Policy and Internet

Requiem for a Dream: On Advancing Human Rights via Internet Architecture

Milton L. Mueller and Farzaneh Badiei

A growing number of scholars and policymakers are calling attention to the relationship between technology standards, protocols, human rights, ethics, and values—also claiming that human rights can be secured (or violated) via the Internet's standards and architecture. However, this assertion of governance through Internet architecture can oversimplify the complex relationship between technology and society. This article argues that human rights are primarily a political and institutional accomplishment, not a simple matter of technical design. By articulating a challenge to uncritical and imperfectly theorized efforts to link standards-setting and protocol development to "values" and human rights objectives, we hope to foster a more realistic approach to Internet standardization and governance processes and a more balanced and well-informed theoretical debate. Situated in the theoretical literature on science, technology, and society, our analysis is also informed by extensive empirical exposure to standardization and Internet governance processes. It includes two short case studies in which standards development and rights issues have intersected in ways that illuminate the relationship between rights and standards, and which can be interpreted to falsify certain claims.

KEY WORDS: Internet architecture, Internet governance, human rights, values in design, Code is Law, IETF

越来越多的学者和政策制定者正在呼吁关注科技标准、协议、人权、道德以及价值观之间的关系，同时主张：人权可以通过互联网标准和机构从而得以保护或受到侵害。然而，这种通过互联网架构进行治理的主张有可能过于简化了科技和社会之间的复杂关系。本文认为，人权主要是一种政治上和制度上的成就，而不仅仅是技术设计这样简单。通过阐明缺乏批判性的不完整理论实践(即将标准设定和协议拟定与“价值观”和人权目标联系起来)所面临的挑战，笔者希望能制定出一项更具有现实意义的措施，用于互联网标准化和治理过程，同时引起更平衡、更全面的理论辩论。基于研究科学、技术和社会的相关理论文献，本文同时对标准化和互联网治理过程进行了广泛的实证分析。分析包括了两例简短案例研究，其中标准化的发展和权利问题在某些方面产生了交集，即权利和标准之间的关系，后者能够通过诠释进而伪造部分论断。

关键词： 互联网架构，网络治理，人权，设计中的价值观，代码即法律，互联网工程任务组(IETF)

Un número creciente de académicos y legisladores llaman la atención sobre la relación entre los estándares tecnológicos, los protocolos, los derechos humanos, la ética y los valores, y también

doi: 10.1002/poi3.190

afirman que los derechos humanos se pueden asegurar (o violar) a través de los estándares y la arquitectura de Internet. Sin embargo, esta afirmación de la gobernanza a través de la arquitectura de Internet puede simplificar en exceso la relación compleja entre la tecnología y la sociedad. Este artículo argumenta que los derechos humanos son principalmente un logro político e institucional, no una simple cuestión de diseño técnico. Al articular un desafío a los esfuerzos acríticos e imperfectamente teorizados para vincular el establecimiento de normas y el desarrollo de protocolos con los "valores" y los objetivos de derechos humanos, esperamos fomentar un enfoque más realista de los procesos de estandarización y gobernanza de Internet y una teoría más equilibrada y bien informada debate. Situada en la literatura teórica sobre ciencia, tecnología y sociedad, nuestro análisis también está basado en una amplia exposición empírica a los procesos de estandarización y gobernanza de Internet. Incluye dos breves estudios de casos en los que el desarrollo de estándares y los problemas de derechos se han cruzado de forma que iluminan la relación entre los derechos y los estándares, y que pueden interpretarse como falsificadores de ciertos reclamos.

PALABRAS CLAVES: arquitectura de Internet, gobernanza de internet, derechos humanos, valores en diseño, código es ley, IETF

Introduction

A growing number of Internet scholars, policymakers, and engineers are debating the relationship between technology standards and protocols, and human rights, ethics, and values. This is a part of a broader effort to bring human rights principles into Internet governance (Hick, Halpin, & Hoskins, 2016; Jørgensen & Pedersen, 2017). National governments and international organizations are contributing to this trend. The Council of Europe, which has been discussing human rights principles on the Internet for some time, recently published a Guide to Human Rights for Internet Users emphasizing that recognized human rights apply equally online and offline.[1] The Brazilian Marco Civil da Internet (the Civil Rights Framework for the Internet), is another example of an attempt to apply notions of rights to the online environment (Tusikov, 2016). In 2016, the advocates of online human rights achieved a milestone when the UN Human Rights Council (2016) passed a resolution on "The Promotion, Protection and Enjoyment of Human Rights on the Internet."

As Internet freedom advocates, we are broadly supportive of human rights in the online environment. But we note that a significant fraction within this Internet/Human Rights discourse has begun to assert that human rights can be advanced through the design of the Internet's standards and architecture (see the literature review below for specifics). Similarly, others have claimed that engineers have an ethical responsibility to be aware of the human rights implications of their design decisions. This has resulted in the entry of human rights (HR) advocates into the Internet Engineering Task Force (IETF) and the formation of a working group on "human rights protocol considerations" within the Internet Research Task Force (IRTF). There have also been plenary sessions devoted to discussion of the problem at recent meetings of the IETF.

Can standards and protocols advance human rights? By raising this question, the Internet governance and technical communities are reopening a longstanding debate over the relationship between technology and society. It might be useful if this discussion was not so one-sided. This article has two goals. The first is to articulate a challenge to what the authors think has been an uncritical and imperfectly theorized effort to link standards-setting and protocol development to "values" and human rights objectives. Second, by raising this challenge, the authors hope to foster a more realistic approach to Internet standardization and governance processes and to provoke a more balanced and well-informed theoretical debate about the relationship between Internet standards and infrastructure on the one hand, and human rights norms and laws on the other.

The article is divided into five sections. Section "Method" explains the methods and data used by the authors. Section "Theories of Techno-Social Influence" situates the argument about human rights, standards and protocols in the scholarly literature on science, technology, and society (STS), cyber law, and Internet governance. The third Section "Human Rights and the IETF" describes the current activities and debates within the IETF regarding human rights and standards development. Section "Waking Up From the Dream" puts forward our critique. We identify four problems with this effort: (i) it is not possible to simply translate legal standards such as the Universal Declaration of Human Rights (UDHR) into protocols or technical designs; (ii) new standards and protocol designs have an incremental, limited influence on Internet infrastructure; (iii) such efforts can encourage undesirable forms of politicization of standards development; and (iv) it is not possible to know in advance exactly how standards will affect human rights. The fifth Section "Why Code Is Not Law: Two Case Studies" looks at two case studies in which IETF standards have intersected with human rights issues; we think these cases clearly falsify certain claims regarding embedding values and rights into designs. A concluding section recaps the argument and explains why we think it is important to engage in a critical examination of the HR activists' incursions into standards development.

