The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights

Corinne Cath[1] · **Luciano Floridi**[1]

Abstract The debate on whether and how the Internet can protect and foster human rights has become a defining issue of our time. This debate often focuses on Internet governance from a *regulatory perspective*, underestimating the influence and power of the governance of the Internet's *architecture*. The technical decisions made by Internet Standard Developing Organisations (SDOs) that build and maintain the technical infrastructure of the Internet influences how information flows. They rearrange the shape of the technically mediated public sphere, including which rights it protects and which practices it enables. In this article, we contribute to the debate on SDOs' ethical responsibility to bring their work in line with human rights. We defend three theses. First, SDOs' work is inherently political. Second, the Internet Engineering Task Force (IETF), one of the most influential SDOs, has a moral obligation to ensure its work is coherent with, and fosters, human rights. Third, the IETF should enable the actualisation of human rights through the protocols and standards it designs by implementing a responsibility-by-design approach to engineering. We conclude by presenting some initial recommendations on how to ensure that work carried out by the IETF may enable human rights.

Keywords Human rights · Information ethics · Internet architecture · Internet Engineering Task Force · Internet governance · Responsibility-by-design · Standard Developing Organisations · Protocols · Right to freedom of expression · Privacy · Standards · Values-by-design

✉ Corinne Cath
corinnecath@gmail.com

[1] Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK

Introduction

The debate on whether and how the Internet can enable and foster human rights has become a defining issue of our time. The growing impact of the Internet on human life means that its technical architecture—that is, its standards and protocols[1]—is increasingly important to this debate, as it determines how information travels across the world, who or what is able to connect with whom or what, and in which ways. This creates the need to ensure that the decisions and choices guiding the design[2] of the Internet's architecture are in line with the United Nations Universal Declaration of Human Rights (UDHR). Questions at the intersection of human rights, ethics and Internet architecture management are particularly important as Internet Standard Developing Organisations (SDOs) are increasingly becoming arenas for tussles over value-sensitive design, and the moral as well as legal responsibility of technologists to protect human rights-by-design (Brown et al. 2010; Clark et al. 2005; Denardis 2013, 2014; Lessig 2006; Post 2015; Rachovitsa 2015). In this article, we intend to contribute to the current, broad debate on SDOs' ethical responsibility to ensure their work enables the actualisation of human rights. We shall address the specific question of whether human rights should be instantiated in the protocols and standards designed by the Internet Engineering Task Force (IETF). Our focus is on the IETF because it is one of the most influential SDOs, capable of making the most significant difference in the architectural implementation of values or human rights (Liddicoat and Doria 2012; Davidson and Morris 2003).

In order to answer the previous question, this article is structured in six sections. In section one "Overview of the Current Debate and Outline of Research Methodology", we provide a brief overview of the current debate. In section two, we outline the "Methodology". In section three "Architectural Values?", we analyse the underlying normative framework that drives technological design decisions made by IETF engineers, and the role played in this context by the engineers' personal ethics. In section four "Responsibility-by-Design", we consider how values enter IETF protocols, and how this enables or constrains specific value-sensitive design decisions. In section five "The IETF's Ethical Responsibility", we address the IETF's responsibility towards human rights, and what obstacles its exercise may encounter when trying to instantiate specific human rights in the Internet's architecture. In the course of the article, we shall provide an in-depth and emic analysis of the normative framework that shapes many technical decisions of IETF engineers, and the IETF's responsibility vis-à-vis human rights. This analysis

[1] It is important to clarify the difference between *standards* and *protocols*. *Standards* enable diverse systems to communicate with each other, making possible interoperability of pieces of different software and hardware made by different vendors. *Protocols* are 'a set of recommendations and rules that outline specific technical standards' (Galloway 2004:7). In this article we use the overarching term "Internet's architecture" in order to refer to both standards and protocols and avoid unnecessary digression. For a good introduction to Internet's architecture, defined as a shortcut for internet standards and protocols, in their turn defined on the basis of the internet protocol suite see Hall, Eric A. 2000. *Internet Core Protocols: The Definitive Guide*—Foreword by Vincent Cerf. Beijing; Farnham: O'Reilly.

[2] On the philosophical importance of design see (Floridi 2011).

is based on data gathered through qualitative interviews, participant observation and discourse analysis (more on the methodology in section two). We hope that this article will further the academic and policy discussion on the role of SDOs in implementing value-sensitive design aimed at the implementation of human rights principles. To this end, we outline some "Policy Recommendations" in the sixth and concluding section.

Overview of the Current Debate and Outline of Research Methodology

As the Internet becomes more globalised, and increasingly impacts all aspects of society (particularly in the Global North), understanding who has the power to decide how the Internet's architecture is managed becomes evermore important (Lessig 2006; Mueller 2004, 2010; Zittrain 2008). The academics initially involved in the creation of the Internet built it on the following set of core technical principles: *openness*, *interoperability*, *redundancy*, and the *end-to-end principle* (Baran 1964; Clark 1988; Clark et al. 2005; Kurose and Ross 2007). It can be argued that these four principles are at the base of the success of the Internet. Yet, non-technical actors and values have consistently influenced the Internet's architecture management (Abbate 2000; Denardis 2014; Lessig 2006). As such, the technology that makes up the Internet's architecture has never been neutral (Abbate 2000; Brown et al. 2010; Busch 2011; Denardis 2014; Franklin 1999; Galloway 2004; Winner 1977). It follows that it is crucial to understand much better the normative frameworks underlying the design choices behind the technical decisions taken by engineers. These decisions influence the creation of protocols and standards, which in turn determine how the Internet may or may not be experienced by end-users (Abbate 2000; Denardis 2015) and to what extent their fundamental human rights may be protected and fostered. To quote Brown et al.:

> Our discipline's objectives in evaluating design choices needs to widen from the narrow performance evaluation that many research efforts are still focusing on, towards the larger socio-economic impact that some choices will have (2010:4).

We agree. Indeed, in the rest of this article we shall argue in favour of an even more inclusive approach, which also covers the potential impact of the design of the Internet's architecture on human rights, by promoting what we refer to as 'responsibility-by-design'. We adopt this term from Sweet and Schneier (2013) and Sweet et al. (2015), in order to refer to the practice of assuming a responsible attitude towards the potential impact of technology on human rights, in a standardized and institutionalized way.

