of expression, freedom of assembly and of association. Conversely, threats to, and violations of, privacy pave the way to censorship or self-censorship and could have chilling effects on freedom of expression, media freedom. The effects of pervasive monitoring cannot be duly appreciated unless one underlines 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.

Despite the serious interests at stake, we are far from fully comprehending the ramifications of the violation and abuse of privacy by means of pervasive monitoring. Affirming that human rights apply equally offline and online is an invaluable and timely pronouncement, but it does not consider the Internet’s special features and, hence, it does not address the fact that privacy is exercised and challenged in different ways in the digital environment compared to the ‘offline’ environment. Notably, there is little, if any, communication between the technical and non-technical epistemic communities. Lawyers and policy makers, in particular, lack a basic

---

3 Id., ¶ 3.
4 Id., ¶ 14.
6 Pervasive monitoring is defined as “widespread (and often covert) surveillance through intrusive gathering of protocols artefacts, including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g. correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. Pervasive monitoring is distinguished by being indiscriminate and very large scale rather than by introducing new types of technical compromise.” in S. Farrell, H. Tschofenig, (May 2014), Pervasive Monitoring Is an Attack, RFC 7258, Best Current Practice 188, at 2, available at http://www.rfc-editor.org/rfc/rfc7258.txt [hereinafter Pervasive Monitoring is an Attack]. ‘Pervasive monitoring’ and ‘surveillance’ will be used interchangeable for the purposes of the article.
9 Examples include whether metadata fall within the protective scope of privacy, what constitutes an interference with privacy and how we conceptualize privacy threats and privacy harms in the online environment. See UN Report on the Right to Privacy, supra note 2, ¶¶ 17-20.

The purpose of this article is to fill in this gap of communication between, on the one hand, the technical community and, on the other hand, the legal and policy-making community. Policy and technology must be designed with a solid understanding of the implications of each other. The article underscores the reasons that policy-makers and lawyers must value the significance of protecting privacy not only as a human rights issue, but also as a fundamental technical property for the well functioning of the Internet.

The article argues that the effective protection of online privacy cannot be thought of only in terms of compliance with legal frameworks but that – in practice - it also needs to be secured through technological means, such as privacy enhancing technologies and, most importantly, privacy by design.\footnote{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, 19-24 (2011), available at \url{http://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf}. Privacy by design is different from privacy enhancing technologies in that the former is a general requirement of the core architecture of a system or product, whereas the latter are employed to strengthen privacy-related components of the system, as a second stage, when the architecture is already implemented.} The article addresses how privacy is hardwired into the core Internet protocols\footnote{For the definition of the core Internet protocols see discussion \textit{infra} Part B.I.} that form the Internet’s basic architecture,\footnote{To computer scientists ‘architecture’ means the attributes of as system as seen by a programmer which includes the conceptual structure and functional behavior, as distinct from the organization of the data flow and controls, the logical design and the physical implementation. The article follows Lessig’s approach to employ ‘architecture’ more generally to refer to both the Internet’s technical protocols and its entrenched structures of governance and social patterns. See LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS ON A CONNECTED WORLD 36 (2001). The terms ‘design’ and ‘architecture’ are used interchangeably herein.} by introducing the important, albeit largely neglected, privacy-related work of the Internet’s technical standardization bodies. It shows that the Internet is regulated and managed by technical standards, the Internet standards, which are developed by private bodies. The Internet Advisory Board (IAB) and the Internet Engineering Task Force (IETF) are the most prominent and influential standardization bodies in the area. Despite an emerging interest in the informal law-making functions
of standardization bodies, the work of the IETF and IAB has escaped the attention of international lawyers. The design of the network and the Internet protocols (as developed via the technical standards) by default encapsulate regulation and, therefore, de facto prescribe a certain level of protection for Internet users. Further, the analysis looks at recent developments in the standardization work of the IETF and IAB and provides evidence of a paradigm shift with respect to integrating ‘privacy by design’ requirements in the Internet protocols, which will have an immense impact on the privacy of global users. Lastly, the article establishes a convergence zone between the ‘privacy as a technical issue’ paradigm and ‘privacy as a human rights issue’ paradigm. It is submitted that an interdisciplinary exercise of reading them together paves the way for effectively protecting online privacy and preserving the integrity of the Internet.

The article proceeds in three Parts. Part B explains why the Internet protocols are important in the architecture of the Internet and it examines the legal value of the Internet standards from an international informal law-making point of view. The analysis finds that both the standardization bodies and the technical standards enjoy great legitimacy despite their informal nature. Part C turns to specifically address the development of technical standards relating to online privacy. The protection of the users’ privacy has recently become a high priority in the work of the IETF and IAB in the face of pervasive monitoring by state and non-state actors. The article submits that the Internet’s standardization bodies have the authority and the responsibility to defend the Internet from a users’ trust breakdown and, hence, to protect privacy as a necessary prerequisite for the proper functioning of the Internet. The work in progress of the bodies evidences that they decided to defend the Internet by adopting a technical solution for the effective protection of online privacy. Their decision to embed privacy by design in the Internet protocols includes the creation of a privacy threat model, the introduction of encryption in the Internet traffic and the

---

E.g., INFORMAL INTERNATIONAL LAWMAKING (Joost Pauwelyn, Ramses Wessel, Jan Wouters eds., 2012); Sandeijn Duquet et al., Upholding the Rule of Law in Informal International Lawmaking Processes 6 HAGUE JOURNAL ON THE RULE OF LAW 75 (2014).

This is not the first time that novel international bodies appear, at first, insignificant or irrelevant in the eyes of international lawyers. See Anne Peters & Simone Peter, International Organizations: Between Technocracy and Democracy, in THE OXFORD HANDBOOK OF THE HISTORY OF INTERNATIONAL LAW 170, 174-175 (Bardo Fassbender et al. eds., 2012) discussing that international law scholarship ignored, at first, the legal significance of the creation of the 19th century international unions.

The Internet is composed of a great number of networks. ‘Internet’ and ‘network’ will be used interchangeably herein.
empowerment of the end-user to make privacy design choices. The analysis also demonstrates how the privacy by design technical standard is being informed by and, in turn, shapes and nurtures legal standards, business practices and regulation. Part D makes an interdisciplinary account of the contours of the technical solution paradigm and the human rights paradigm in the area of online privacy. It explores the double function of privacy as a technical issue and as a human right by pointing out the confines of both perspectives and by showing how the technical analysis may and reinforce the human rights analysis’ arguments concerning the protection of privacy.

B. Informal Law-making by the Internet Standardization Bodies

The governance of the Internet is highly fragmented in terms of the distribution of authority, which reflects the decentralized nature of the network itself. The evolution and use of the Internet is 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 in varying degrees to formal and informal governance arrangements.17

Despite this fragmentation and lack of formal authority, a limited de facto hierarchy exists in the day-to-day management of the Internet.18 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’19 and its mission is to identify and suggest solutions for technical problems and to develop Internet protocols. The IAB, in turn, is responsible for reviewing the overall technical and engineering development of the Internet and engages with

---

17 NETmundial Statement, supra note 10, at 6; World Summit on the Information Society, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005, ¶ 34 [hereinafter Tunis Agenda]; Lee-Andrew Bygrave & Terje Michelsen, Governors of the Internet, in INTERNET GOVERNANCE 92 (Lee-Andrew Bygrave & Jon Bing eds., 2009).
creating Internet protocols to protect the users’ privacy. These two bodies are the most important global standard setters in the field and, hence, their work merits careful study.

This Part explains what the Internet protocols are from an engineering point of view and why they are critical to the Internet’s architecture. It proceeds to address the protocols’ legal value as informal law-making and it analyses the standard-setting process that the IETF follows. The discussion aims to introduce the work of the standardization bodies and establish the international legitimacy that they enjoy, before Part C assesses their substantive contribution to the area of online privacy.

I. The Function of the Internet Protocols and their Normative Value

Internet protocols form the foundations upon which the Internet, as we know it, is built. Once protocol designers (IETF) specify a protocol it then becomes an Internet standard and programmers can utilize it when building programs. Protocols are not software in themselves – they are standards that can be implemented in software giving rise to many applications.