Method

The article is grounded in direct observation of HR activists' interventions in IETF and ICANN meetings over an 18-month period (January 2016–July 2017).[2] It is also grounded in collecting, reading, and analyzing all the documents produced by the HR protocol considerations group. The article seeks to accurately describe and then critically examine the claims made by HR advocates to justify their focus on technical standardization processes. We document the fact that HR advocates cite theoretical scholarship on Internet governance and STS studies to support their belief that human rights can be advanced through the standards process. We map their claims to specific theoretical positions in the STS literature, and then identify conceptual flaws and limitations in the theories invoked. We also observe logical problems in

the way the theories are applied to the specific case of IETF standards development (e.g., we note that much of the theory invoked suggests that design can affect rights *ex ante* but most of the actual HR concerns are raised *ex post*).

To further bolster the critique, we examine two real instances in which standards development in the IETF have intersected with law, policy, and HR concerns. We selected the two cases because both were repeatedly cited by the HR activists themselves as illustrations of the relevance of human rights to IETF processes and as evidence of the need for HR interventions. The analysis of these two cases should not be confused with a statistical method which purports to compile a representative sample of all IETF protocol documents (of which there are thousands), nor can they be dismissed as anecdotal. Rather, they provide concrete refutations, in the Popperian sense, of the relationship between rights and standards claimed by many of the activists and some engineers. The cases indicate that the rights impact of IETF standards fail to conform to the "code is law" or "values in design" theories.

Theories of Techno-Social Influence

The intersection of standards development and human rights seems to be based on recent scholarly literature asserting that protocols have politics and that Internet architecture embodies human rights, or mediates struggles over rights (Cath & Floridi, 2017; DeNardis, 2010, 2014; DeNardis & Hackl, 2016; Musiani, 2012). It also has connections to the literature on "values in design" (Flanagan, Howe, & Nissenbaum, 2008; Nissenbaum, 2001).

If one examines the intense discussions around human rights within the IETF, one sees multiple claims being made about the relationship between protocol developers and society: "technology is not neutral," "protocols have politics," "code is law," "architecture mediates rights," "designers have an ethical responsibility," "values can be (or should be) embedded in design." Many of these claims have different theoretical bases and practical implications. These need to be clearly distinguished and the implications of each position carefully thought through.

In this section, we situate these claims in the scholarly and scientific literature on STS and Internet governance. The arguments can be quite fluid and overlap, but we group them into three categories: (i) a *code is law* argument; (ii) an assertion that *Internet architecture mediates rights*; and (iii) an assertion that *designs embody values and therefore engineers should consciously take social values into account* when developing or designing technical systems. In this article, we will consider the three claims separately in order to provide a more precise picture of scholarly work on Internet protocols and architecture as a governance tool.

Code Is Law

Those who assert the power of architecture and infrastructure in Internet governance characterize their view as the "turn to infrastructure in Internet

governance" (DeNardis, 2014, p. 184; Musiani, Cogburn, DeNardis, & Levinson, 2016). However, we are not sure when and where this "turn" took place, given architecture and infrastructure have played a prominent role in Internet governance discussions from the beginning. We cannot identify the exact start of the discussion but as early as 1996, Mitchell argued that "out there on the electronic frontier, code is the law" (Mitchell, 1996, p. 111). Soon thereafter, Reidenberg (1997) argued that Internet policy can be created and enforced through technology, hence creating a system (*Lex Informatica*) that is analogous to a legal system. Lessig (1999a) is most strongly associated with claims that code is law, with his famous book *Code and Other Laws of Cyberspace* transforming the assertion into a common aphorism. In it, he argued that intermediaries can regulate behavior by modifying their architecture:

> If AOL does not like a certain behavior, then in at least some cases it can regulate that behavior by changing its architecture. If AOL is trying to control indecent language, it can write routines that monitor language usage... (Lessig, 1999a, p. 71)[3]

Lessig, however, recognized that code is but one of four elements producing social control: the others being law, norms, and the market. To this day, dozens of young Internet law and governance scholars dutifully repeat this quadrinity, as if Lessig had invented sociology. But *Code is Law* became the lasting meme because cyberspace was seen as almost entirely man-made, so the significance of architecture (Lessig believed) was now drastically increased in relation to other modalities. While he rarely mentions the term "governance," the main message in his later book "*The Future of Ideas*" (Lessig, 2002) was that control will eventually take place through various layers of the Internet. Other scholars have also claimed that norms can be embedded in code to regulate society, and have explored the legitimacy concerns created by this (Graber, 2012; Koops, 2008; Nunziato, 2000). Tien (2005) warned that laws and regulations can be embedded in Internet architecture; users are governed by strictly structuring the setting of their online communication before they even start acting on the Internet. Mayer-Schonberger (2000) argued that this kind of governance can even surpass the normal avenues of lawmaking such as the parliament and courts.

The code is law argument created many discussions similar to the "turn to Internet infrastructure" discussion (Asscher & Dommering, 2006), but this similarity is scarcely acknowledged in the recent literature (see Brown, Clark, & Trossen, 2010; Musiani, 2013). For example, Musiani (2013) makes assertions very similar to the claim that "code is law" although she does not specifically mention the literature. She states that:

> technical architecture appears as one of the strongest, if not the strongest structuring element of internet governance: what is shaped into architecture and infrastructure can seldom be undone by institutional negotiation and dialogue alone, and institutions find it increasingly complicated to

> keep up with 'creative' governance by architecture and by infrastructure. (Musiani, 2013)

The lack of reference to the earlier "code is law" literature might be because Lessig's usage of the term "code" could be interpreted as software applications and not as Internet protocol or architecture. In fact, Lessig also referred to architecture, and he used the term "code" very broadly to refer to "the rules and instructions embedded in the software and hardware that together constitute cyberspace as it is" (Lessig, 1999b). This broad definition would seem to include any and all protocols as well as the basic design or architecture of the Internet.

At its most basic, the idea that code is law implies that society and behavior are shaped *ex ante*, by design. Adherents of this view might then advocate for HR activists to get involved with the IETF and other standards bodies, for if they can shape or control Internet standards processes they will gain a powerful competitive advantage in the struggles to secure or advance human rights.

Architecture as Mediator of Struggles Over Rights

The viewpoint that Internet architecture *mediates* rights has some similarities to the code is law argument, and adherents sometimes jump between the two positions. But in fact it is a distinct argument with its own strand of literature. To our knowledge, use of the term "mediation" started gaining prevalence when DeNardis (2014, p. 1) stated that "technologies of Internet governance mediate civil liberties such as freedom of expression." Mediation implies a more subtle relationship between rights and architecture. It indicates that the same rights, if they are to be retained in a new technological environment, have to be reconfigured and redefined, because the new structure of the medium creates new practices and hence new opportunities for limiting or advancing rights. This approach also focuses more on *ex post* attempts to affect behavior by modifying Internet infrastructure rather than *ex ante* design. It is, therefore, less deterministic. It implies that the infrastructure can be seized upon by states or private actors to curb freedoms, eliminate privacy, or discourage bad behavior. The implications of this view for HR activists are less clear. Not just architecture and protocol designs, but also their implementation and day to day operation, become a contested arena around which struggles over rights take place. This view implies, more realistically, that HR advocates are engaged in what is essentially a *political* or *policy* struggle, not simply a design process.