Political and legislative bodies are increasingly codifying the link between human rights and the Internet. Important documents include: the 2012 UN Human Rights Council on 'Internet Free Speech',[3] which codified that rights apply online as

[3] For details see: https://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech/.

they do offline; the 2013 UN General Assembly resolution, which affirmed 'the right to privacy in the digital age'[4]; the 2003 World Summit on the Information Society (WSIS)[5]—one of the first summits to include in its Declaration of Principles the link between the information society and human rights; and the 2014 Netmundial Initiative (NMI)[6] outcome document, that declared that 'human rights should underpin Internet governance principles'.[7] Many different political entities and lawmakers have codified the relationship between the Internet and human rights, to ensure that the Internet remains a human rights enabling medium. These debates on how to safeguard human rights on the Internet often focus on regulatory and legal perspectives, but neglect the influence and power of the governance of the Internet's architecture.

Part of the difficulty is that instantiating human rights in Internet protocols is very challenging (Rachovitsa 2015; Bless and Orwat 2016). The problems encountered when attempting to do so are indicative of the larger issues surrounding value-sensitive design: its technical feasibility (Clark et al. 2005), the SDO's legitimacy to act as a 'lawmakers' (Lessig 2006), and the nature of human rights.

Human rights are not absolute in the legal sense of being 'global black letter law'. The UDHR is part and parcel of most legal systems, but is interpreted locally (Brysk 2002). This presents some difficulties, when trying to decide how to instantiate human rights principles in Internet protocols and standards that work globally and in a context-independent way. This process is further complicated by the fundamentally different approach governments take to defining important concepts (Abrams 1998). Socio-politically, policy makers tend to define concepts like human rights broadly and flexibly, in order to establish and maintain consensus and interactions. However, technically, engineers need to define the same concepts narrowly and rigidly, to establish and maintain communication and interoperability (Kurose and Ross 2007). These issues present real barriers to instantiating human rights using protocols. Additionally, whereas governments have clearly defined obligations and responsibilities vis-à-vis human rights, such obligations are much less clear for non-state actors. This creates the sense that a right cannot be granted, enabled or applied for unless and until a corresponding responsibility or obligation is defined and accepted.

[4] For details see: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

[5] A two-phase UN summit on the information society, held in 2003 in Geneva and in Tunis in 2005, with the aim of 'developing and fostering a clear statement of political will and taking concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. (…) Putting Geneva's Plan of Action into motion as well as finding solutions and reaching agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents.' For more information see: https://www.itu.int/net/wsis/basic/about.html.

[6] The Netmundial Initiative (NMI) aims to 'provide a platform that helps catalyse practical cooperation between all stakeholders in order to address Internet issues and advance the implementation of the NETmundial Principles and Roadmap.' This roadmap was created during a one time meeting, held April 2014 in Brazil. It brought together over 1400 stakeholders from almost 100 countries and all different sectors to tackle various Internet governance challenges. For more information see: https://www.netmundial.org/.

[7] For full Netmundial Initiative (NMI) outcome document see: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

These difficulties would be less pressing if the IETF had the legitimacy to make or interpret laws. Since this is not the case, Lessig is right in stressing the problems surrounding a shift of power from legal systems to code (2006). He argues that, when technological artefacts constrain our behaviour, the processes shaping these behaviours ought to be legitimised by the people subject to them. This is not currently the case with the IETF, nor is this necessarily a desirable situation, in addition to being hard to achieve considering its informal status (Galloway 2004). Finally, even if the IETF were to gain the legitimacy necessary to protect human rights, and decided to enable these through Internet standards and protocols, there is a real risk of (further) Internet fragmentation:

> When governments become sufficiently frustrated with the way standards are being designed, or find that the existing standards process no longer serves their national economic or security interests, then we might see a large country like China, or a coalition of countries, decide to abandon the current standards process, effectively cleaving the Internet at the logical layer (Hill 2013:36).

This leaves the IETF in a difficult predicament. On the one hand, it does not have the legitimacy to enable (or protect) human rights, yet in the past it has already made decisions to that effect. On the other hand, when the IETF does not emphasise the importance of its technology for human rights, it risks implicitly condoning uses of the Internet that enable political and economic developments that are geared towards a less open and accessible Internet. This would mean moving away from the Internet as defined by the four fundamental architectural principles, *openness*, *interoperability*, *redundancy*, and the *end-to-end principle*. Yet, if the IETF does actively instantiate particular human rights into the Internet's architecture, this can result in further fragmentation, which undermines connectivity, the main goal of the IETF, as will be argued here.

In response to these challenges, we found that the IETF has developed a strategy of responding to value-sensitive and human rights-by-design questions in technical terms, and by pursuing the discussion when there is limited commercial or political push-back as will be detailed throughout the paper. By adopting such a pragmatic approach, the IETF is implicitly acknowledging that, lacking the legitimacy to protect human rights, it also cannot be held responsible for the negative repercussions of its work on human rights. However, the IETF's realpolitik approach may not be easily defensible, as will be shown in this article.

The influence of commercial and political forces on the management of the Internet's architecture is well documented in the academic literature and need not be rehearsed here (Benkler 2006; Berkman Center Report 2016; Brown et al. 2010; Denardis 2014; Lessig 2006; Mueller 2004; Zittrain 2008). Suffice it to say that the IETF tries to push back against developments that lead to the standardisation of surveillance and other issues that may negatively influence end-users' experience of the Internet (Denardis 2014, 2015). Much more interesting is the relatively unchartered territory of the role that societal values—in particular human rights—can and should play in the design, management and development of the Internet's architecture. In this context, it is possible to identify two main positions in the academic debate. Both are normative rather than descriptive because both focus on the question of whether particular societal values *should* be followed when designing protocols. On the one hand, Clark et al. argue that there is a need for 'tussle', meaning that engineers need to:

> Design for variation in outcome, so that the outcome can be different in different places, and the tussle takes place within the design (…) [as] Rigid designs will be broken; designs that permit variation will flex under pressure and survive (2005:2).

On the other hand, Brown et al. argue that:

> Some key, universal values—of which the UDHR is the most legitimate expression—should be baked into the architecture at design time (2010:3).

In this article, we shall discuss the 'tussle theory' suggested by Clark et al. (2005) and add further complexity to the 'baking-in theory supported by Brown et al. (2010). These theories are important because they pinpoint the tension in the debate, namely whether protocols and standards made by SDOs, should be used to enable the actualisation of human rights. Many authors have tangentially touched upon these issues (Abbate 2000; Denardis 2015; Lessig 2006; Rabkin et al. 2010), however the articles by Clark et al. (2005) and Brown et al. (2010) fully define the problem.