Lawrence Lessig provides an illustrative account of the role of the protocols. The transfer of data via the Internet can be depicted in four layers: there is the data link layer, the network, the transport, and the applications’ layer. The Internet is constructed by a set of basic protocols together referred to as TCP/IP (Transmission Control Protocol/Internet Protocol). The TCP/IP protocols facilitate the transfer of the data through the different layers of the network. Three of these layers - data link, network and transport layers – qualify as the core of the internet, even if they are invisible to the eye of the average internet user. The data link layer handles local network interactions and few protocols operate therein. More protocols exist at the network layer where the IP protocol is dominant. It routes data between hosts and across network links. At the transport layer the TCP protocol negotiates the flow of data between two network hosts. On top of these three layers is the applications layer.

---

22 LAWRENCE LESSIG, CODE 2.0 145 (2006).
23 Id., at 143-145.
of the Internet. The application layer is the most familiar to the users – it consists of many protocols and their respective implementations via software, including network application protocols, such as the FTP (File Transfer Protocol), HTTP (HyperText Transfer Protocol) and HTML (HyperText Markup Language).

Internet protocols are important for two main reasons. First, they constitute the backbone of the Internet as the basis upon which all the layers of the network are created. As such, they define - to a significant extent - what the Internet is and how it functions. Due to their position at the low level of the Internet’s layered architecture, they advance a great impact through the whole network.24 This impact via the technical infrastructure has serious regulatory and legal implications. Internet protocols, by way of defining the architecture of the Internet, form regulation by default.25 The core architecture of the Internet is one of the strongest modes of regulation since technological capabilities and design choices impose rules on the online user regarding the access and use of information. The system’s configurations shape and limit the user’s preferences and choices. In other words, Internet protocols are a ‘hidden’ but powerful regulatory force complementing the law, the markets and various social norms developed online.26

A lawyer may perhaps struggle to identify the normative value of these protocols. The Internet protocols are engineered on the basis of technical standards, known as Internet standards, developed by the IETF and the IAB.27 The Internet was created and is evolving by voluntary adherence to these standards: industry, organizations, Internet users and states adhere to the non-binding technical standards

---

24 When Lessig discusses the regulation by code, he refers to protocols and software by way of excluding the TCP/IP and including code complementing or closely connected to the TCP/IP. The present discussion includes the TCP/IP and other Internet protocols in the data, network and transport layers of the network (but not software). See Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology* 76 Texas Law Review 553, 582 (1998).


26 Lessig highlights these four regulatory forces in the Internet in Lessig, supra note 22, at 223.

27 According to the IETF the Internet standard is “a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementation with substantial operational experience, enjoys significant public support and is recognizably useful in some or all parts of the Internet”, in S. Bradner, (October 1996), The Internet Standards Process – Revision 3, RFC 2026, Best Current Practice 9, at 2, available at ftp://www.ietf.org/rfc/rfc2026.txt [hereinafter The Internet Standards Process – Revision 3].
and, hence, 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”.  

Second, Internet protocols are important because they are open standards - namely a particular type of non-proprietary code. No one has monopoly on a protocol or its implementation, which encourages experimentation and innovation. Open standards encapsulate and reinforce the special features of the network insofar its open, decentralized and interoperable architecture. As it will be discussed in detail below, standards are developed in a collaborative fashion reflecting inclusive and participatory processes in a multi-stakeholder ecosystem. If it were not for the use of open standards, the interoperability of the network on a global scale would not have been feasible.

II. The Internet Standard-setting Process

Many technical standards are developed by private standard-setting organizations. This is also the case with the Internet standards set by the IETF and IAB. Informal standard-setting does not observe formalities traditionally associated with the production of international law in terms of the processes followed, the actors involved and the final output. Despite this, informal law has a great impact and responds to specific needs of the international society: low cost, flexibility and expertise, for example. Recently, there has been a significant discussion in international law regarding the question of how informal law-making should be

---

28 Duquet et al., supra note 14, at 90.
29 Lessig, supra note 22, at 145; MILTON L. MUELLER, RULING THE ROOT 91 (2002).
30 NETmundial Statement, supra note 10, at 5, 7; Council of Europe, Declaration by the Committee of Ministers on Internet Governance Principles, 21 September 2011, ¶ 8 [hereinafter CoE Declaration on Internet Governance Principles].
31 Greenleaf, supra note 25, at 606.
33 Formal standard-setting organisations, including the International Telecommunications Union (ITU) and the International Standards Organisation (ISO), adopt formal international standards.
35 Joost Pauwelyn, Ramses Wessel, Jan Wouters, Informal International Lawmaking: An Assessment and Template to Keep it Both Effective and Accountable, in Pauwelyn, Wessel, Wouters, supra note 14, 503, at 503-509.
treated in and by international law and what challenges this informality poses to the legitimacy and accountability of such norms. By way of accepting the immense impact of informal norms in practice, suggestions have been made as to how the accountability of the bodies producing informal law should be enhanced without diminishing their effectiveness. The issue of accountability is mainly examined in terms of the legitimacy, transparency and inclusiveness of the informal law-making body.\(^{36}\) Pertinent criteria of assessment include: the institutional design of the organization (the organizational structure, the procedural rules followed and the inclusiveness of its membership), the implementation and application of the informal law, and any existing forms of oversight.\(^{37}\) The examination of the informal law-making process followed by the Internet’s standardization bodies strongly suggests that they observe a high standard of transparency and, thus, they are legitimate standard-setters in the area of online privacy.

More specifically, one cannot escape noticing at the outset that the establishment of the Internet’s standardization bodies is purely informal. The IETF emerged from a quasi-academic setting, which originates in the creation of the Internet. It was established as a body in 1986, although until the current day it is not an independent legal entity but is, rather, organized as an activity of the Internet Society (ISOC) - a US non-profit entity. The IAB, formed in 1992, is chartered both as a committee of the IETF and an advisory body of the ISOC.\(^{38}\) Informality extends to the internal structure of the two bodies coupled, nonetheless, with a high degree of transparency and inclusiveness. The IETF does not have an elected board. Participation is free and open to all interested individuals on a volunteer basis and anyone can attend its meetings (held three times per year) or be involved via its email lists. The participation, reflecting the multi-stakeholder model, includes protocol designers, software developers, industry representatives, government officials, civil society and legal/privacy experts. It should be highlighted that the public officials participate in the proceedings on an equal footing to other stakeholders.\(^{39}\) Moreover,

\(^{36}\) See, e.g., Duquet et al., supra note 14; Joost Pauwelyn, Ramses Wessel, Jan Wouters, Informal International Law as Presumptive Law, in INTERNATIONAL LAW-MAKING – ESSAYS IN HONOUR OF JAN KLABBERS 75 (Rain Liivoja & Jarna Petman eds., 2013).

\(^{37}\) Brad Biddle et al., The Expanding Role and Importance of Standards in the ICT Industry, 52 JURIMETRICS 177, 180-185 (2012); Dan L. Burk, Legal and Technical Standards in Digital Rights Management Technology 74 FORDHAM LAW REVIEW 537, 554 (2005).

\(^{38}\) Bygrave & Michaelsen, supra note 17, at 96-97.

\(^{39}\) This means that IETF and IAB do not exercise public authority as delimited by the ‘Informal Lawmaking Project’. It is not, therefore, clear why the IETF was included in their case studies. Cf.
the IETF is financially independent, funding its operations from conferences’ fees and the ISOC’s membership fees. The technical specifications (Internet standards) are freely available on the IETF website and all the stages of the informal law-making process can be easily traced. Hence, transparency is an organizing principle of the standard-making process.

In its day-to-day work, technical standards are developed by the IETF working groups, which are set up on an ad-hoc basis to address specific operational and technical problems. The groups publish technical standards and produce other deliverables, such as guidelines, or best current practices. The standard-setting process is stipulated in a detailed set of procedural rules including an appeal mechanism. Each new proposal for a specification undergoes a period of review and revision and is initially published as a ‘Request for Comment’ (RFC), reflecting the strong collaborative nature of the standards’ development. The proposed standard is a draft under discussion until (if) it reaches a certain level of maturity and turns into an Internet standard. There are no formal voting rules and new standards are approved by ‘rough consensus and running code’, which means that the value of the ideas is assessed by the empirical proof of their feasibility and the combined engineering judgment of the participants. Therefore, the process and the final


Harald Alvestrand & Hakon Wium Lie, Development of Core Internet Standards: the Work of the IETF and W3C, in Bygrave & Bing, supra note 17, 126, at 128, 135.