In the "architecture mediates rights" literature, scholars have emphasized the way parts of the technical architecture have been pressed into service by *external interest groups* (not the original engineers or designers) to effectuate censorship and intellectual property enforcement (DeNardis & Hackl, 2016). The Protect IP Act (PIPA) and Stop Online Piracy Act (SOPA) are two examples of what Musiani (2016) calls governance by infrastructure. These laws tried to configure the

domain name system to preempt or regulate copyright infringement. Regulation of Internet architecture to mediate rights has also been extensively discussed by Brown and Marsden (2013). Relatedly, there is a large literature on intermediary liability, which examines efforts to push responsibility for various Internet-related social problems (including hate speech, terrorist speech, cybersecurity, and copyright infringement) onto platform providers or Internet service providers (ISPs; Bendrath & Mueller, 2011; Bridy, 2010; OECD, 2011).

Another difference between "code is law" and "architecture as the mediator of rights" is the level of "embeddedness." The code is law literature sees regulation as embedded in Internet architecture, sometimes invisibly or without the user's knowledge (Lessig, 2006). The Internet architecture literature, in contrast, focuses more on how different laws and regulations try to consciously regulate behavior and enforce laws by shaping Internet architecture or infrastructure.

Values in Design

The idea that political, ethical, and cultural values are "embodied" in technology can be traced back to Lewis Mumford (1934) and the work of Winner (1986). The values in design (VID) movement is a more recent and narrowly scoped derivative of this line of thinking. VID adherents believe that "technology is never neutral," because "design decisions enable or restrict the ways in which material objects may be used, and those decisions feed back into the myths and symbols we think are meaningful."[4] Yet in practice VID does not offer a macro-level theory like Mumford or Winner. Instead, it focuses on the design of specific systems, calling attention to the way technical design choices reflect specific values or pose ethical choices that need to be taken into consideration in the design process (Flanagan et al., 2008; Nissenbaum, 2001).

A similar approach to design is reflected in the notion of regulating by design (Yeung, 2008), Privacy Enhancing Technologies (PETs), as well as Privacy by Design (PbD). All three emphasize the ways the design of technology can protect privacy and help achieve compliance with data protection legislation. The PbD literature can be or is encouraged to be prescriptive rather than descriptive (Bélanger & Crossler, 2011).

Cavoukian (2011) is credited with developing the concept of PbD in the mid 1990s. She defined it briefly as "embed privacy into the architecture of technologies and practices" (Cavoukian, 2011). More extensively, she stated that "Privacy by Design extends to a 'Trilogy' of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure" (Cavoukian, 2011). As we can see from the principles, PbD is a multifaceted concept, it includes both embedding values in a technology by the engineers as well as generating processes, policies, and organizational arrangements to protect privacy in design of technology (Rubinstein, 2011, p. 1421).

PbD uses PETs either as a *substitute* for regulatory oversight targeting privacy violations, or as a *complement* to support compliance with data protection

regulations. Rubinstein (2011, p. 1419) argues that complementary uses of PETs are much more successful than the substitutes. In other words, embedding privacy in the design of the technology has not really happened, while adopting and enforcing privacy preserving laws and policies has given actors real incentives to use PETs. As Koops and Leenes (2014) emphasize, privacy regulation cannot be hardcoded in the system or an architecture. Hence the concept of PbD has not embedded values in technology; rather, policies, laws, and incentives have changed the ways software companies use technology that collects and handles data.

Since the 1990s the awareness of the value-laden nature of technical design choices has evolved into a theory and method to "account for" human values in a systematic manner throughout the design process. This is known as value sensitive design (VSD). It includes an attempt to analyze and get input from direct and indirect stakeholders in a technical system and to incorporate individual, group, and societal levels of analysis. The attempt to reach out to stakeholders raises a number of thorny issues, however. As Manders-Huits (2011, p. 279) argues, technical ecosystems are now so complex that it can be difficult even to identify all indirect stakeholders, much less collect their input, as "people may be unaware of the implicit normativity of a technology until it is experienced." Furthermore, stakeholder input pulls designers away from the promise of promoting a specific set of values such as human rights, and instead pushes them toward incorporating the *prevailing* set of values and trade-offs demanded by various stakeholders, who may not favor classic human rights. Ironically, while VID is rooted in the idea that technology cannot be neutral, some adherents, when confronted with the existence of conflicting values in society, seem to imply that VSD should strive to make design decisions that accommodate value differences—which sounds suspiciously like an attempt to achieve neutrality.[5]

The VID perspective is especially relevant to the Internet governance domain because some of its leading promoters have received grants from the U.S. National Science Foundation's Future Internet Architecture (FIA) program. The FIA or "Genie" program sought to explore the possibilities of a complete redesign of the Internet, with the implied hope that the new Internet would rectify or avoid many of the problems (both technical and social) posed by the existing Internet. Social scientists were enlisted in the redesign effort, based on the premise that their input would make it possible to engineer good values into it, and thus preemptively solve future social problems. The VID adherents encouraged these grand aspirations, claiming that just as engineers set forth technical and functional specifications and constraints as design requirements, so should "those who design and produce systems take into consideration, that is, engineer, values as among the functionalities and constraints of their systems."[6]

Human Rights and the IETF

The intellectual climate set by the theories discussed above has led to an intersection of HR groups and the Internet technical community. The IETF is an

environment where certain values favoring Internet freedom, and a culture rooted in high-tech industries and universities, prevail. The human rights push is centered within the IRTF, which focuses on the longer-term research issues related to the Internet. In addition, a plenary session at the March 2017 meeting of the IETF (IETF 98)[7] featured a widely attended discussion of "Can Internet Protocols Affect Human Rights?" The discussion featured presentations by one of the veterans of early Internet design, David Clark, and one of the co-chairs of the HRPC RG, Niels ten Oever of free expression advocacy group Article 19.

The Research Group on Human Rights Protocol Considerations

Co-chaired by Article 19 and Internet governance activist Avri Doria, the IRTF in July 2015 chartered a Research Group on "Human Rights Protocol Considerations" (hereafter, the HRPC RG).[8] The charter of the HRPC RG states that the group was established: "to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the UDHR and the International Covenant on Civil and Political Rights (ICCPR)."

The HR advocates point to the UDHR as a set of values that can be enabled through Internet protocols (Cath & Floridi, 2017). UDHR/ICCPR is usually cited because it is thought to have more legitimacy and authority than other values because the majority of the international community has (nominally) accepted it (Brown et al., 2010). However, there are now more than a dozen internationally agreed instruments creating a vast number of "human rights," involving not only the UDHR/ICCPR but also a "right to development," a broad set of economic, social, and cultural rights including a "right to social security," and the right to "periodic holidays with pay." The HRPC has thus chosen to be selective in their approach to internationally agreed human rights: "we're not discussing all human rights because not all human rights are relevant to ICTs in general and protocols and standards in particular" (IRTF, 2017, p. 39).