Currently, there are only a limited number of case studies that examine both positions in-depth (Bless and Orwat 2016; Denardis 2015; Thompson 2013; Rachovitsa 2015; Rabkin et al. 2010). This shortcoming was among the initial motivations for this research. Filling this knowledge gap is important not only because protocols and standards shape the Internet, but also because the software and hardware that define the infrastructure of cyberspace are increasingly perceived to have the same power in society as law (Lessig 2006), but they are not measured or developed by the same standards as other legal instruments for enabling human rights.

Arguably, if code is law, then protocols and standards should be brought more in line with the existing bodies of law of the offline world (Brown et al. 2010; Dutton 2011; OHCHR 2015; UNESCO 2015). As shown earlier, technology is not neutral. Technology, by its very nature, is inherently connected to the practices of its use (Busch 2011; Franklin 1999; Galloway 2004; Winner 1977). Such practices are embedded in culture, which means that technology cannot be detached from the context in which it is applied and, by extension, its ethical and legal principles. Considering the global nature of the Internet, and the many different contexts and cultures it permeates, the most relevant ethical and legal framework to be upheld by those designing its structure is the United Nations Declaration of Human Rights (UDHR). It is the basis of a plethora of international, national, and regional laws aimed at protecting and promoting fundamental human rights (Brysk 2002). Several of these rights have a clear online application, such as freedom of expression and assembly (Dutton 2011; UNESCO 2015). Indeed, one may argue that the Internet has become one of the primary media through which opinions can be expressed, not least because of its widespread diffusion, low costs, and interactivity. So, it is not surprising that there has been an increased call for value-sensitive Internet design that takes into account human rights (Cavoukian 2009; Denardis 2015; OHCHR 2014; OHCHR 2015; Post 2015; Rachovitsa 2015). These calls hold that code can—and should—be used to protect particular societal values like human rights. However, the focus is mostly on privacy (Doty 2015; Rabkin et al. 2010). And the language remains vague, not specifying how human rights should enter the engineering process. As anticipated, this article will attempt to address this issue within the context of the Internet Engineering Task Force (IETF). But first, let us clarify the methodology we adopted. The reader interested only in the results may wish to skip the following section.

Methodology

This research used a mixed-methods approach to collecting and analysing data. Initially, data were gathered using a simple Python-based content analyser from primary sources such as IETF mailing lists, Requests for Comments[8] (RFCs), and video and audio content generated by the IETF. This was also used to collect secondary sources, such as academic publications and articles in the press. In total, over 200 documents and 40 video and audio recordings were collected and analysed for various keywords. This stage of the research was informed by the methodological approach to discourse analysis as laid out by Jabri (1996) and Demmers (2012). The insights from the qualitative analysis were used for the semi-structured interviews and participant observation, which took place in the period between the 92nd IETF and 93rd conference of the IETF in 2015. A total of 30 interviews were conducted. The participants were selected through purposive sampling (Babbie 2010:184). The interviewees included individuals in leadership positions [Working Group (WG) chairs, Area Directors (ADs)], 'regular participants', and individuals working for specific entities (corporate, civil society, political, academic), and represented various backgrounds, nationalities and genders.

This research method and design is limited by the potential biases of the interviewees, the researchers (Richie and Lewis 2003), and the sampling method (Creswell 2013). To ensure the conclusions drawn on the basis of the different interviews did not over-represent some views, the data were triangulated (Harvey 2011) with the findings of the discourse analysis, the literature review, and participant observation.[9] It has been argued that the findings so obtained are at best 'partial', and at worst 'partisan' (Denzin and Lincoln 2000). However, as Denzin and Lincoln (2000) also detail, there are many advantages to collecting a substantial amount of data on a limited number of cases instead of limited data on many cases. And such data are often used as the base for quantitative research (Richie and Lewis 2003) and to encourage further research (Blee and Taylor 2002).

[8] The official IETF working documents that describe Internet specifications, communications protocols, procedures and other IETF related issues.

[9] We follow Richards (2009), according to which data triangulation mitigates some of the issues surrounding 'double hermeneutics', as well as purposive sampling, inherent to this research.

In the following sections, we shall present our results in detail. In a nutshell, the analysis performed on the data gathered presented various distinct but interrelated results. First, it became evident that the four architectural design principles on which the Internet is built are based upon a normative understanding of what the Internet *should* be and *should* do. Second, this normative understanding is largely in line with the 'Western' notion of the Internet as a connectivity-enabling platform for freedom of expression. Third, the particular composition of the IETF participant base reinforces this normative understanding of the Internet. Jointly, these results showcase the normativity at the base of the creation of Internet protocols at the IETF and the overlap between protocols and human rights.

From the data, three conditions were extracted that need to be present in order for the IETF to enable human rights through protocols. These are crucial steps to answering questions about whether human rights should be embedded in protocols, the topic of the following sections.

Architectural Values?

As already mentioned, the Internet was built on the basis of four architectural principles—openness, interoperability, redundancy, and the end-to-end principle—which guide the IETF's work (Clark et al. 2005; Denardis 2014). They shape today's Internet because of their technical aptitude and because many at the IETF conceptualise the Internet as a fundamentally open, accessible platform for unhindered connectivity. Examining the IETF's guiding principles, like RFC 1958 'Architectural Principles of the Internet', further corroborates the existence of such an underlying normative conceptualisation of what the Internet is and should be. RFC 1958 states that:

> The current exponential growth of the network seems to show that connectivity is its own reward, and is more valuable than any individual application such as mail or the World-Wide Web. The key to global connectivity is the inter-networking layer.

The IETF strives to create an Internet that is a global network of networks that provides connectivity for all users and many diverse usages at any time. This particular conceptualisation of the Internet can also be seen in RFC 1958, which specifies the architectural principles of the Internet:

> The community believes that the goal is connectivity, the tool is the Internet Protocol (IP), and the intelligence is end-to-end rather than hidden in the network.

Both the technical and the social values that guide IETF engineers' design decisions are normative. When considering the alternative ways in which the Internet could have been built (per-pay-connectivity, proprietary protocols, limited nodes, and centralised intelligence) (Denardis 2015), it becomes clear that the IETF is focused on creating a particular Internet, a network with the fundamental goal of connectivity. This can also be seen in the mission statement of the IETF, which holds that:

> The Internet isn't value-neutral, and neither is the IETF. We want the Internet to be useful for communities that share our commitment to openness and fairness. We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community. These concepts have little to do with the technology that's possible, and much to do with the technology that we choose to create. (RFC 3935)

Personal values and ethics thus guide protocol development or, as Denardis 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 (Denardis 2013:10).

Considering the heavy presence in the IETF[10] of mostly male,[11] Western,[12] and white (first author's field notes) representatives of large companies,[13] their personal and ethical positions are often in line with the Western democratic popular understanding of the Internet as an allegedly democratising tool.