The Best Current Practice (BCP) is a subseries of the RFCs. BCP aims at defining and ratifying the IETF’s best current thinking on specific issues. BCPs may vary in style and content but are subject to the same consensus-building and review process as all proposed standards. See The Internet Standards Process – Revision 3, supra note 27, at 15-16.


Reducing the Standards Track to Two Maturity Levels, supra note 43, at 2.

Alvestrand & Wium Lie, supra note 40, at 132; Mueller, supra note 29, at 91. Interestingly, see how Berners-Lee, the inventor of the World Wide Web, describes his experience with engaging with the IETF in Berners-Lee, supra note 32, at 53-63.
outcome are supported by a strong and broad consensus, which is built and affirmed by the voluntary adherence of the Internet users and the industry to the standards.  

From a substantive point of view three requirements have to be met for an Internet standard to be adopted. First, the specification needs to be of the highest technical quality. Second, the draft standard must be supported by widespread community consensus. Third, an assessment of the interests of all affected parties as well as the specification’s contribution to the Internet takes place. The fact that the technical quality of the draft standard is not the only criterion for its adoption, is of great interest. The IETF values the general acceptance of the draft standard by the engineering community and the evaluation accommodates the interests of all affected parties, as well as the contribution to the Internet’s evolution. Thus, although the IETF is a technical body, it is mandated to appreciate and consider other values and interests when these fall within its scope. This way, specific societal interests and external concerns are raised and assessed within the remit of the bodies’ work, by way of strengthening their legitimacy.

Overall, the flexibility inherent in IETF and IAB processes is carefully balanced with robust procedural rules - similar to the procedural rules followed by formal standard-setting organizations. Transparency and inclusiveness seem to be not only formal procedural requirements but, in fact, an integral part of the bodies’ working principles and culture. They enjoy a great degree of independence. Although they are technical bodies, they are committed to consensus-making mechanisms and adhere to specific values. The maturity of an Internet draft to an Internet standard depends not only on the technical quality of the suggested standard but also on the interests of affected parties and its contribution to the network’s evolution amplifying its responsiveness to external and broader concerns. The legitimacy of the Internet standards stems from their clarity and functionality and is subsequently reinforced by the adherence of public and private actors to the voluntary standards. States and other stakeholders underlined in the Tunis Agenda the immense contribution of the

---

48 See Pauwelyn, Wessel, Wouters, supra note 35, at 521; Pauwelyn, supra note 34, at 18.
49 Biddle et al., supra note 37, at 180-185.
50 Coleman, supra note 32, at 179.
technical community to the shaping and evolution of the Internet, hence, acknowledging the legitimacy of the IETF and IAB to regulate the Internet.\textsuperscript{51}

\textbf{C. Developing Internet Standards to Secure Online Privacy}

Part B explained the role of the Internet protocols in the architecture of the network and highlighted the significance of the respective Internet standards in the de facto regulation of the Internet. It also established that the IETF’s standard-setting process aspires to introduce new, high standards of international legitimacy with regard to informal law making. Part C turns now to discuss how the IETF and IAB progressively develop the Internet standards in the area of online privacy. It argues, first, that the Internet’s standardization bodies have the authority - and, indeed, the responsibility - to safeguard privacy against pervasive monitoring. Second, it argues that there is a paradigm shift in the bodies’ standardization work with regard to integrating privacy by design technical requirements when setting Internet standards. This development will have a substantial impact on proactively protecting the Internet users’ privacy. The analysis situates the Internet standards within their institutional context and explores the reasons that the engineering community values the privacy of the Internet users.

The first section briefly highlights certain challenges relating to privacy in the online environment in order to stress the need for protective technological measures. The second section discusses the technical mandates of the standardization bodies in light of their readiness to protect privacy. The IETF and IAB decided to defend the network against pervasive monitoring and privacy threats. Pursuant to their mandates, however, privacy is valued not as a human right per se or a legal consideration, but as a condition for maintaining the users’ trust to the Internet. The third section demonstrates the shift in the bodies’ work in relation to the protection of online

\textsuperscript{51} Tunis Agenda, \textit{supra} note 17, ¶¶ 35 (e), 36.
privacy. It discusses aspects of the ongoing standardization process, which aims to offer a technical solution to privacy threats. The analysis also highlights how the technical bodies, on the one hand, inform their work by consulting legal standards and, on the other hand, contribute to legal and regulatory aspects of online privacy.

I. Understanding Online Privacy and the Need for Technology Driven Privacy Solutions

Technology brought new challenges regarding privacy - that are not encountered ‘offline’ - into fore. Online privacy concerns informational privacy, that is the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others. The digital environment exemplifies the fact that privacy is not about ‘being left alone’ or ‘hiding information’, but it refers to the right of the online users to have control over the collection, use and disclosure of their personally identifiable data.

The ease with which the identity of the online user can be compromised and exposed presents a significant difficulty. Preserving anonymity is a necessary, but not sufficient, condition for safeguarding online privacy. The protection of identifiability, meaning the possibility to be identified through correlation and

---

52 Cavoukian, supra note 11, at 6, 17; 2013 UN Report on Freedom of Expression, supra note 5, ¶¶ 22-23.
54 Identity, from a technical point of view, is defined as “any subset of an individual’s attributes, including names, that identifies the individual within a given context. Individuals usually have multiple identities for use in different contexts” in 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, ISSN: 2070-1721, at 9, available at https://tools.ietf.org/html/rfc6973 [hereinafter Privacy Considerations for Internet Protocols].
55 Anonymity, from a technical point of view, is defined as “a state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals”, id.
56 Identifiability, from a technical point of view, is defined as “a property in which an individual’s identity is capable of being known to an observer or attacker”, id.
fingerprinting, goes straight to the heart of the discussion. Applications and protocols share so many unique identifiers as part of their ordinary operation that it is increasingly easy to create unique device or application ‘fingerprints’. Re-identification of the same devices or applications over time exposes one’s privacy. Moreover, a specific feature of online privacy is that it is experienced contextually; in other words, it is subject to the said online environment and the individual circumstances of the user. In the digital environment the distinction between, on one hand, being in private (and not sharing data) and, being in public (and sharing data) is illusive. Rather, the aim is to create and promote privacy tools that enable users to give their informed consent and express their privacy preferences in order to customize their digital environment. Consequently, the default settings – from the design of the Internet protocols to a particular application or a browser - are instrumental as to whether and, if yes, to what extent users are empowered to intervene in the flow of their data.

For this reason, the Internet’s technical community, code writers and technology developers create and implement technology driven privacy solutions that can be incorporated into software and hardware products in order to preserve, to the extent possible, the un-detectability, un-linkability and un-identifiability of information and data. Examples of privacy enhancing technologies are: anonymizers, identity management systems, privacy proxies, encryption software and filters. In particular, the Internet’s engineers are developing privacy by design properties into the core Internet protocols. Incorporating privacy requirements into the fundamental architecture of the Internet is crucial since it facilitates the

---

57 Fingerprinting, from a technical point of view, is defined as “the process of an observer or attacker uniquely identifying (with a sufficiently high probability) a device or application instance based on multiple information elements communicated to the observer or attacker”, id., at 8.
60 Seda Gürses & Bettina Berendt, PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm, in DATA PROTECTION IN A PROFILED WORLD 301, 317 (Serge Gutwirth, Yves Poulelet, Paul De Hert eds., 2010).
61 Privacy Considerations for Internet Protocols, supra note 54, at 8.
63 See Métayer, supra note 62, at 325-326.
customization of the digital environment, it empowers the user and it preserves, to the extent possible, the un-identifiability of the information and data. The special features of the digital sphere call for technological measures in order to secure the privacy of the users. In this sense, embedding privacy by design in the Internet is a necessary technological complement to the law.\textsuperscript{64}

II. The Mandate of the Internet’s Engineers to Protect Online Privacy against Pervasive Monitoring

Even though privacy has always been a consideration in the work of the IETF and IAB, the recent disclosures on mass surveillance by states\textsuperscript{65} have forced the engineering community to face one of their major concerns - not to extend beyond their technical mandates or get involved in politics. When it comes to the issue of privacy they do not feel comfortable with turning into human rights developing bodies. This section suggests that, although these concerns are not without merit, the mandates of the Internet’s standardization bodies include and, in fact, dictate the protection of online privacy in order to restore and maintain the trust of the Internet users to the network.