The list of HR values that the HRPC RG says can be affected by Internet protocols includes nondiscrimination, rights to life, liberty, and security, freedom of opinion and expression, freedom of assembly and association, rights to equal protection, legal remedy, fair trial, due process, presumption of innocence, appropriate social and international order, participation in public affairs, participation in cultural life, protection of intellectual property, and privacy (IRTF, 2017, p. 38). According to the IRTF, this list is not exhaustive and other human rights can be added to it.

The HRPC WG charter states that "Since the Internet's objective of connectivity makes it an enabler of human rights, its architectural design converges with the human rights framework" (IRTF, 2017). The statement that the Internet's architectural design "converges with the HR framework" does not have a clear meaning. Is it a strong, "code is law" claim, or merely a statement that the two are complementary or compatible? The charter seems to imply that it is the "Internet's objective of connectivity," not its specific protocol design or architecture *per se*, that enables freedom of expression. This would imply that non-

technical things that promote connectivity, such as economic policies that incentivize widespread and affordable access, would also play a role in enabling human rights. The claim that technology "enables" freedom of expression is quite a pullback from "inscribing," "baking in," "encoding" or "embedding" values and human rights in technology[9] (Cath & Floridi, 2017; DeNardis, 2009; Milan & ten Oever, 2017).

Cath and Floridi (2017) provide some guidance as to what "a human rights enabling environment" means. They suggest that, for example, IETF could "enable" privacy by including privacy considerations in their Requests For Comments (RFC) documents, the formal standards developed by the IETF. An RFC does not, they realize, bind the engineers to protect privacy when developing protocols but it does "allow the technology to enable the actualisation of the right to privacy" (Cath & Floridi, 2017, p. 458). In their definition, an "enabler" is not the same as an *enforcer* or *protector* of human rights; it merely makes it possible to experience them, but obviously can be overcome by state power or regulations (e.g., by banning use of the technology or by state-mandated release of private information by intermediaries, or simply by relevant parties not using the enabling technology). So once again we find a significant pullback from the stronger claims about the relationship between technology design and human rights.

Waking Up From the Dream

The idea that technology designers or developers can make choices that advance certain values is an appealing one. To extend that idea further, into a claim that IETF protocol developers can actualize the UDHR, is even more so. In this section, we feel compelled to throw cold water on some of those claims. The authors of this article are supporters of Internet freedom and the fundamental individual rights to freedom of expression and assembly, privacy, security, and due process. Our problem is not with the goals, but with unrealistic notions of how they can be achieved.

Problem 1: The UDHR Is Too Complex and Too Laden With Baggage

As noted above, the HR advocates within the IETF have put a great deal of emphasis on the UDHR/ICCPR as a baseline set of values to guide design. They have even brought international law experts into IETF meetings to discuss with the engineers the intricacies of internationally recognized human rights instruments. We believe this fixation on the UDHR is a mistake. While it does purport to be universal and global like IETF standards, international human rights law is not a precise or even consistent set of documents. An insistence on a specific corpus of international law can divert and confuse rights-conscious engineers more than it clarifies and guides their design choices. The more basic problem is that *legal* conceptions of rights cannot be isomorphically translated into *technical* standards.

Network engineers and information systems designers have a solid idea of what is meant by the security and confidentiality of information (Allen, 2001; Layton, 2007). In technical contexts, the notion of "privacy" is understood to mean the *confidentiality* of information, which is defined as the property that "information is not made available or disclosed to unauthorized individuals, entities, or processes" (Allen, 2001, p. 26). The IETF's work has been deeply concerned with privacy (confidentiality) and security since long before the inception of the HR group. Instructions to RFC authors say "All RFCs must contain a section near the end of the document that discusses the security considerations of the protocol or procedures that are the main topic of the RFC" (Postel & Reynolds, 1997, p. 10). Moreover, the technical shortcomings that were exploited by the National Security Agency to carry out mass-scale surveillance were recognized by the IETF before the Snowden revelations (Garfinkel, 1995, p.167; IETF, 2005). Post-Snowden, the IETF claimed that "Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."[10] What, then, is gained by invoking the UDHR?

Compared to privacy and security, there is even more ambiguity about the way technical design relates to the concepts of freedom of expression and freedom of association. But these principles have a legal and political meaning that pre-dates the UDHR by centuries, and it is difficult to see how any of the ambiguities around their application to technical systems are eliminated by invoking the UDHR. If privacy, free expression and free association are the core values the HR advocates want to preserve on the Internet, it is unclear what is gained by linking these efforts to the UDHR.

What is lost by doing so? It would be an understatement to say that not all rights enshrined in the UDHR are relevant to Internet or information and communication technology; indeed, the HRPC RG explicitly acknowledges this fact and, as we have shown, selects out a few key values. However, the HRPC RG cannot have it both ways. If the rights that protocol designers are trying to protect gain their legitimacy and authority by virtue of their presence in the UDHR/ICCPR, then the IETF cannot be selective about what rights or values in the UDHR they are trying to protect. They are committed to any and every right declared by the United Nations. And because United Nations instruments are laden with rights claims that are often overly expansive, highly qualified, and subject to conflicting claims, these United Nations instruments could be used to limit or undermine the scope of some fundamental individual rights. Multiple inconsistent rights claims could cancel each other out. Invoking the UDHR could come back to haunt them.

The emphasis on the UDHR might be motivated by an attempt to let engineers off the hook for determining which rights or values they are promoting in their standards. Using the UDHR as a guide, they can claim they are not making policy but are merely implementing already well-established rights. But this effort breaks down when the HRPC RG becomes selective in its choice of relevant rights. It breaks down even further when it requires protocol developers to "balance" conflicts among rights. Even the rights deemed most relevant to information and communication technologies and networking contain internal

conflicts. This is especially true of values such as free speech and privacy, which have a fundamental impact on individual autonomy and the distribution of power in societies. Article 12 of the UDHR says "No one shall be subjected to ... attacks upon his honour and reputation." Article 19 of the UDHR says "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The potential for tension or conflict between these two is obvious; someone might use their freedom of expression to attack another's reputation. In law, these rights can be balanced by means of a case by case consideration of their interaction by a judge. It is unlikely that a protocol design can resolve this conflict. Similarly, Article 27 (2) recognizes a right to intellectual property protection which can also conflict with freedom of expression. Ironically, it is opposition to SOPA/PIPA and similar attempts to embed copyright protection in the infrastructure that has sparked so much opposition in the technical community and motivated much of the "turn to infrastructure" literature among Internet governance scholars. Yet a strict adherence to UDHR might suggest that SOPA/PIPA was a legitimate attempt to encode UDHR values in the Internet.

To its credit, the HRPC RG recognizes the existence of conflicts among rights.[11] But its response to this problem can only be characterized by the IETF expression "hand-waving." It says "the different affected rights need to be balanced" and "decisions on design and deployment need to take [rights conflicts] into account." Balanced how? What does it mean to "take rights conflicts into account?" How does that provide any guidance as to how to resolve conflicts? Notice here how far the HRPC WG charter backs away from the harder, "code is law" and VID approaches to human rights, even going so far as to say "technology can never be fully equated with a human right." Instead, they scale back their claim to an attempt to provide "guidelines for human rights considerations to ensure that protocols developed in the IETF do not have an adverse impact on the realization of human rights on the Internet" (IRTF, 2017, p. 4).