Although the IETF's architectural design principles are frequently presented as technical considerations, they also embody a socio-political conceptualisation of what many technical engineers view the Internet to be: a connectivity-enabling platform for free expression. This conceptualisation is further reified by the view that IETF participants are a relatively non-diverse group with a largely shared ethics towards Internet architecture management. According to Lessig 'the architecture of cyberspace is power in this sense; how could it be different. Politics is about how [and what] we decide. Politics is how that power is exercised, and by whom' (2006:59).

By upholding the four aforementioned technical principles, the IETF facilitates greater all-to-all connectivity (Davidson and Morris 2003). This, in its turn, increases the ability of individuals to communicate with each other and to express themselves in the digital age. Such open, secure and dependable connectivity is increasingly essential to the implementation of basic human rights (Dutton 2011; OHCHR 2011; OHCHR 2015; UNESCO 2015). Access to the Internet in itself is not (yet) a human right. However, as our society increasingly relies on the Internet for everything, including the ability to exercise human rights, it is important for the Internet's architecture to provide open, secure and dependable connectivity so

[10] The figures come from the IETF website. There are many flaws in the data visualizations. As the website states: The technical term that experts like to use for the level of quality achieved by this tool is "crap".' See http://www.arkko.com/tools/authorstats.html#quality The point, however, is that one does not need perfect data visualizations, as even these approximate figures support the conclusion that the IETF participant base is relatively homogenous.

[11] http://www.arkko.com/tools/rfcstats/genderdistrhist.html.

[12] http://www.arkko.com/tools/allstats/d-countryeudistr.html, http://www.arkko.com/tools/rfcstats/countrydistrhist.html.

[13] http://www.arkko.com/tools/rfcstats/companydistrhist.html.

people can exercise their rights. Clarifying this specific connection between the Internet's architecture and human rights and the normative conceptualization that underlies its standards and protocols is important, as it is crucial to understanding why and how—as will be argued later in the article—the IETF must ensure its work enables the actualisation of human rights.

Responsibility-by-Design

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 (Dutton 2011; UN OHCHR 2011, 2015; UNESCO 2015). The IETF has a long-standing history of taking privacy into account in protocol design (Denardis 2015). Privacy considerations, for instance, became an important part of the work, and hence of the Internet's architecture, following the 2013 Snowden revelations about the dangers of 'Pervasive Monitoring'. In the summer of 2013, various responses were drafted to deal with the impact of dragnet surveillance on the network. For instance, RFC 7258 'Pervasive Monitoring Is an Attack' states that:

> Current capabilities permit some actors to monitor content and metadata across the Internet at a scale never before seen. This pervasive monitoring is an attack on Internet privacy. The IETF will strive to produce specifications that mitigate against pervasive monitoring attacks.

RFC 7258 indicates that the IETF was aware of some of the monitoring going on, but did not see it as a significant threat to the network.[14] Revelations around the sheer scale of the monitoring, however, did deeply upset the IETF community, for two reasons. It presented a technical threat to the functioning of the network (Denardis 2015). And, we argue, it undermined the IETF's conceptualisation of the Internet (as explained earlier) by breaking some of its fundamental architectural principles.

In response, the IETF decided to enable a social value through protocols. This was done by developing 'privacy considerations'.[15] These provide guidelines for engineers developing protocols to ensure they have considered the potential impact of their work on privacy. Implementing these considerations is not mandatory but the end goal is to include the privacy considerations in the RFC. As such, they do not instantiate privacy in protocols but do allow the technology to enable the actualisation of the right to privacy.

However, the engineers approached the privacy breach as a technical attack that undermined trust in the network (see RFC 7258), not as a human rights issue. This technical approach to design decisions goes a long way toward explaining why many IETF engineers do not feel a moral obligation to ensure that their work has a positive impact on human rights (first author's interviews).

[14] For future details on how and why the monitoring was considered to be a threat see RFC 7258 "Pervasive Monitoring is an attack https://tools.ietf.org/html/rfc7258.

[15] See RFC 6973 Privacy Considerations for Internet Protocols https://tools.ietf.org/html/rfc6973.

By taking strong stances on issues like privacy after the Snowden revelations in 2013—a value that has both technical and human rights properties—the IETF enables the expression of values through protocols. This is not to say that the IETF is always able to do so. The IETF's ability to enable the promotion of values, both in designing specifications and in the actual running of the code, is mediated by contextual factors, like political and market dynamics. Sometimes, these align with views held by IETF engineers on the fundamental nature of the Internet, but sometimes they diverge. If the IETF lacks a strong technical justification for enabling a particular value through protocols, it is often pressured to follow the market or political dynamics (Berkman Center Report 2016; Lessig 2006) that might move away from issues like privacy or security.

An example of how values can get 'baked into' the design is the discussion on status code 451,[16] which peaked in 2015. As surveillance and censorship of the Internet became more commonplace, voices were raised at the IETF to introduce a new status code that indicates when something is not available for 'legal reasons' like censorship. The status code, which has recently been approved by the Internet Engineering Steering Group (IESG), is named '451', a reference to Bradbury's famous novel on censorship, *Fahrenheit 451*.[17] In practice the code looks like this (Fig. 1).

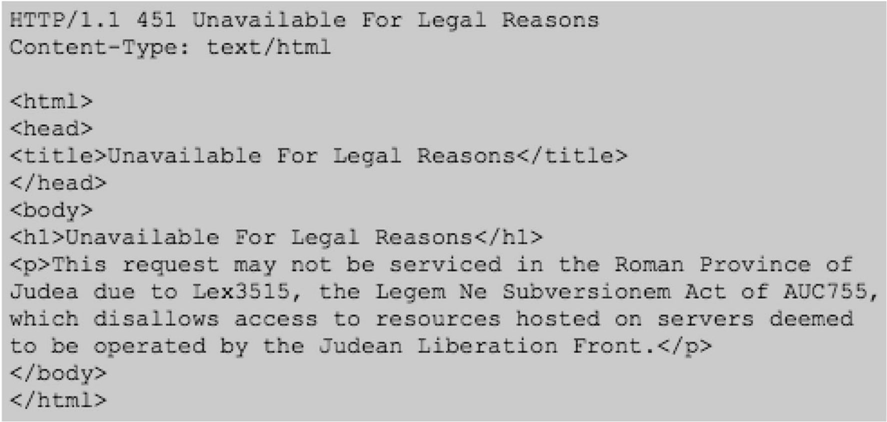
During the 2015 IETF meeting in Dallas, there was discussion about the usefulness of '451'. The main tension revolved around the lack of an apparent machine-readable technical use of the information. The extent to which '451' is just 'political theatre' or whether it has a concrete technical use was the object of heated debated. Some argued[18] that 'the 451 status code is just a status code with a response body' others said it was problematic because 'it brings law into the picture'. Again others argued that it would be useful for individuals, or organisations like the 'Chilling Effects' project, who are crawling the web to get an indication of censorship (IETF discussion on '451'—first author's field notes March 2015). However, ultimately there was no outright objection during the 2015 IETF Dallas meeting against moving forward on status code '451'. So, in December 2015, it became an IETF approved HTTP status code to signal online censorship.[19]