First and foremost, no technical mandate exists in a vacuum or is neutral. Mandates are inevitably embedded within an overall socioeconomic framework fulfilling certain goals and serving specific needs.\textsuperscript{66} Since Internet protocols are a form of regulation by default, standardization bodies also make choices by default.\textsuperscript{67} Moreover, the IETF’s mission statement clearly reads that “the Internet isn’t value-free and neither is the IETF”.\textsuperscript{68} The IETF chooses to create certain technology by embracing specific technical concepts, including decentralized control, edge-user

\textsuperscript{64} Resolution on Privacy by Design, 32\textsuperscript{nd} International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, available at http://privacyconference2012.org/wps/wcm/connect/c6a587804adc37639aa9aa0feaa628d8/2010_J5.pdf?

\textsuperscript{65} UN Report on the Right to Privacy, supra note 2, ¶¶ 2-4.

\textsuperscript{66} Berners-Lee, supra note 32, at 125.


\textsuperscript{68} A Mission Statement for the IETF, supra note 19, at 3.
empowerment and sharing resources. The IAB, for its part, is entrusted with protecting the reliable operation of the Internet and the free flow of information, which is, in fact, a broadly defined responsibility. Consequently, debating the alleged neutrality of the technical bodies’ mandates is not particularly useful as a starting point.

Second, as the function and scope of the Internet evolves, so too the role of the expert bodies entrusted with a public policy role in the Internet governance. Protocols’ designers are more than familiar with the evolving function of the Internet. According to them, the only principle of the Internet that would survive indefinitely is the principle of constant change: the architectural principle of the Internet aims at providing a set of rules (protocols) that generates a continuously evolving space of technology.

This is clear in how the Internet is envisioned and how the Internet standards develop. Therefore, although these bodies are bound by their technical mandates, the mandates have to be read in the light of the needs of the users in the name of whom they act. The protection of the users’ privacy is a serious and legitimate concern to be considered when designing and updating protocols. As discussed earlier, the affected parties’ interests and the possible contribution to the Internet’s evolution are requirements to be appreciated in the standardization process.

Even though anticipating privacy threats is limited (since Internet protocols are deployed within larger systems and are not always used in ways envisioned at the time of design), the choices in the design of the Internet protocols have profound implications on identifying and mitigating privacy threats.

The IETF and IAB have accepted that their mandates cover privacy issues by recently acknowledging that serious and systematic violations of the users’ privacy pose significant risks to the reliable operation of the Internet. The IETF Chair

---

72 The Internet Standards Process – Revision 3, supra note 27, at 3.
74 Privacy Considerations for Internet Protocols, supra note 54, at 5-6.
proclaimed that pervasive monitoring is a threat against which the Internet’s engineers should defend. Many strong voices from within the technical community take the position that engineers should re-consider the impact of protocol and system design choices in light of the serious interests involved in the protection of privacy. In 2014, the IETF asserted its strong consensus in stating that “[pervasive monitoring] is an attack on the privacy of Internet users and organizations”.

Nonetheless, one should not lose sight from the fact that the IETF does not discuss privacy as a human rights issue, but rather addresses privacy as a technical issue relating to the function of the network. Due to the unique features of the Internet’s architecture, the relevant threats to the users’ privacy equally qualify as threats to the fundamental value of the network – that is trust among the users. The core architecture of the network is its end-to-end design: the Internet is designed to connect the end-points and, consequently, the intelligence of the system is not centralized but lies in the end-users. This design, however, is based upon the presumption of trust among the users. Privacy threats and risks, and especially pervasive monitoring, directly impact the level of trust placed by the users to the network: compromising the users privacy undermines the network because the network is its end-users. In this way, the users’ participation in the network is adversely affected, the free flow of information is inhibited and the integrity and confidentiality of information are endangered. According to the engineering community’s mind-set, pervasive monitoring is an attack because threats to the user privacy undermine the reliable operation and the responsible use of the network as a whole. Hence, the IETF statement on pervasive monitoring being an attack on the network is a statement of values strongly underlying and pertaining the reliable

---

78 Pervasive Monitoring is an Attack, supra note 6, at 2 (emphases added).
80 Otherwise described as the principle of simplicity. See Architectural Principles of the Internet, supra note 71, at 1 and R. Bush, D. Meyer, (December 2002), Some Internet Architectural Guidelines and Philosophy, RFC 3439, Informational, at 3, available at https://www.ietf.org/rfc/rfc3439.txt. It was thought that network operation will be more efficient if specific applications for computing or data processing are located at the end points of the network rather than in its communications protocols. See Dan L. Burk, Federalism in Cyberspace Revisited, in Thierer & Wayne Crews eds., supra note 25, 119, at 127.
functioning of the Internet as a network.\textsuperscript{81}

To summarize, the IETF and IAB have recently decided that they have the authority to protect the Internet users from pervasive monitoring, including governmental surveillance. The engineering community’s decision is based on the fact that pervasive monitoring is perceived as an attack to the trust to the network – a fundamental value for the proper functioning of the Internet. The next section turns to demonstrate how the standardization bodies introduce privacy by design when developing (or updating existing) Internet standards,\textsuperscript{82} thereby adopting a technical solution to mitigate serious threats to online privacy.

III. The Technical Solution: Introducing Privacy by Design Requirements in the Internet Standards

This subsection discusses the decision of the Internet’s standardization bodies to integrate privacy by design requirements in the Internet protocols. This decision cannot be properly appreciated unless first it is explained in what way it transforms the so far prevalent architectural paradigm. The changes underway are not merely a peripheral issue in the development of Internet standards: they radically update the work of the bodies, enrich the working culture of the Internet’s engineers and evidence a holistic reassessment of the network’s properties. The standardization work in progress is worth of careful examination not only on the merits of the introduction of privacy by design considerations in the Internet standards; this work further reinforces the arguments made in this article on the legitimacy of these bodies and the intrinsic value of online privacy to the reliable operation of the Internet.

1. Pervasive Monitoring as a Trust Breakdown

Privacy has always been a consideration in the Internet’s design. The very first Internet protocols discussed privacy, albeit mostly in the context of network security. Although network security properties (confidentiality, data integrity and

\textsuperscript{81} Denardis, supra note 69, at 86.

\textsuperscript{82} Privacy Considerations for Internet Protocols, supra note 54; Ethics and the Internet, supra note 70, at 1-2.
authentication) secure the privacy of the users, security is an essential but not a sufficient condition for mitigating all privacy threats. For this reason privacy threats’ mitigation gradually became an autonomous concept when designing and updating Internet standards. Notwithstanding (or due to) the increasing relevance of privacy in the development of the Internet standards, a paradigm shift in the standardization work of the IETF and IAB recently took place. This shift occurred in 2014 when the IETF declared pervasive monitoring an attack on the privacy of Internet users and the network. In response to this attack the technical bodies decided to evolve their work by way of integrating privacy as a design requirement into the Internet standards.

It was earlier explained that the IETF considers pervasive monitoring an attack to the network because it compromises the users’ trust to the network and it undermines its end-to-end design. The end-to-end design encapsulates the (implicit) choice made in the early development of the Internet to leave security and privacy issues to be addressed by the end-users (end-points) in order to keep the core communication Internet protocols as simple as possible. It is for this reason that the Internet’s engineers deemed that privacy was not a requirement when designing Internet but it should rather be secured by the end-users. This essential design principle, however, rests upon the working presumption that the Internet was originally built by a community of like-minded professionals who trusted each other. This presumption is not valid anymore due to the increasing lack of trust among the end-users. Hence, the application of the end-to-end principle and the limited relevance of privacy to engineering the Internet protocols have been regularly come into question from various directions. For example, for some time now, there existed concerns with regard to the question of whether and, if yes, how commercial services in the network may compromise privacy, security, and data integrity.

Equally concerning is the growth in users who are either not technologically

---

84 For the concept of “paradigm shift” see THOMAS S. KHUN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1996).
86 Architectural Principles of the Internet, supra note 71, at 1, 2, 5.
88 Id., at 4-5.
sophisticated enough or simply uninterested in maintaining their own security and privacy.

Despite the various concerns, the revelations on pervasive monitoring set a new scene. The pervasive nature of monitoring by specific States in collaboration with non-State actors is a trust breakdown. The capabilities and activities of the attackers are greater and extremely more pervasive than in the past. Pervasive monitoring is distinguished from other threats to the users’ privacy by being indiscriminate and on a very large scale. The attacks are designed to indiscriminately gather as much data as possible and they are physically pervasive affecting a large number of Internet communications. They are also pervasive in content, consuming and exploiting any information revealed by the protocol and they are pervasive in technology exploiting vulnerabilities in many different Internet protocols. In light of these recent developments, and with the aim to restore the trust to the network, the IETF re-examines its choice to leave privacy and security issues almost exclusively to the end-users. In this sense, the integration of privacy requirements in the Internet standards signifies a rearrangement of its standardization work in order to consider privacy prior to designing new protocols and when updating existing protocols.