Problem 2: The Limited Role of Standards and Protocol Design

The HR push in the IETF can easily overstate the significance of protocol design in the overall Internet freedom equation. To begin with, adoption of IETF standards is entirely voluntary. Software and equipment vendors can do what they want with the standards after the IETF is finished with them. IETF standards enable compatibility among actors willing to achieve compatibility, but they do not compel adoption, so anyone is free to opt out of any values that are "embedded" in their protocols. The stronger the degree to which standards control behavior or impose values on their users, the more likely it will be that actors who do not like those values will not adopt those standards (see Case Study 2).

Further, the Internet is not a new thing anymore. It is an increasingly mature and, some have claimed, increasingly sclerotic infrastructure. Its basic architecture

and most of its protocols and standards are already in place, and are deeply embedded in operations and infrastructures. Truly new standards—as opposed to minor modifications or extensions of existing standards—have a difficult time gaining acceptance. This is not to say that the system is static. There are many changes taking place in protocols and standards, and many of these changes are significant. But major new protocols (such as IPv6 or DNSSEC) have adoption trajectories and effects that will play out over a period of decades, not months. Thus, it would be an exaggeration to suggest that *current* violations of human rights can be combated by altering *new* standards documents. And the effects of these standards, as we argue in more detail later, are not easily predicted or controlled.

Problem 3: Whose Values? Technical Design and Politics

Insofar as they attempt to encode a specific set of values into their work, standards and protocol developers open themselves up to the charge that they lack the legitimacy to define, enforce, or balance rights for society as a whole. They may also open the door to forms of politics that could stifle radical or disruptive innovation.

Let's assume that protocol authors can predict which rights their protocol will affect, and how (We raise serious doubts about this possibility in Problem 4 below.) Should the authors of an Internet protocol be the ones to balance conflicting rights? If standards developers are in the business of finding the correct "balance" between conflicting rights claims, and if those decisions have a major impact on human behavior (another questionable assumption, see next section), then developers are *de facto* judges or policymakers. If so, rights-promoting Internet engineers will not be the only ones actively engaged in standards and protocol development. Stakeholders who want to limit or violate human rights will be there, too.

If code making and architecture design really are the same as governance or public policymaking, does this mean we should be electing delegates to the IETF through elections, in which all citizens, regardless of their technical expertise, should hold equal weight? More dangerously, this argument might be used to argue that government policymakers should be afforded some kind of review or veto power over IETF products. IETF meeting participants are not democratically accountable and thus it could be claimed they do not have the necessary legitimacy to decide on which rights to enable and how to balance conflicting rights. One wonders whether the IETF, and the HR advocates urging them into this space, are fully aware of the broader political implications of the belief that they are inserting specific values into society via the technical infrastructure.

The VSD methodology has already stumbled onto this problem. Its method attempts to ensure that designers seek input from affected stakeholders, both direct and indirect. At a small, localized implementation scale, such consultations are routine and common-sensical: the intended users of a technology should be

consulted in developing specifications and functionalities. These consultations become increasingly problematic, however, as the social scope and scale increase, and as the technology being designed becomes more general purpose or more radical in its effects. There are severe limits on the ability of protocol designers (or anyone else) to predict who will be affected by new designs and how. The designers of the DNS protocol, for example, had no idea that domain name registrations would be commercialized in the future and that a burgeoning market for domain names would in turn have a major impact on the rights balance between trademark holders and free expression advocates.

More troubling, the more the technical design process comes to resemble a process of public policymaking with stakeholder input and representation, the more difficult it will be for radical and disruptive innovations to emerge. Some of the world's most life-altering technologies never would have seen the light of day if their developers had been required to acquire the consent of, or permit the influence of, established stakeholders in society. The Internet is most likely one of those technologies. Had incumbent telephone companies and heads of state been consulted about how to make the Internet's design reflect their "values," for example, it is hard to imagine how its globalized, open structure would have survived.

Our critique of the tacit politicization of protocol development should not be confused with a contention that the protocol/standards development process is entirely apolitical or "outside" of the political economy. Standards processes are already deeply political in the narrow and limited sense that vendors and user groups who are directly affected by choices made at the standards level will strive to shape the process to suit their immediate interests. Engineers, and their employers, are certainly affected by economic incentives, political constraints, and by internal organizational and personal politics. But while political economy sets the context within which technical problems are posed and solved, one cannot reduce the practice of engineering to legislating or making public policy.

Problem 4: Design Is Ex Ante*; Societal Impacts Are Known* Ex Post

The HR advocates imply that the translation of rights into Internet architecture should take place by design (Cath & Floridi, 2017). Rights should be considered in the process of drafting Internet standards, *ex ante*, before any violation happens. But the IRTF RG group's proposed methodology recommends mapping the protocols that have been used to undermine human rights and creating a "glossary" of the protocols that are human rights enablers.[12] This is a curious approach, because the assessment of human rights impact is *ex post* rather than *ex ante*. Addressing rights *ex post*, in response to actual incidents and uses, is a more sensible and realistic approach—but it is qualitatively different from the "code is law" or VID models. Modifying standards after incidents to mitigate their misuse means that we have *not* embedded rights in the Internet architecture. It means that the primary human rights impact occurs not in the standardization process but afterward, in implementation and use. This suggests that it is not possible to simply translate rights into the Internet architecture and thereby insulate them from future violations. It suggests,

instead, that the infrastructure is a site of ongoing contention by various actors with conflicting needs and interests.

We would generalize this argument to claim that it is never obvious how a new protocol, technology, or standard will affect society in the future. MIT's David Clark is a co-author of the renowned technical paper on the "end to end argument," a key principle of Internet architecture that has been retroactively credited with supporting the values of openness, network neutrality, and Internet freedom (Saltzer, Reed, & Clark, 1984). But at the IETF 98 plenary, Clark flatly denied that this was their intent. "If you go read the paper," he said, "it's about building a system that works;" that is, they were concerned with solving a technical problem regarding the relationship between the application layer and the transport layer. Clark stated, "back then when we were designing things we were not at all able to articulate how these might play out in a larger space …. The network we built came to express values that we could not have articulated at the time."[13]

Even when values are explicitly present in IETF design considerations there is still uncertainty about how things will play out in the real world. The HRPC RG guidelines urge designers to look at RFC 6973 (IETF, 2013) for guidance about protecting privacy. But even that RFC explains that privacy protections at the protocol level do not guarantee "undetectability," and recommends continued striving toward security goals.[14]

Why Code Is Not Law: Two Case Studies

This section examines two specific instances in which HR considerations interacted directly with policy, law, and rights. They demonstrate clear deviations from the expectations and predictions of a "code is law" or "values in design" theory.