[16] The Hyper Text Transfer Protocol (HTTP) status code '451 Unavailable for Legal Reasons' is the protocol that guides how messages are transmitted and formatted and how servers and browsers should deal with various commands—error status code. It is displayed when a resource (web servers or pages) can't be accessed because of legal reasons, often because a government blocks them. This status code would create more transparency about how legal and political issues affect the ability of end-users to connect.

[17] The choice is slightly ironic because Bradbury chose that title in order to refer to the alleged temperature at which paper self-combusts. The Gutenberg age still deeply influences the Turing age.

[18] See http://tools.ietf.org/wg/httpbis/minutes?item=minutes-92-httpbis.html discussions on 451 at IETF 92 in Dallas.

[19] We understand that the usefulness of status code 451 is limited, as it will most likely be used in cases of cooperative, legal content removal like for instance copyright infringements. It does not provide a method to detect censorship across the board, as it requires those entities doing the filtering to voluntarily inject the status code. This being said, we believe it remains an important development as it creates more transparency about online censorship.



```
HTTP/1.1 451 Unavailable For Legal Reasons
Content-Type: text/html

<html>
<head>
<title>Unavailable For Legal Reasons</title>
</head>
<body>
<h1>Unavailable For Legal Reasons</h1>
<p>This request may not be serviced in the Roman Province of
Judea due to Lex3515, the Legem Ne Subversionem Act of AUC755,
which disallows access to resources hosted on servers deemed
to be operated by the Judean Liberation Front.</p>
</body>
</html>
```

Fig. 1 Status code 451 *Source*: Website Bray (2012), author of the 451-status code ID, https://tools.ietf.org/html/draft-tbray-http-legally-restricted-status-00

Online censorship is a quintessential human rights issue, and one of the main vehicles through which the right to freedom of expression can be chilled online. Interestingly, not only technical arguments but also the status code's potential use for civil society played a substantial role (first author's field notes) in shaping the discussion, and the decision to move forward with this technology.

We have seen that the IETF does indeed enable—and some times even "bakes in"—particular values through the Internet's architecture. From the data analysis it became clear that there are three conditions that need to be met for values to become enabled by protocols. First, there needs to be a clear technical justification. Second, the enabling of values can occur only when there is no strong commercial or political resistance. Third, the value needs to work towards maintaining the fourfold normative conceptualization of the Internet as presented earlier.

None of this undermines the 'tussle theory' argument made by Clark et al. (2005), because that argument is normative (it argues what the case should be, not what the case is). However, it does put some pressure on it, insofar as the IETF makes decisions that limit the space for tussle by elevating a the actualisation of a particular societal value to a global norm, thereby also determining the path contingency of technology, what practices it enables, and which rights it protects. In their paper on 'tussle in cyberspace' Clark et al. argue *factually* (and not just *normatively*) that:

> Societies are structured around "controlled tussle" – regulated by mechanisms such as laws, judges, societal opinion, shared values, and the like. Today, this is the way the Internet is defined – by a series of on-going tussles (2005:2).

Yet, the previous statement and the further observation—made by Clark et al. later in their paper—that 'there is no "final outcome" of these interactions, no stable point, and no acquiescence to a static architectural model' (2005:2) are not always true. This does not mean that we should opt in favour of the 'baking-in theory'. The IETF is not, as Brown et al. (2010:3) would like, purposefully 'baking fundamental values into the architecture'. Neither of these theories fully maps onto the empirical findings presented in this article. This seems to suggest that, in some in cases, the IETF does enable social values to manifest, yet not necessarily by baking them into the design of protocols. Rather, the IETF engineers opt for 'soft-measures', like privacy considerations, which ask engineers to consider the possible impact their technology might have on privacy. By giving a detailed overview of potential issues, and documenting them, the engineers are not necessarily engaging in value-sensitive design but rather in 'responsibility-by-design'. They do not 'bake in' or instantiate certain values in protocols, but they do build parameters,[20] around the possible 'tussles' that can take place within designs. As a result, the IETF has implicitly created a mechanism that introduces an element of 'responsibility-by-design'. It has created procedures (not protocols) that mandate and entice engineers to design, code, and act responsibly by considering and documenting the potential negative impact their designs might have on certain values. But what does this mean for the responsibility of the IETF to enable the actualisation of human rights? This is the topic of the next section.

The IETF's Ethical Responsibility

Acknowledging the fact that sometimes particular values get enabled through protocols is not equivalent to arguing that the IETF *should* do so. When analysing past and contemporary IETF debates, engineers often repudiate responsibility for the potential impact of their work on human rights by arguing that the technology they build is neutral. In order to deflect responsibility, they separate their role in creating technology from its potential use for reprehensible purposes. Today, this line of reasoning is at worst untenable and at best in need of a much stronger justification, since it is well known that technology, including that made by the IETF, is by no means neutral (Denardis 2015; Thompson 2013). IETF engineers have a clear responsibility to ensure that human rights are accounted for in the design of the Internet's architecture. This responsibility is based on a combination of the following factors: first, the Internet is becoming increasingly important for enabling and inhibiting human rights, most obviously for rights like freedom of expression, access to information and freedom of assembly (Dutton 2011; UNESCO 2015). Second, the protocols and standards made by the IETF to a large extent shape the Internet by defining how and to what people can connect (Denardis 2015; Liddicoat and Doria 2012). Through this the IETF determines the path contingency of technology, what practices it enables, and which rights it protects. Third, throughout its history the IETF has selectively enabled the actualisation of certain

[20] These parameters come in the form of privacy and security considerations, that when considered 'too grave', means that an RFC will be not be approved by the Internet Engineering Steering Group (IESG), until the issues are sufficiently addressed. 'The Internet Engineering Steering Group (IESG) is responsible for technical management of IETF activities and the Internet standards process. (…) The IESG is directly responsible for the actions associated with entry into and movement along the Internet "standards track," including final approval of specifications as Internet Standards.' For more information please see: https://www.ietf.org/iesg/.

rights. Fourth, considering the global nature of the Internet and IETF's influence in shaping it, the IETF can no longer cherry-pick which rights it choses to protect. Instead it has a moral responsibility, and perhaps even a legal one (Bless and Orwat 2016), to ensure that it provides a blanket protection of the most accepted standards for human rights shared across the globe: the United Declaration of Human Rights (UDHR).