2. Developing a Privacy Threat Model concerning Pervasive Monitoring

In 2012 the IAB issued a Report from the Internet Privacy Workshop identifying a number of steps that should be taken in order to understand how to systematically address privacy within the Internet standards’ development. The IAB emphasizes the need for privacy-related design choices and the integration of privacy requirements into the design of the Internet’s core protocols. This is the first time that the standardization bodies urge for the design of a privacy threat model with a focus on pervasive monitoring.

---


90 Pervasive Monitoring is an Attack, supra note 6, at 2.

91 The Rise of the Middle and the Future of the End-to-End, supra note 87, at 5, 8. See also Clark, Sollins, Wroclawski, Braden, supra note 67; New Security and Privacy Program established by the IAB in May 2014, available at https://www.iab.org/activities/programs/privacy-and-security-program/.

92 Report from the Internet Privacy Workshop, supra note 59, at 4-5 and 6-9 respectively.
The IAB outlines an action plan and sets a series of priorities. The first priority is to document and understand practices that pose a risk to privacy. A threat model is being developed describing how pervasive attacks take place and how they can be mitigated on a technical level.93 Further, the IAB established a privacy directorate to review the IETF’s standard-setting process and oversee the privacy aspects of the draft standards.94 The creation of the directorate indicates that the protection of privacy becomes an integral part of, and updates the institutional design of, these bodies.

One of the most notable contributions of the model is a set of guidelines addressed to the Internet engineers on how to embed privacy protection in protocol design.95 The model engages with the definition of privacy threats and establishes privacy terminology.96 The development of a privacy vocabulary serves a twofold aim. The first aim is to introduce privacy-related concepts to the engineering community. Protocol designers need to be aware of specific engineering choices that can impact privacy when setting Internet standards. In the same vein that the legal community is struggling to comprehend the technical aspects of privacy, the technical community is putting a serious effort to identify and understand the value of privacy as a pertinent consideration to their work.97 The second aim of creating a privacy vocabulary is to employ privacy threats’ terminology that is accessible and comprehensible to people outside the technical community, including business actors and end-users. Raising awareness about what the Internet users must do and not do is a clear priority.98

Interestingly, the IETF’s work demonstrates how the technical community uses legal standards to inform its own guidelines and, at the same time, makes a contribution valuable to the legal community insofar the conceptualization of online

---

94 Report from the Internet Privacy Workshop, supra note 59, at 14.
95 Privacy Considerations for Internet Protocols, supra note 54, at 4.
96 Report from the Internet Privacy Workshop, supra note 59, at 14.
privacy is concerned. The IETF documents not only the technical means employed to conduct pervasive monitoring, but also draws upon existing legal and policy privacy frameworks, such as the Fair Information Practices, the OECD guidelines concerning the collection and use of personal data and the Privacy by Design concept. Notwithstanding that the guidance to the Internet’s engineers is not constrained by national or international legal frameworks (since it informs the design of the core architecture of the Internet anywhere in the world) legal references are still substantially informative.

Conversely, the discussion on privacy harms adds value to the legal aspects of the right to privacy online. The IEFT, in order to effectively address privacy risks, elaborates on the different ways that the end-users feel threatened or are harmed, including harms to financial standing, reputation, autonomy, and safety. The different types of privacy harms are also discussed in length by referencing views of legal experts and texts by the Council of Europe. 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”. It is further emphasized that “the 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”. The impact of surveillance on the autonomy and behavior of the users is a crucial consideration from a technical point of view in assessing the decrease of trust placed to the network. From a legal standpoint, substantiating the nexus between surveillance and personal autonomy could prove to be an interesting consideration with regard to the definition of privacy harm in the digital environment.

---


100 Privacy Considerations for Internet Protocols, supra note 54, at 4, 18.

101 Id., at 4.

102 Id., at 12.

103 Id.

104 Id., at 13 (emphases added).

105 For the question of whether a specific type of privacy harm is needed to ascertain a privacy breach see Lessig, supra note 22, at 213.
3. Mitigating Privacy Threats

It needs to be clarified at the outset that the term *mitigation* does not imply that the technical community has the ability to completely prevent an attack. Internet protocols that will be designed to mitigate pervasive monitoring will not prevent an attack but they can significantly alter the threat (significantly increase the cost of attacking, force what was covert to be overt, or make the attack more likely to be detected).\(^{106}\)

Another preliminary note concerns the question of whether the IETF makes any special mention to pervasive monitoring by states. From a technical point of view, the motivation for conducting pervasive monitoring is irrelevant for the purpose of mitigating privacy threats. Hence, it is indifferent whether the actor conducting monitoring is a state, a criminal organization or a commercial entity.\(^{107}\) The IETF notes, however, the role of states because they are one of the few actors, which have the necessary resources to conduct monitoring on a large and pervasive scale.\(^{108}\) Other than that, the IETF works to mitigate the technical aspects of surveillance, as they do for any protocol vulnerabilities.\(^{109}\) Therefore, mitigating privacy threats on a technical level acquires a far broader scope comparing to the human rights perspective of the right to privacy, which is typically limited to the State-individual relationship.

The Internet engineering community is currently focusing on three broad areas to mitigate privacy threats: 1) data minimization; 2) user participation; and 3) security.\(^{110}\) The discussion that follows provides certain selective insights from the areas of security and user participation.\(^{111}\)

a) Security

The Internet’s engineers classify online surveillance as a combined security

\(^{106}\) Pervasive Monitoring is an Attack, *supra* note 6, at 3.
\(^{107}\) *Id.*, at 2.
\(^{109}\) Pervasive Monitoring is an Attack, *supra* note 6, at 3.
\(^{110}\) These three areas can loosely be 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, *supra* note 54, at 18; Sprint Workshop Report, *supra* note 98, at 21.
\(^{111}\) Many other examples can be given from the recent IETF’s work. On the issue of incorporating privacy into the IPv6 address design see Denardis, *supra* note 69, at 77-88.
and privacy threat.\textsuperscript{112} This signifies the strict interconnection between security and privacy,\textsuperscript{113} but it also points out to the need for a tailored approach addressing specific aspects pertaining to pervasive monitoring, such as the confidentiality of protocol metadata, countering traffic analysis, or data minimization.\textsuperscript{114} Although security and privacy were always distinct concepts,\textsuperscript{115} the IETF felt that it is now necessary to outline, for the first time, a comprehensive framework for establishing privacy guidelines to Internet engineers. In this respect, security mechanisms are important in preserving and safeguarding the users’ online privacy.

A significant thread in the IETF’s work at the moment is the introduction of encryption into the Internet protocols. In November 2014, the IAB issued a Statement on Internet Confidentiality in which it reinstated that the growth of the Internet depends on the users having confidence that the network will protect their private information.\textsuperscript{116} The IAB underscored the importance for protocol designers, developers and operators to make encryption the norm for Internet traffic and it specifically urged protocol designers to design for confidential operation by default. The issue at stake is that protocol design is often predicated on the assumption that recipients, intermediaries, and enablers are authorized to receive and use data. This is not necessarily a correct presumption, since the end systems engaging in a protocol exchange may have been compromised. In the absence of authentication mechanisms, privacy analysis requires questioning this assumption.\textsuperscript{117} The ongoing standardization work on ‘opportunistic security’ concerns precisely the increase of encryption in the absence of authentication.\textsuperscript{118} Opportunistic security signifies a shift of perspective for the protocol designers. It means that, even if full end-to-end security is not possible,