Case 1: CALEA

A revealing case study of how the relationship between political power, human rights, and technical architecture plays out is provided by the history of the U.S. Communications Assistance for Law Enforcement Act (CALEA). CALEA forced U.S. telephone companies to redesign their network architectures to facilitate wiretapping of telephone calls by law enforcement agencies. The law was deemed necessary because earlier forms of wiretapping based on analogue technology simply did not work on the new digital and fiber technologies. The law passed in 1994, just before the Internet emerged as the dominant medium of communication. For that reason, CALEA did not apply to ISPs.

As the Internet grew in importance, the FBI became increasingly concerned about ISPs' exemption from CALEA and sought to extend the law to include the Internet. In 1999, in connection with its standards work on Voice over IP technologies, the IETF reputedly was asked by the FBI to redesign certain protocols to facilitate lawful intercept of Internet communications. In October 1999, the Internet Engineering Steering Group (IESG) opened a new email discussion

list, known as Raven, to encourage discussion of "the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping" (IESG, 1999). After months of intense exchanges, in which the technical community's general antipathy to government surveillance was evident, the IETF produced RFC 2804, "IETF Policy on Wiretapping" (IETF, 2000). RFC 2804 stated, "The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards."

The refusal came primarily from the IETF's status as a global standards developer: "The IETF, an international standards body, believes itself to be the wrong forum for designing protocol or equipment features that address needs arising from the laws of individual countries" (IETF, 2000, p. 1). A commitment to privacy (but not couched in the language of international human rights law) also played a role: "The IETF restates its strongly held belief, stated at greater length in [RFC 1984], that both commercial development of the Internet and adequate privacy for its users against illegal intrusion requires the wide availability of strong cryptographic technology" (IETF, 2000, p. 2).

The IETF's refusal to build surveillance capabilities desired by the United States into its fundamental standards did not, however, settle the matter. In 2004 the U.S. Department of Justice, FBI, and the Drug Enforcement Administration filed a joint petition with the Federal Communications Commission (FCC) asking it to expand CALEA to cover U.S. broadband providers, Voice over IP telephony, and instant messaging programs.[15] Privacy, civil liberties, and Internet freedom advocates all objected, but there was little support for their case in Congress and the FCC. Court challenges also failed. In 2005 the FCC adopted new rules implementing CALEA's extension to Internet services in the United States.[16] The United States is not alone in requiring ISPs to implement wiretapping, ISPs in most other countries (e.g., in the European Union) are also required to implement lawful intercept. In the post-9/11 environment, surveillance won out over privacy politically, regardless of the IETF's standards. Retrospectively, some have argued that the IETF's refusal to standardize lawful interception simply pushed the governmental intervention into other forums. Others think they made the right choice.

Looking at this case, we see no supremacy of code, law, or markets. The refusal of the IETF to re-architect its standards did not safeguard human rights, as the legislative and regulatory power of the state was used to reshape Internet privacy policy through other means. On the other hand, the global scope of IETF and the Internet, the rise and liberalization of encryption technologies, privacy movements, and the distributed authority over the Internet provided and continue to provide a countervailing force. The technical reconfigurations are part of a broader political struggle involving stakeholders from industry, civil society groups, consumers and public safety, intelligence, and law enforcement agencies. That struggle continues to this day.

Case 2: TLS 1.3

Transport Layer Security Protocol (TLS) is one of the most important protocols affecting security on the Internet. It can be used to cryptographically

protect Internet communications such as online banking, email traffic, and web browsing. The current standard (TLS version 1.2) was defined by the IETF in RFC 5246, 2008.[17] TLS 1.2 was less secure than some thought it should be because it lacked the property known as forward secrecy, which practically eliminates the ability of any third party to snoop on the traffic. Some law enforcement or intelligence agencies are not in favor of forward secrecy, for obvious reasons. Less obviously, some large enterprise network operators realized that forward secrecy would reduce their ability to inspect traffic for the purpose of troubleshooting problems within their own networks. They want to be able to decrypt traffic that is inside their networks. So they asked the TLS WG to restore some of the removed cipher suites or provide some other mechanism to support their internal network requirements (Checkoway, 2017; see also Adrian et al., 2015).

The new 1.3 TLS standard thus posed a dilemma for the IETF. Privacy/security and HR advocates believe that forward secrecy should be a requirement of the new standard. They oppose any effort to dilute it. Building forward secrecy into the standard will do more to protect end user privacy, assuming the standard is widely adopted. IETF approved the protocol in March 2018.[18] In doing so, it has clearly made a value judgment—that the security of individual end users is more important than the interests of intelligence and law enforcement agencies who might want to compromise or limit the security of the standard, and more important than enterprise network stakeholders' desire for a standard that enhances their ability to monitor and manage their internal networks.

That choice is only part of the story, however; merely the first step in a sequence of actions and reactions. The enterprise network stakeholders could get what they want by continuing to use the older version of TLS 1.2. Thus, the stronger security of TLS 1.3 might strengthen the privacy of those who adopt it, but limit its adoption by certain parties. Also, a refusal to put the requested capabilities into the new standard might have some ill effects on the global compatibility of the Internet, as Checkoway (2017) notes:

> whether or not enterprise network operators really need the decryption capability, some of them really want it. And since they really want it, they're going to do *something* to get it. It's strictly better for the mechanism to be designed in public, following normal IETF procedures, than to be cobbled together by people whose focus is on operations and not, necessarily, on security.

So by making that values choice, the IETF does not prevent other actors from making other arrangements. Indeed, the choice also can lead to a kind of forum-shopping among standards development organizations. Another standards development organization, the Institute of Electrical and Electronics Engineers (IEEE), has a working group that is tasked with developing a version of TLS called "multi-context TLS." It would allow negotiated third parties to look into encrypted traffic. This IEEE group seems to have arisen as an alternative for stakeholders who fear they may not get what they want out

of the IETF process. So the power of the IETF's choice is limited potentially by other sources of standards development.

Analysis of the Cases

In both of these cases, we see political and economic contention among stakeholder groups as the key factor shaping the definition and exercise of rights. While standards and designs shape the social environment, they are also shaped by it. It is a mistake to look at code, standards, and designs as an intentional and exogenous source of leverage on human rights. Standards and protocols are produced in a political, economic, and institutional context by actors with specific incentives, objectives, and constraints. This is more in line with the "architecture mediates rights" perspective in theory, but even that theory tends to understate the role of economic incentives.

Most code is created in and for the market economy, and the incentives that drive its production are set by the market (Brown & Marsden, 2013). Likewise, there are numerous instances when the code and architecture of the cyber environment were and are being altered through politics, regulation, legislation, and judicial decisions. Law can supersede code and often does (Asscher & Dommering, 2006). It is true that technological change alters the parameters of policy discourse and can dramatically shift the cost structure of enforcing laws and policies, leading to disruptive change. But when this happens, it usually happens unpredictably and unintentionally; there is no simple linear relationship in which protocol standards dictate society's rules. Technical standards and designs are embedded within this broader political economy environment.