Many IETF engineers disagree. On multiple occasions, they expressed their preference for a 'technologically neutral' approach to the design of protocols. One engineer drew the following analogy to make this point:

> Of course, no well-trained ethically conscious engineer would ever write a "destroy Baghdad" procedure. He would write a "destroy city" procedure, and passing Baghdad as a parameter. (…) It is not that people here [at the IETF] are opposed to human rights. They just want to write their code so you can bomb any city, rather than one specific city. They want to be neutral about everything. (Interview collected by first author, March 2015)

However, we hold that it is precisely the ability to mediate the experience of individuals online across the globe that lies at the base of the IETF's responsibility to act in such a fashion that its standards enable the realisation of human rights. Or as Liddicoat and Doria (2012:15) argue:

> The technical community will not only be best placed but will have the sole ability to protect human rights standards in relation to the free flow of information and ideas, precisely because they are the only community able to see the human rights issues that have been hard-wired into the very way in which the Internet operates.

The question remains whether instantiating human rights *in* protocols is the best way to achieve this goal, and what alternatives exist. This question will be answered in the final section below.

Conclusion: Policy Recommendations

Throughout this article the word 'should' has played an important role, not as a mere recommendation, but as a call to action for the IETF. It refers to the necessity for the IETF to recognise its ethical responsibility to ensure that its work is in line with the UDHR principles.

The IETF strives to create an Internet that provides continuous connectivity for all its users at all times, and for any content. Although the four main architectural design principles—to reiterate: openness, interoperability, redundancy and end-to-end—are presented as strictly technical, they represent a socio-political conceptualisation of how IETF engineers see the Internet: a medium for connectivity and, by extension, a support for the rights like the right to privacy and freedom of expression. This underlying normative framework drives the technological design decisions by IETF engineers, and is reinforced by the particular composition of the IETF participant base. We identified three particular factors as crucial in understanding situations where the IETF decided that it could, and should, enabled the realisation of a particular social value into the Internet's architecture. We have argued, in four steps, that the IETF has a clear, ethical obligation to ensure that its work is in line with the UDHR principles, even though it is not traditionally recognized as an actor with direct obligations to safe guard human rights. But does this mean that the IETF *should* encode values *always* or *only* when it perceives it *can* do so? This article has walked a fine line between answering the question of whether human rights *can* be enabled in protocols and whether human rights *should* be enabled in protocols.

On the one hand, the debate on pervasive monitoring indicates that the IETF is not inclined to entertain the question of whether it *should* encode values if it perceives that the three basic conditions (necessary to ensure that it *can* encode values) are not satisfied. On the other hand, the debate on status code '451' indicates that there is a cultural shift going on within the IETF where the first condition (a strictly technical reason for enabling a social value) is no longer an absolute requirement.

We believe that despite the current challenges outlined in this paper, the IETF should find an explicit and consensual way to implement the UDHR principles. We saw that the IETF enables individuals to exercise their human rights by maintaining the Internet as a network of unfettered connectivity. Directly 'baking' human rights into protocols—considering the current political and commercial climate—can be counterproductive to the IETF's overarching goal of maintaining connectivity. It might lead to important market and political stakeholders opting out of the IETF, were it to encode protocols with human rights. This would effectively draw the logical layer of the Internet further into the politicized debate on Internet governance.

But this does not mean the IETF should not find other ways to enable human rights through its work, without directly implementing human rights-by-design, as it has effectively been doing by instituting several 'responsibility-by-design' measures, like privacy and security considerations. Nor does it mean that there are no exceptions to this rule. In some cases design decision that instantiate a certain rights enabling feature—like for instance the Hyper Text Transfer Secure (HTTPS)[21] protocol—can have a positive effect on human rights. We however argue that 'soft' responsibility-by-design measures are, at this time and considering the limited body of knowledge on the impact of baked-in solutions, the best way forward.

Additionally, we should not be naive about the current state-of-play. The IETF is, and always has been, a politicized body. Organizations responsible for Internet standard setting and managing its architecture, including the IETF, the Internet Corporation for Assigned Names and Numbers (ICANN),[22] and the United Nations International Telecommunications Union (ITU),[23] have always been subject to

[21] The Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of the Hyper Text Transfer Protocol (HTTP). HTTP is the protocol that sends data between a browser and a requested website. Secure in this case means that the communication between the browser and the website is encrypted.

[22] ICANN is a crucial Internet governance organization. This technical non-profit multistakeholder organization, is responsible for managing a crucial part of the Internet's core infrastructure and ensures

realpolitik. When the IETF feels so compelled, it has enabled social values that effectively enable the realisation of human rights like privacy and freedom of expression.

Considering the global nature of the Internet, its importance vis-à-vis human rights and the unique role of the IETF in maintaining the Internet—the IETF should ensure that human rights become an integral part of its work. Especially as we concur with Broeders (2015) that 'although national states will inevitably want to 'create an Internet in their own image', we must find ways to continue guaranteeing the overall integrity and functionality of the public core of the Internet.' The IETF should bite the bullet, and formalize what it has implicitly done for many years: building an Internet that is a fundamental enabler of human rights.

Furthermore, the merits of attempting to bring the work of the IETF more in line with the UDHR principles, especially article 19, should not be overlooked. Given that, making the Internet respect the UDHR principles could strengthen its architecture. We should be discussing openly and in depth the policy recommendations that can ensure that the IETF develops the Internet's architecture in a way that is fully supportive of human rights. What follows are three recommendations that we hope may facilitate the debate.