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{112}Privacy Considerations for Internet Protocols, \textit{supra} note 54, at 13.
  \item \textsuperscript{113}The IAB created the Security and Privacy Program in May 2014 by way of merging two separate programs on security and privacy respectively.
  \item \textsuperscript{114}Pervasive Monitoring is an Attack, \textit{supra} note 6, at 3; Privacy Considerations for Internet Protocols, \textit{supra} note 54, at 13.
  \item \textsuperscript{115}For example, the IETF distinguishes between a data confidentiality service, which is a security service to protect data against unauthorized disclosure to unauthorized individuals or processes, from privacy. In other words, confidentiality is only one of the security mechanisms to support the protection of privacy. See Strong Security Requirements, \textit{supra} note 99, at 2.
  \item \textsuperscript{116}IAB Statement on Internet Confidentiality, \textit{supra} note 89.
  \item \textsuperscript{117}Privacy Considerations for Internet Protocols, \textit{supra} note 54, at 10.
  \item \textsuperscript{118}V. Dukhovni, (December 2014), Opportunistic Security: Some Protection Most of the Time, RFC 7435, Informational, ISSN: 2070-1721, at 3, available at \url{http://www.rfc-editor.org/rfc/rfc7435.txt}.
\end{itemize}
\end{footnotesize}
then some security is better than none.\textsuperscript{119} In particular, the Internet-draft on the effect of ubiquitous encryption examines ways to introduce encryption in Internet traffic.\textsuperscript{120}

A few new Working Groups have been created in the IETF to explore how security mechanisms should be reinforced to address specific aspects of pervasive monitoring. The focus lays 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 in 2014\textsuperscript{121} to increase the security of transmissions over the Internet. In this instance, the underlying problem is that current transport Internet protocols include the addresses of the end-points exposing the metadata of these connections to all locations in the communications path. Improving e-mail privacy is one of the cornerstones of this standardization work. The Working Group has already produced the Request For Comment 7457\textsuperscript{122} and many Internet-drafts identifying existing best practices and helping application protocol developers to use TLS and unauthenticated encryption in future application definitions.\textsuperscript{123} Another example is the new Working Group on Domain Name System privacy considerations which has been set up to develop a private exchange mechanism so that DNS transactions and queries become more private.\textsuperscript{124}

b) User Participation


\textsuperscript{121} Available at https://datatracker.ietf.org/wg/uta/documents/.


As already mentioned, raising awareness among the end-users on privacy choices is a primary concern of the IETF and IAB. Location data is one the most, if not the most, critical metadata exposing many aspects of one’s privacy online. An example of how the standardization bodies promote and value user participation and empowerment is the work of the Geographical Location/Privacy Working Group (hereinafter Geopriv Working Group). The Geopriv working group has been created to design a protocol for privacy protection in location based services. Addressing the privacy of sensitive location information used by many emerging technologies has an immense impact. The group introduced a standardized privacy and security focused architecture for location-based services, such as navigation services, friend finders’ applications (Geopriv architecture). The Geopriv architecture aims to secure the integrity and confidentiality of location objects (users). Moreover, it aims at ensuring that the location information is transmitted in compliance with the user’s privacy preferences. This means that location information should always be bound to the privacy rules that the user chooses: the user distributes location information only to authorized entities and informs these entities about how they are authorized to use the location information. Security mechanisms are put in place to support the application of the privacy rules, such as authentication to validate the identity of the entities and confidentiality to protect the location information en route between privacy preserving entities. The work of the Geopriv work, including many recent Requests For Comments, is of continuous relevance with respect to introducing privacy by design technical features into the Internet protocols.

4. Implementing Privacy by Design in all Layers of the Network

One of the innovative features that the IETF’s new privacy model introduces is that it encourages the implementation of privacy by design into all layers of the Internet – and not only in the core (low-layer) Internet protocols. The Internet engineering community has focused so far mostly on the design and update of Internet protocols and not on the implementation of these protocols in the application layer of the Internet. This is because it is difficult for protocol designers to foresee all pertinent privacy risks when standards are implemented. Hence, the new emphasis on the implementation of the Internet standards paves the way for expanding the scope of work of the IEFT by way of exploring ways to deploy privacy by design features and technology in all layers of the Internet. In this sense, informal technical standards can nurture privacy-protective practices in the industry sector.

An example of a work in progress towards this direction is the privacy choices for Internet data services. The draft standard argues that the Internet service providers should maximize, to the extent possible, the privacy protection offered to the users. Therefore, the best choice for a service provider is the ‘opt-in’ privacy option, meaning that it should not be left to the end-user to opt-in for the most protective privacy settings, but these settings should be the default - unless the user chooses decides to opt out. In light of the complex social factors forming the context for such choices and the existence of many users who are uninterested in making an informed choice, many experts suggest that it could best to remove the necessity for making such choices. If service providers adopt such a business practice, it will ensure by default the most privacy-protective option.

Other examples of implementing privacy by design in all layers of the Internet, include mobility protocols, privacy extensions for IPV6 addresses and onion routing; these technologies will mitigate the ease of fingerprinting and, hence, safeguard the anonymity and un-linkability of the users’ data. Private browsing and Do Not Track technologies can be built into the browser level providing users with a

---

128 Privacy Considerations for Internet Protocols, supra note 54, at 5-6; Report from the Internet Privacy Workshop, supra note 59, at 9-11.
129 Privacy Considerations for Internet Protocols, supra note 54; Report from the Internet Privacy Workshop, supra note 59.
simple way to opt out of web tracking. Even though business actors have been discussing *Do Not Track* technologies for a long time now, no serious steps have been taken to incorporate them into their systems and practices.

In these instances, Internet standards have the potential to shape business practices and future regulation. The draft EU Regulation on data protection already prescribes privacy by design as a requirement that should be implemented by any person or organization that controls the collection, processes, holds or uses personal information. It is the first (draft) legal document articulating privacy by design as a legal obligation. The APEC privacy framework also provides for the ‘preventing harm principle’ - recognizing that all means of regulating privacy (including technology, self-regulation and the law) must be designed to prevent privacy harm to individuals. Accordingly, it will be necessary to explore in the future how the privacy by design technological standard embedded in the Internet interrelates with the legal standard of privacy by design.

Overall, the IETF’s and IAB’s work clearly qualifies as a shift in the prevailing paradigm regarding the importance attached to privacy by design in the Internet’s core engineering. The new privacy threat model developed by the IAB, the introduction of encryption as the norm in Internet traffic, the mitigation of protocol vulnerabilities from a privacy point of view and the empowerment of the end-user do not only aim to mitigate the adverse implications of abusing the network, or to avoid privacy violations, but - most importantly - they establish support for privacy as a principle in the Internet’s protocol design. Privacy protection is no longer a mere concern, but it is now a guiding, structural principle of protocol design embedded into the DNA of the Internet and further disseminated into the deployment of Internet

---


protocols. Privacy protection becomes a thread running through the fundamental fabric of the Internet tapestry, which is made feasible by the inherent plasticity of the architecture.\textsuperscript{136} It is incorporated in the informal Internet standards and is built into the institutional design of the IETF by creating the privacy directorate. Following the 2014 IETF’s emphatic statement on pervasive monitoring as an attack and having demonstrated herein 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.\textsuperscript{137}

D. Online Privacy as a Technical Issue and as a Human Right: A Convergence Zone

Part D brings together the different perspectives on online privacy as a technical issue and as a human right. It argues that there is a convergence zone that needs to be explored, thereby establishing a common reference point for policy-makers and lawyers as well as the technical community. It discusses the confines of both perspectives and, it continues by showing that the two approaches interrelate and inform each other. The Internet engineering analysis of privacy employs the legal and policy point of view and, conversely, the human rights (and policy/legal) analysis benefits from the technical perspective of privacy as ‘trust to the network’. Although online privacy can be of course be seen and discussed under many different angles – some of which will be briefly examined below, it is the view of the present author that the convergence of the technical and human rights’ analyses and the coordination of the respective epistemic communities will be proven critical in the future for the effective protection of online privacy.

I. Online Privacy as a Technical Issue

\textsuperscript{136} Greenleaf, \textit{supra} note 25, at 606-607; Lessig, \textit{supra} note 13, at 39.
\textsuperscript{137} See the W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring, London, 28 February – 1 March 2014, \textit{available at} \url{https://www.w3.org/2014/strint/Overview.html}. 
As the article has stressed thus far, the Internet’s standardization bodies perceive privacy as a technical issue and, according to their mandates, they seek technical solutions to serious threats and violations of the users’ privacy. Technical standardization has gradually gained ground in international regulation. Many argue that one of the reasons for the standardization’s popularity is because it is associated with effectiveness and an elusive neutrality. The technical property of a standard, the problem-solving mandate of a body, the aim of adopting a technical solution to a given problem - all appear to be value-free and, hence, neutral and objective, self-validating, perhaps, their authority and legitimacy to resolve problems. Nonetheless, Part B established that the development of Internet standards and the mandates of the IETF and IAB reflect specific values (open and global architecture, interoperability, end-to-end design, decentralized management) and, at the same time, accommodate external, broader interests as long at the latter concern the development of the Internet and the needs of the global users.