In general, the HR movement in IETF, the code is law school, and the VID movement vastly overstate the role of intentional design in shaping society. Adherents could benefit from a strong dose of F.A. Hayek's theories regarding the role of dispersed knowledge, distributed decision making, and price signals in governing social outcomes (Hayek, 1945). The price system interacts with institutions and political systems to aggregate the choices and preferences of a diverse population into specific outcomes. The results are the product of human action but not the result of human design. Similarly, law and politics shape technology as well as vice versa.

Logically, these cases do not prove inductively that our political economy approach to understanding the relationship between technology design and human rights is generally true; but they do refute the stronger claims of "code is law" and "values in design" adherents. The cases provide existence proofs of how the relationship between rights and standards do not conform to the code is law or VID models.

Conclusion

This article hopes to stimulate a more nuanced and productive debate about the role of Internet protocols and standards in governance. It differentiates

between three distinct positions on the relationship between human rights and Internet standards and architecture: a stronger "code is law" claim, a claim that Internet architecture or infrastructure "mediate" human rights, and a "values in design" claim that technical design embodies or promotes specific values.

We argue that code is not law. Economic incentives, laws, and policies can and often do supersede, reverse, or dictate design and the designers' intentions. Embedding human rights into the design of Internet architecture is not possible for a number of reasons. The enumerated rights can conflict among themselves, and acts of balancing and proportionality are outside the scope of technical standards. *Ex ante* predictions of whether or how a design affects rights in the future is not always possible. Focusing on Internet architecture and the design of protocols is not the solution to many Internet human rights violations.

Insofar as the HR advocates present a nuanced and accurate picture of the relationship between technology and society, they emphasize reciprocal influence and complex forms of interdependence among varying interests and stakeholders (the architecture mediates rights view). But this appreciation undermines the argument that designing protocols can secure human rights. In this view, protocols are artifacts reflecting how society works, and perhaps in some ways reinforcing the forces that put it into place. This kind of scholarly literature provides no support whatsoever for the belief that protocol designers have a kind of Archimedean leverage point with which to move the world.

We do agree that Internet architecture is an important part of the broader Internet governance landscape. Struggles over rights and user interests often do take place over the configuration of Internet infrastructure and protocol or architectural design. But we are puzzled by the overemphasis on the standardization or design process among scholars and advocates. Prioritizing Internet architecture and its design for advancing rights is not justified since other actors' roles are equally if not more important. We conclude that the dream that one can find novel ways to advance human rights through Internet architecture or standards is a false one. Puncturing this dream serves important purposes. It prevents HR advocates from misdirecting their resources, and calls attention to issues that have been ignored if one focuses exclusively on Internet architecture and standards.

Milton L. Mueller, Ph.D., Professor, Georgia Institute of Technology—School of Public Policy, Atlanta, Georgia.

Farzaneh Badiei, Ph.D., Research Associate, Georgia Institute of Technology—School of Public Policy, Atlanta, Georgia [farzi@gatech.edu].

Notes

1. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on April 16, 2014 at the 1197th meeting of the Ministers' Deputies).

2. The specific meetings observed were ICANN 55 (Marrakech), IETF 96 (Berlin), ICANN 57 (Hyderabad), IETF 98 (Chicago), and IETF 99 (Prague).
3. Note that in this formulation, Lessig blurs the distinction between public and private actors. AOL may indeed be able to regulate behavior within its own platform through code and architecture, but nothing compels anyone to use that platform, and there may be other platforms available with different rules.
4. By this definition, it would literally be impossible for technology to be "neutral" because "neutrality" would mean that design would impose zero constraints on its users.
5. See, for example, Knobel and Bowker (2011, p. 26) talk about "reconciling" national security and privacy values through a "compromise design," and mention "cultural valence," the idea that "systems designed by one group (e.g., Americans) should not impose American values. . ."
6. Nissenbaum, H. Principal Investigator. *EAGER: Values in Design in the Future Internet Architecture.* http://www.nyu.edu/projects/nissenbaum/EAGER.html.
7. IETF 98 Plenary Minutes, see https://datatracker.ietf.org/meeting/98/materials/minutes-98-ietf-201703291530.
8. Charter of the Human Rights Protocol Considerations working group. https://irtf.org/hrpc. The IRTF HRPC is a document which is work in progress and subject to change.
9. As DeNardis (2009, p. 10) puts it: "As sites of control over technology, the decisions embedded within protocols embed values and reflect the socioeconomic and political interests of protocol developers." Cath and Floridi (2017, p. 458) explain that: "There are many ways to protect human rights, one of which is to ensure that Internet protocols and standards are encoded with privacy requirements, like encryption." Or they say sometimes even that values are "baked in" to architecture: "We have seen that the IETF does indeed enable—and some times even "bakes in"—particular values through the Internet's architecture"(Cath & Floridi, 2017, p. 460).
10. RFC 6973 (2013) and RFC 7258 (2014). https://datatracker.ietf.org/doc/rfc7258/.
11. "Human rights can be in conflict with each other, such as the right to freedom of expression and the right to privacy. In such cases the different affected rights need to be balanced. In order to do this it is crucial that the rights impacts are clearly documented in order to mitigate the potential harm. Making that process tangible and practical for protocol developers is what this research aims to ultimately contribute to. Technology can never be fully equated with a human right. Whereas a specific technology might be strong enabler of a specific human right, it might have an adverse impact on another human right. In this case decisions on design and deployment need to take this into account."[#] (IRTF, 2017, p. 3).
12. https://tools.ietf.org/html/draft-varon-hrpc-methodology-00. This document was solely informational and expired in 2016.
13. Quotes from a live video of the IETF 98 Combined Technical and Administrative Plenary, March 29, 2017. https://www.youtube.com/watch?v=qvgIX3-pAZE&t=3870s.
14. "Note that even when these goals are achieved, the existence of items of interest – attributes, identifiers, identities, communications, actions (such as the sending or receiving of communication), or anything else an attacker or observer might be interested in – may still be detectable, even if they are not readable. Thus, undetectability, in which an observer or attacker cannot sufficiently distinguish whether an item of interest exists or not, may be considered as a further security goal (albeit one that can be extremely difficult to accomplish)" RFC 6973 (IETF, 2013, p. 21).
15. Electronic Frontier Foundation, FAQ on CALEA. https://www.eff.org/issues/calea.
16. The FCC required Internet Broadband providers and Voice over IP providers to comply with CALEA. It requests that such providers "have the necessary surveillance capabilities to comply with legal requests for information. Communications services and facilities utilizing Circuit Mode equipment, packet mode equipment, facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service are all subject to CALEA. These compliance requirements include wireless services, routing and soft switched services, and internet-based telecommunications present in applications used by telecommunications devices." See https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.
17. https://www.ietf.org/rfc/rfc5246.txt.
18. https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html. The protocol was published as an RFC in August 2018: https://tools.ietf.org/html/rfc8446.

References

Adrian, D., K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J.A. Halderman, N. Heninger et al. 2015. "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice." In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. New York: ACM, 5–17.

Allen, J.H. 2001. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley.

Asscher, L., and E. Dommering. 2006. "Code: Further Research." In *Information Technology and Law Series*, eds. E. Dommering and L. Asscher. The Hague: T.M.C. Asser Press, 249–55.