First, as the Internet increasingly becomes 'a mirror of the societies in which it operates' (Clark et al. 2005:475), it makes sense to mirror the work of the IETF to the UDHR guiding these societies. This means finding novel ways to have human rights inform protocol development. The IETF has an Internet Research Task Force (IRTF) research group on human rights that is currently spearheading this attempt (disclosure: the first author of this article is a member of the group). The group is creating an RFC with 'Human Rights Protocol Considerations'.[24] These considerations are modelled on the protocol considerations for privacy (RFC 6973) and security (RFC 3552), but with a specific focus on human rights. This particular format of protocol considerations fits the IETF's structure: it is a procedure to which the IETF engineers are accustomed, and it leaves enough flexibility to circumvent issues raised about the legitimacy of the IETF to act as a law making or interpreting body, or active resistance by large market players. Human rights considerations, like privacy and security considerations, would require engineers to consider human rights in their designs, as well as inform RFC readers and implementers of relevant human rights issues. Admittedly, security and privacy considerations are historically considered weak, in the sense that those reading and implementing the RFCs can choose to ignore them. Nevertheless, creating explicit human rights considerations provides a strong first step towards integrating human rights into the IETF's work,

Footnote 22 continued
the network's stability and secure operation. ICANN is responsible for managing IP addresses, domain names, and root servers.

[23] ITU is the United Nations organisation responsible for developing telecommunications standards; it is also involved in developing new standards for broadband Internet, latest-generation wireless technologies, Internet data and access.

[24] See here for the most recent Internet Draft (I-D) by the Human Rights Protocol Considerations (HRPC) research group, which includes the first iteration of the human rights protocol considerations: https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/.

while sensitizing engineers to the potential impact of their work on human rights. It would also formalize a ‘responsibility-by-design’ approach to technical engineering.

Hence, we argue that the IETF should opt for an approach that enables human rights *through* protocols over designing them *in* protocols. This is not to say that we completely rule out the potential positive impact of embedded human rights solutions. However, considering the political and economic developments mentioned earlier this approach seems less viable at this point in time.

Second, it seems reasonable to increase the number of technical engineers that act as custodians for human rights at the IETF. Theoretically, engineers come to the IETF in their personal capacity. Yet, participation in the offline gatherings of the IETF is costly. As such, it is only feasible for those individuals whose companies or organizations provide them with the budget to participate.[25] The IETF’s own statistics reveal that the majority of its participants work for large companies like Cisco, Microsoft and AT&T.[26] Inevitably, these engineers come to the IETF with a particular ethos, and agenda, which does not automatically take into consideration broader human rights issues.

Considering the impact of the Internet’s architecture on society, it is important to ensure that human rights as outlined in the UDHR are represented at the IETF. The past 20 years have shown that, when technical engineers from, for instance, the Centre for Democracy and Technology (CDT), the American Civil Liberties Union (ACLU) or ARTICLE 19 actively participate in specific IETF working groups, they effectively identify and improve the work that has a potential impact on human rights. The recent development of the RFC on privacy considerations is an example of such a procedure in which these human rights custodians played an important role. Another is the development of the HTTP Secure (HTTPS) protocol and status code 451.

Both these policy recommendations however run the same risk that may undermine security and privacy considerations: faulty implementation or partial deployment of RFCs. This is why they need to be buttressed by a third recommendation.

This third recommendation is that the four key architectural principles as laid out by Clark et al. (2005) must play a necessary role in protocol design. Unfortunately, due to commercial developments, the market is moving away from these four foundational principles. For instance, the erosion of net neutrality undermines the end-to-end principle by transferring the intelligence originally held by the end-users to the network.[27] Similarly, the market’s move towards a locked-in or ‘walled garden’ approach to software development (Benkler 2006; Zittrain 2008) undermines interoperability. Many of the social networks that present themselves as crucial for the implementation and enactment of, for instance, the right to freedom of expression, are not interoperable, effectively silo-ing users into their platform,

[25] See discussions on the IAOC mailinglist on 26-04-2016 under the title: “What is the default hotel?” https://mailarchive.ietf.org/arch/search/?email_list=mtgvenue.

[26] See http://www.arkko.com/tools/allstats/companydistr.html.

[27] For an elaborate analysis of link between net neutrality and the end-to-end principle see: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/NetNeutrality/Articles/Proponents.html.

diminishing properties of the network that could enable freedom of expression. Although these platforms cannot be forced to adopt interoperating solutions, and ISPs and legislators cannot be coerced into maintaining net-neutrality, the IETF can make a statement and lead by example, by ensuring its work maintains the basic principles that led the Internet to become a crucial support for human rights.

These three recommendations present realistic and technically feasible ways to ensure that human rights concerns are addressed within the IETF, without designing them directly into technologies. They favour a broad ethical approach to the design of Internet's architecture, address the issues surrounding Internet fragmentation arising from market and political developments, are in line with the IETF's current modus operandi, and are built upon the technical foundation that underlies the Internet's architecture.

The design decisions made by the IETF's technical engineers fundamentally shape the Internet's architecture, the path contingency of technology, and how end-users are enabled or inhibited from exercising their fundamental human rights. Gaining a clear picture of how values can be enabled, as well as when and why various technical and personal factors influence value-sensitive design decisions, is vital to understanding how the Internet can continue to develop as a crucial platform for the realisation of human rights. This research has shown why it is currently feasible and indeed necessary for the IETF to implement an explicit 'responsibility-by-design' approach to engineering that accounts for the UDHR principles, and that ensures that the IETF's work enables and supports human rights.

Acknowledgments We discussed multiple versions of this article on many occasions during academic conferences, IETF meetings, and with policy makers in the field of Internet governance. Specifically, the first author discussed some of the ideas included in this article at RIPE 70 in Amsterdam May 2015, IETF 94 in Yokohama November 2015, Computers, Privacy and Data Protection (CPDP) in Brussels January 2016, and IETF 95 in Buenos Aires April 2016. We are deeply indebted for the feedback we received from these various communities and audiences. In particular, we wish to thank the two anonymous reviewers whose comments greatly improved the final version. We also want to thank Niels Ten Oever and the Human Rights Protocol Considerations Research (HRPC) group at the Internet Research Task Force (IRTF) for their insightful comments and for the time they put into discussing the ideas presented in this article. We are grateful to David Sutcliffe for his editorial revisions of the penultimate version.

References

Abbate, J. (2000). *Inventing the internet*. Cambridge, MA: MIT Press.

Abrams, P. (1998). Notes on the difficulty of studying the state. *Journal of Historical Sociology, 1*(1), 58–89.

Babbie, E. (2010). *The basics of social research*. Belmont, CA: Cengage.

Baran, P. (1964). *On distributed communications: Twelve volumes*. Washington, D.C.: RAND Report Series.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven and London: Yale University Press.

Berkman Center Report. (2016). *Don't panic: Making progress on the "going dark" debate*. Retrieved February 2, 2016, https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Blee, K., & Taylor, V. (2002). Semi-structured interviewing in social movement research. In B. Klandermans & S. Staggenborg (Eds.), *Methods of social movement research* (pp. 92–117). Minneapolis and London: University of Minnesota Press.