Technical solutions, in general, appear to live a life parallel to the law and they are somehow expected to compensate for its shortcomings. Likewise, in the area of online privacy, the industry sector and Internet users think 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”. Even though the perception of the technical solution as replacing or displacing the law could lead to a technocratic government of experts, standardization, in the present context, does not necessarily have a negative connotation. ‘The geeks will save the Internet and privacy’ is a prevalent narrative among the Internet users. In other words, the Internet’s technical community is, or at least is perceived as being, the legitimate guardian of the network and the respective values it carries within it. The positive and

139 Pauwelyn, Wessel, Wouters, supra note 35, at 503 discuss the authority stemming from expert knowledge and epistemic/professional communities.
140 Peters & Peter, supra note 15, at 193-194 discussing the strict functional orientation and technical mandate of an international organization. The analysis is equally applicable to informal international standards-setting bodies.
142 Pauwelyn, Wessel, Wouters, supra note 36, at 90-91; Peters & Peter, supra note 15, at 195.
widespread reception of the standards by their addresses is a significant indicator of the bodies’ legitimacy.\textsuperscript{144}

However, when one discusses the technical solution paradigm it is important to be mindful of its confines. First, the technical solution paradigm includes many different nuances: the IETF and IAB are not the only standardization bodies whose work is pertinent to privacy and Internet-related matters. There is already proof of a power struggle between informal (IETF, IAB) and formal standardization bodies (such as the International Telecommunication Union and the International Standardization Organization) over issues of Internet governance.\textsuperscript{145} This struggle brings conflicting agendas and goals to surface, as well as competing standardization cultures, which may be a game changer with respect to the future of the Internet. It is sufficient to simply highlight two core differences between the ISO and ITU and their informal counterparts: 1) they lack the multi-stakeholder model of the IETF and 2) their standard-setting processes do not ensure an equivalent measure of transparency and inclusiveness.\textsuperscript{146}

A second caveat regarding the confines of the technical solution approach is that pervasive monitoring - from the standardization bodies’ point of view - is a technical issue and the incorporation of privacy by design in the Internet protocols is the respective technical solution. Although there is strong evidence suggesting that the technical community informs their point of view in light of the human rights (and largely legal) analysis of privacy,\textsuperscript{147} the IETF and IAB (being aware of their restricted mandate) do not frame privacy as a legal challenge or as an international human right, but rather as an attack on the reliable operation of the network that they safeguard. The IETF clearly stated that “the non-technical (e.g. legal and political) aspects of mitigating pervasive monitoring are outside of [its] scope. The broader Internet

\textsuperscript{144} Pauwelyn, Wessel, Wouters, \textit{supra} note 36, at 86-87.
\textsuperscript{146} Cafaggi, \textit{supra} note 79, at 702.
community will need to step forward to tackle [pervasive monitoring], if it is to be fully addressed.”

II. Online Privacy as an International Human Rights Issue

Besides being a technical issue, the consideration of global users’ privacy brings serious questions and interests under international law into the fore. The international human rights paradigm is currently one of the prevailing paradigms to address online privacy. The pressing need to address the protection of online privacy led to a series of activities and developments in the United Nations, including the recent decision by the Human Rights Council to create the mandate for the UN Special Rapporteur on Privacy. Further, the UN General Assembly in its 2014 Resolution on The Right to Privacy in the Digital Age affirmed, for the first time, that the right to privacy applies in digital communications and called upon states to respect their pertinent international obligations. Similarly, the UN Human Rights Council confirmed that the same rights that people have offline must also be protected online and stressed that all states should address security concerns on the Internet in accordance with their human rights obligations. The OHCHR and the UN Special Rapporteur on the Freedom of Expression, Frank La Rue, 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

---

148 Pervasive Monitoring Is an Attack, supra note 6, at 3; Sprint Workshop Report, supra note 98, at 9-10.
151 GA Res. 68/167, supra note 8, ¶¶ 3, 4; GA Res. 69/166, supra note 8.
the relevant international human rights law framework applicable to recent practices of states and other actors.\textsuperscript{153}

The human rights paradigm concerns the formal acknowledgment that human rights apply to the online environment. It follows that any interference with the right to privacy should be assessed on the basis of relevant international obligations and that states must revise their domestic legislation in order to set limits on their authority to monitor online communications. It is not clear at the moment 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 in light of these advancements will suffice. Pertinent suggestions on the UN level include the adoption of a new Optional Protocol to the ICCPR with regard to protecting privacy in the digital sphere\textsuperscript{154} or that the Human Rights Committee revisits General Comments 16 and 31.\textsuperscript{155}

Furthermore, the human rights paradigm frames the discussion on privacy in terms of a rights-based approach to the Internet. Pillay underlined in her Report that “international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed".\textsuperscript{156} In the same vein, the Council of Europe’s Committee of Ministers has highlighted (in the 2011 Declaration on Internet Governance Principles) the need for a “rights-based approach to the Internet”.\textsuperscript{157} Interestingly, besides international human rights bodies, other stakeholders endorse the rights-based approach as well. 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


\textsuperscript{156} UN Report on the Right to Privacy, supra note 2, ¶ 12 (emphases added).

\textsuperscript{157} CoE Declaration on Internet Governance Principles, supra note 30, ¶ 5 (emphases added).
standards must be consistent with human rights. Moreover, ISOC welcomed the “formal endorsement of a rights-based approach for the Internet” when the Human Rights Council affirmed that human rights are applicable online. There is an underlying significant value in establishing a prevailing narrative for the international discussion on privacy; such a narrative sets the parameters for defining the issues at stake and even prioritizes diverging or conflicting interests.

Nonetheless, it cannot go unnoticed that few international and/or human rights bodies engage with the legal implications of the Internet’s design principles and its special features. This reflects the lack of communication between the technical and non-technical communities. International lawyers and the international human rights community need to realize that the effective protection of online privacy entails both legal and technical measures. Technological tools, such as privacy by design or privacy enhancing solutions, and the development of legal informatics require the coordination of different epistemic communities. Bridging the gap between the different paradigms and the respective communities will be greatly beneficial, and provide significant enrichment, to the human rights analysis. Two points are worth mentioning in this respect.

The first point is that privacy by design should be tailored and incorporated into international human rights law and practice. It is often argued that technology renders the law irrelevant or that informal law replaces traditional (international)

---

158 NETmundial Statement, supra note 10, at 7.
160 The Rapporteur on the Freedom of Expression in the Organization of American States (supra note 1, ¶ 523) and the Council of Europe Committee of Ministers’ in the CoE Declaration on Internet Governance Principles (supra note 30) are the only bodies discussing this issue. The UN Special Rapporteur on the Freedom of Expression (supra note 5, ¶ 30) and the Human Rights Council in its 2014 Resolution (supra note 8, 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, (supra note 2) the Human Rights Council in its 2012 Resolution (supra note 8) and the UN General Assembly in its Resolution on the Right to Privacy in the Digital Age (supra note 8) do not make any reference to the special features of the Internet.
161 NETmundial Statement, supra note 10, at 9; 2013 UN Report on Freedom of Expression, supra note 5, ¶ 98.
law,\textsuperscript{164} but, in this instance, the technical solution paradigm not only complements but also strengthens the human rights paradigm.\textsuperscript{165} Privacy by design evidences that Internet’s engineers and the technical community are able to secure, to a great extent, online privacy.\textsuperscript{166} Despite the available technologies, policy-makers do not create incentives for the industry to develop and apply them in practice.\textsuperscript{167} States and legislators do not seem willing – with the exception of the draft EU Regulation - to explore how privacy by design can be ‘translated’ as a legal obligation or standard in national and international law. On the other side of the spectrum, the Internet Society puts an effort to explore the convergence between the human rights and technical approaches to privacy;\textsuperscript{168} the technical community incorporates the users’ perspective into its standardization work and attempts to effectively convey the implications of pervasive monitoring to policy-makers.\textsuperscript{169} Therefore, lawyers and policy makers should revisit our low level of engagement with the function of privacy as a technical issue.