Bélanger, F., and R.E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4): 1017–42.

Bendrath, R., and M. Mueller. 2011. "The End of the Net as We Know It? Deep Packet Inspection and Internet Governance." *New Media and Society* 13 (7): 1142–60.

Bridy, A. 2010. "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement." *Oregon Law Review* 89: 81–132.

Brown, I., D.D. Clark, and D. Trossen. 2010. "Should Specific Values Be Embedded in the Internet Architecture?" In *Proceedings of the Re-Architecting the Internet Workshop on—ReARCH '10*. https://doi.org/10.1145/1921233.1921246.

Brown, I., and C.T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, MA: MIT Press.

Cath, C., and L. Floridi. 2017. "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights." *Science and Engineering Ethics* 23 (2): 449–68.

Cavoukian, A. 2011. *Privacy by Design, the 7 Foundational Principles*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Checkoway, S. 2017. "TLS 1.3 in Enterprise Networks." *Blog Post*. https://www.cs.uic.edu/~s/musings/tls13-enterprises/.

DeNardis, L. 2009. *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.

DeNardis, L. 2010. "The Emerging Field of Internet Governance." *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343.

DeNardis, L., and A.M. Hackl. 2016. "Internet Control Points as LGBT Rights Mediation." *Information, Communication and Society* 19 (6): 753–70.

DeNardis, L. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

Dommering, E., 2006. "Regulating Technology: Code Is Not Law." In *Information Technology and Law Series*, eds. E. Dommering and L. Asscher. The Hague: T.M.C. Asser Press, 1–16.

Flanagan, M., D.C. Howe, and H. Nissenbaum. 2008. "Embodying Values in Technology: Theory and Practice." In *Information Technology and Moral Philosophy*, eds. J. van den Hoven and J. Weckert. Cambridge: Cambridge University Press, 322.

Garfinkel, S. 1995. *PGP: Pretty Good Privacy*. Sebastopol, CA: O'Reilly Media, Inc.

Graber, C.B. 2012. "Internet Creativity, Communicative Freedom and a Constitutional Rights Theory Response to 'Code Is Law.'" *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1737630.

Hayek, F.A. 1945. "The Use of Knowledge in Society." *American Economic Review* 35 (4): 519–30.

Hick, S., E. Halpin, and E. Hoskins, eds. 2016. *Human Rights and the Internet*. New York: Springer.

Internet Engineering Steering Group (IESG). 1999. *[Raven] The IETF's Position on Technology to Support Legal Intercept*. October 11. https://www.ietf.org/mail-archive/web/raven/current/msg00000.html.

IETF. 2000. *IETF Policy on Wiretapping. Request for Comments 2804 (Informational)*. May. https://tools.ietf.org/html/rfc2804.

IETF. 2005. *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. December. https://tools.ietf.org/html/rfc4307.

IETF. 2013. *Privacy Considerations for Internet Protocols, Request for Comments 6973*. https://tools.ietf.org/html/rfc6973.

IRTF. 2017. *Human Rights Protocol Considerations Charter*. https://datatracker.ietf.org/rg/hrpc/about/.

Jørgensen, R.F., and A.M. Pedersen. 2017. "Online Service Providers as Human Rights Arbiters." In *The Responsibilities of Online Service Providers*. New York: Springer International Publishing, 179–99.

Knobel, C., and G. Bowker. 2011. "Values in Design." *Communications of the ACM* 54 (7): 26–8.

Koops, B.J. 2008. "Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values." In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, ed. Y. Brownsword. Sydney: Bloomsbury Publishing.

Koops, B.J., and R. Leenes. 2014. "Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law." *International Review of Law, Computers & Technology* 28 (2): 159–71.

Layton, T.P. 2007. *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach Publications.

Lessig, L. 1999a. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L. 1999b. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113 (2): 501.

Lessig, L. 2002. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Vintage.

Lessig, L. 2006. *Code*. New York: Basic Books.

Manders-Huits, N. 2011. "What Values in Design? The Challenge of Incorporating Moral Values Into Design." *Science and Engineering Ethics* 17 (2): 271–87.

Mayer-Schonberger, V. 2000. "Impeach the Internet." *Loyola Law Review* 46: 569–601.

Milan, S., and N. ten Oever. 2017. "Coding and Encoding Rights in Internet Infrastructure." *Internet Policy Review* 6 (1). https://policyreview.info/articles/analysis/coding-and-encoding-rights-internet-infrastructure.

Mitchell, W.J. 1996. *City of Bits: Space, Place, and the Infobahn*. Cambridge, MA: MIT Press.

Mumford, L. 1934. *Technics and Civilization*. London: Harcourt.

Musiani, F. 2012. "Caring About the Plumbing: On the Importance of Architectures in Social Studies of (Peer-to-Peer) Technology." *Journal of Peer Production* 1: 8.

Musiani, F. 2013. "Network Architecture as Internet Governance." *Internet Policy Review* 2 (4). https://policyreview.info/articles/analysis/network-architecture-internet-governance.

Musiani, F. 2016. "Alternative Technologies as Alternative Institutions: The Case of the Domain Name System." In *The Turn to Infrastructure in Internet Governance*, eds. L. Musiani, D.L. Cogburn, L. DeNardis, and N.S. Levinson. New York: Palgrave MacMillan, 73–86.

Musiani, F., D.L. Cogburn, L. DeNardis, and N.S. Levinson. 2016. *The Turn to Infrastructure in Internet Governance*. New York: Palgrave MacMillan.

Nissenbaum, H. 2001. "How Computer Systems Embody Values." *Computer* 34 (3): 120–19. https://ieeexplore.ieee.org/document/910905.

Nunziato, D.C. 2000. "Exit, Voice, and Values on the Net." *Berkeley Technology Law Journal* 34: 753–75.

OECD. 2011. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm.

Postel, J., and J. Reynolds. 1997. *Instructions to RFC Authors, RFC 2223*. October. https://tools.ietf.org/html/rfc2223.

Reidenberg, J.R. 1997. "Lex Informatica: The Formulation of Information Policy Rules Through Technology." *Texas Law Review* 76: 553.

Rubinstein, I.S. 2011. "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26 (3): 1409–56.

Saltzer, J., D. Reed, and D. Clark. 1984. "End to End Arguments in System Design." *ACM Transactions in Computer Systems* 2 (4): 277–88.

Tien, L. 2005. "Architectural Regulation and the Evolution of Social Norms." *Yale Journal of Law & Technology* 7: 1.

Tusikov, N. 2016. *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.

UN Human Rights Council. 2016. Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/32/L.20. http://digitallibrary.un.org/record/845728?ln=en.

Winner, L. 1986. *Do Artifacts Have Politics? The Whale and the Reactor*. Chicago: The University of Chicago Press, 19–39.

Yeung, K. 2008. "Towards an Understanding of Regulation by Design." In *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, eds. R. Brownsword and K. Yeung. Oxford: Hart Publishing, 79–107.