Secondly, addressing privacy as an intrinsic value for the proper functioning and integrity of the network has certain important advantages over addressing privacy as a human right. Recent developments, following the revelations on pervasive monitoring, indicate that many states invoke the right of their citizens to online privacy – or, at least, use it as a convenient pretext - to subject the free flow of information and the Internet’s interoperability to their sovereignty.\textsuperscript{170} The motivations and reasons driving such policies vary; these policies find, however, their common denominator in the fact that many states - including Russia, Brazil and Saudi Arabia - argue for their right to “digital sovereignty” (mostly on the basis of the protection of

\textsuperscript{164} See Pauwelyn, Wessel, Wouters, \textit{supra} note 36, at 97.
\textsuperscript{165} Reidenberg, \textit{supra} note 24, at 583. \textit{Cf.} Cafaggi, \textit{supra} note 79, at 716 and Weiser, \textit{supra} note 162 who point out only the complementary function between legal and technical standards.
\textsuperscript{166} Wisman, \textit{supra} note 163.
\textsuperscript{167} Métayer, \textit{supra} note 62, at 323, 329-330; European Parliament Resolution on Surveillance, \textit{supra} note 7, ¶¶ 62, 63, 110.
\textsuperscript{169} See discussion infra Part C.III.
their citizens’ privacy). Hence, privacy in the human rights paradigm is - ironically - being (ab)used as a manifestation of state sovereignty in order to support practices leading to the fragmentation of the global and open nature of the Internet and the creation of many “national Internets”. Yet, the analysis in Part C showed that protecting the users’ privacy and their trust in the network is strictly interconnected to the freedom of information and the interoperability of the Internet on a global level. In this sense, within the context of ‘privacy as a technical issue’, the freedom of information and privacy are interlinked without states being able to invoke privacy as a possible limitation to freedom of information.

Moreover, the regulation of Internet users’ privacy has implications well beyond the reach of the right to privacy as such. The human rights perspective brings debates on values and cultural diversity into fore. Certain states contended in a draft resolution to the General Assembly that respect for human rights online, including privacy, should be balanced with cultural considerations and social systems of all countries. It should not be disregarded that, even though 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 in 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 concerning terrorism, extremism, racism and religious intolerance. Although the oral amendment was voted down, fifteen states supported the amendment, which makes it clear that there is no global consensus on Internet-

---


174 The oral amendment was voted down by twenty-eight to fifteen votes. The states that voted in favor of the amendment were: Algeria, China, Congo, Cuba, Namibia, Russia, Pakistan, Saudi Arabia, South Africa, UAE, Venezuela, Vietnam. Four states absented (Gabon, India, Indonesia, Philippines).
related or privacy-related issues.\textsuperscript{175} Therefore, even though the human rights angle brings pressure over states regarding the protection of online privacy, it also brings along cultural considerations which are employed to furnish limitations to the effective exercise of privacy. The technical point of view, on the other hand, promotes a language that certain states would perhaps be more willing to regard, without provoking the different cultural values’ debate or at least by way of laying the basis for a less heated cultural debate. The technical paradigm of privacy also enhances a rigorous understanding of the significance of the users’ privacy as a necessary precondition for States to invest in the digital economy. Policy-makers need to realize that privacy online is not only a human right, but also an enabler of public trust to the network and, therefore, of the digital economy. The growth of the Internet depends on users having confidence that the network will protect their private information.\textsuperscript{176}

This is a point that has been explicitly underlined by the International Conference of Data Protection and Privacy Commissioners and the European Data Protection Authorities by way of acknowledging the value in safeguarding the integrity of the network.\textsuperscript{177}

Finally, promoting privacy as a value for the Internet’s proper functioning brings new light into the discussion on whether the nationality or the location of the individuals under surveillance matters. 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.\textsuperscript{178} However, according to the technical point of view, the nationality or the


\textsuperscript{176} IAB Statement on Internet Confidentiality, \textit{supra} note 89.


\textsuperscript{178} UN Report on the Right to Privacy, \textit{supra} note 2, ¶¶ 31-36, 47; UN Special Rapporteur on Torture, \textit{supra} note 153, ¶ 62; GA Res. 69/166, \textit{supra} note 8. 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, \textit{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, 23 April 2014, U.N. Doc CCPR/C/USA/CO/4, ¶ 22 (a) (emphases added).
location of the individuals under surveillance are not relevant considerations since the Internet is global and transcends national boundaries. A threat to the users’ privacy and, hence, to the network exists regardless of nationality requirements or the geographical considerations at hand. The practice of Article 19, an international NGO dedicating its work to the protection of the freedom of expression, is very interesting in this respect. Article 19 in its oral statement to the Human Rights Council Panel Discussion on Privacy, decided to defend the human right to online privacy by adopting the perspective of the technical community; it reads 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, \emph{is a systemic and structural attack on the Internet}, regardless of the nationality or location of the ‘target’.”\footnote{179}

The above considerations about converging the two paradigms do not suggest that the technical standards take priority over human rights and the law or that the technical perspective should be preferred. Yet, on certain occasions, the human rights analysis and the effective exercise of privacy benefit from the value and function of the privacy seen from a technical point of view.\footnote{180} The latter may provide new arguments and, most importantly, can be a solid basis for the policy-makers to comprehend that the privacy of the end-users is interconnected to the trust to the network and the development of the digital economy.

\textbf{E. Conclusions}

Online privacy is a serious global issue that will define the future of the Internet as a platform for the realization of human rights as well as a driving force in


\footnote{180} It is to be noted that there are important points of divergence between the two paradigms. The values of the network and the values of human rights do not always converge. The goals and priorities of the two epistemic communities also differ. The technical community traditionally resists governmental interference since it believes that the evolution of the network should be free from any interference by states, whereas the human rights community strives to bring into play the responsibilities of the states under human rights law. See Liddicoat & Doria, \textit{supra} note 131, at 15. The scope of their work differs too since the IETF’s privacy threat model addresses attacks by any state and non-state actor.
the acceleration of the digital economy and international development. Policy and technology must be designed hand in hand while being mindful of the ramifications of each other.

The article argued that the effective protection of online privacy is not merely a matter of law but it also needs to be secured through technological means. Online privacy is hardwired into the basic infrastructure of the Internet, the Internet protocols, which are engineered on the basis of Internet standards. Internet protocols are, therefore, a powerful regulatory force that predetermines and shapes the privacy choices available to the users.

To this end, the article introduced and evaluated the work of the IETF and IAB entrusted with the technical management of the Internet. The analysis demonstrated that, despite the informal regulation of the Internet, said standardization bodies are highly regarded as the guardians of the network and the Internet standards enjoy great legitimacy. In the face of pervasive monitoring, the IETF and IAB decided to defend the privacy of the global users. It was stressed that, in accordance with their technical mandates, online privacy is valued as a condition for maintaining the users’ trust to the Internet and not as a human right per se or a legal consideration.

The technical solution to securing online privacy comprises of the integration of privacy by design into the Internet standards. The standardization work in progress strongly evidences a paradigm shift regarding the importance attached by the IAB and IETF to privacy considerations. Privacy qualifies now as a requirement when designing and updating Internet standards. The IAB has developed a privacy threat model to mitigate pervasive monitoring and established a privacy directorate overseeing all privacy related aspects of the technical standardization. The IETF, in its turn, is currently working on finding ways to mitigate protocol vulnerabilities from a privacy point of view. The introduction of encryption and the exploration of ‘opportunistic security’ serve the need of enhancing privacy protection in neglected, thus far, areas in the network, such as for example metadata and Internet traffic. Further, raising awareness among the end-users on privacy choices and empowering them to make pertinent informed decisions online is a high priority for the IETF. Overall, privacy by design is not only integrated into the Internet protocols as a requirement, but it is also built into the institutional design of the IETF and it enriches the engineering mindset of the technical community. Exploring the possibility of
implementing privacy by design into the application layer of the Internet could have significant ramifications insofar business practices are concerned.

Lastly, the article took the discussion one step further by examining how the technical solution paradigm strengthens the human rights analysis of the right to privacy. The role of privacy as a sine qua non condition for maintaining the users’ trust to the network lays the basis for a solid understanding of the value of privacy online and it is a convincing consideration for relevant policy making decisions. Moreover, the role of privacy within the institutional context of the technical community informs the point of view of the legal and the human rights communities. It brings new light to legal questions regarding the nationality or geographical requirements for protecting the human right to privacy as well as with respect to conceptualizing and applying existing legal concepts in the digital sphere.