Bless, R., & Orwat, K. (2016). *Values and networks—Steps toward exploring their relationships.* ACM: Sigcomm. Retrieved April 29, 2016, from http://www.sigcomm.org/ccr/papers/2016/April/0000000.0000003.

Bray, T. (2012). *ID 2616 a new HTTP status code for legally-restricted resources draft-tbray-http-legally-restricted-status-00*. Retrieved May 1, 2015, from https://tools.ietf.org/html/draft-tbray-http-legally-restricted-status-00

Broeders, D. (2015). *The public core of the internet*. Amsterdam: University Amsterdam Press.

Brown, I., Clark, D., & Trossen, D. (2010). *Should specific values be embedded in the Internet architecture?* Retrieved February 13, 2015, from http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf.

Brysk, A. (2002). *Human rights and globalization*. Berkeley: University of California Press.

Busch, L. (2011). *Standards: Recipes for realities*. Cambridge, MA: MIT Press.

Cavoukian, A. (2009). *Privacy by design*. Ottawa: IPC Publications.

Clark, D. (1988). *The design philosophy of the DARPA Internet protocols*. Retrieved February 12, 2015, from http://ccr.sigcomm.org/archive/1995/jan95/ccr-9501-clark.pdf.

Clark, D., Wroclawski, J., Sollins, K., & Braden, R. (2005). Tussle in cyberspace: Defining tomorrow's internet. *IEEE/ACM Transactions on Networking, 13*(3), 462–475.

Creswell, J. W. (2013). Five qualitative approaches to inquiry. In J. W. Creswell (Ed.), *Qualitative inquiry and research design: Choosing among five approaches* (Vol. 3, pp. 53–84). Thousand Oaks CA: Sage.

Davidson, A., & Morris, J. (2003). *Policy impact assessments: Considering the public interest in Internet standards development*. Retrieved February 27, 2015, from https://www.cdt.org/files/publications/pia.pdf.

Demmers, J. (2012). *Theories of violent conflict: An introduction*. NYC: Routledge.

Denardis, L. (2013). *Protocol politics: The globalization of Internet governance*. Boston: MIT Press.

Denardis, L. (2014). *The global war for Internet governance*. New Haven: Yale University Press.

Denardis, L. (2015). *The Internet design tension between surveillance and security*. Retrieved 3 March, 2015 from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7116471.

Denzin, N. K., & Lincoln, Y. S. (2000). *Handbook of qualitative research*. Thousand Oaks, CA: Sage.

Doty, N. (2015). *Reviewing for privacy in Internet and Web standard-setting*. Retrieved March 29, 2016, from https://npdoty.name/slides/nickdoty_reviewing-for-privacy.pdf.

Dutton, W. (2011). *Freedom of connection, freedom of expression: The changing legal and regulatory ecology shaping the internet*. UNESCO. Retrieved December 22, 2014, from http://portal.unesco.org/ci/en/ev.php-URL_ID=31397&URL_DO=DO_TOPIC&URL_SECTION=201.html.

Floridi, L. (2011). A defence of constructionism: Philosophy as conceptual engineering. *Metaphilosophy, 42*(3), 282–304.

Franklin, U. M. (1999). *The real world of technology*. Toronto: Toronto University Press.

Galloway, A. (2004). *Protocol*. Boston: MIT Press.

Harvey, W. (2011). *Strategies for conducting elite interviews*. Retrieved June 29, 2015, from http://www.researchgate.net/profile/William_Harvey6/publication/228312871_Strategies_for_Conducting_Elite_Interviews/links/543fc38f0cf2fd72f99da47b.pdf.

Hill, J. F. (2013). *A balkanized Internet? The uncertain future of global Internet standards*. Retrieved November 2, 2014, from http://journal.georgetown.edu/a-balkanized-internet-the-uncertain-future-of-global-internet-standards-by-jonah-force-hill/.

Internet Engineering Task Force. (1996). *RFC 1958 architectural principles of the Internet*. Retrieved March 25, 2015, from https://www.ietf.org/rfc/rfc1958.txt.

Internet Engineering Task Force. (1997). *RFC 2119 key words for use in RFCs to indicate requirement levels*. Retrieved March 4, 2015 from https://www.ietf.org/rfc/rfc2119.txt.

Internet Engineering Task Force. (1998). *RFC 2418 security considerations*. Retrieved April 2, 2015, from https://tools.ietf.org/html/rfc2418#page-23.

Internet Engineering Task Force. (2002). *RFC 3426 general architectural and policy considerations*. Retrieved February 17, 2015 from http://www.rfc-base.org/rfc-3426.html.

Internet Engineering Task Force. (2003). *RFC 3552 guidelines for writing RFC text on security considerations*. Retrieved March 13, 2015, from https://www.ietf.org/rfc/rfc3552.txt.

Internet Engineering Task Force. (2004). *RFC 3935 a mission statement for the IETF*. Retrieved May 1, 2015, from https://www.ietf.org/rfc/rfc3935.txt.

Internet Engineering Task Force. (2013). *RFC 6973 privacy considerations*. Retrieved July 5, 2015, from https://www.rfc-editor.org/rfc/rfc6973.txt.

Internet Engineering Task Force. (2014). *RFC 7258 pervasive monitoring is an attack*. Retrieved March 13, 2015, from https://tools.ietf.org/html/rfc7258.

Jabri, V. (1996). *Discourses on violence: Conflict analysis reconsidered*. Manchester and New York: Manchester University Press.

Kurose, J., & Ross, K. W. (2007). *Computer networking: A top-down approach* (4th ed.). Boston: Addison-Wesley.

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0*. New York: Basic Books.

Liddicoat, J., & Doria, A. (2012). *Human rights and Internet protocols: Comparing processes and principles*. Retrieved July 13, 2015, from https://www.unesco-ci.org/cmscore/sites/default/files/2013wsis10/human_rights_and_internet_protocols-_comparing_processes_and_principles28129.pdf.

Mueller, M. (2004). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge MA: MIT Press.

Mueller, M. (2010). *Networks and states*. Cambridge MA: MIT Press.

Post, D. (2015). *Internet infrastructure and IP censorship*. Retrieved August 1, 2015, from http://www.ipjustice.org/digital-rights/internet-infrastructure-and-ip-censorship-by-david-post/.

Rabkin, A., Doty, N. & Mulligan, D. K. (2010). *Facilitate, don't man-date*. Retrieved January 1, 2016 from http://www.iab.org/wp-content/IAB-uploads/2011/03/nickdoty.pdf.

Rachovitsa, A. (2015). *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*. Retrieved May 5, 2015, from http://www.ietf.org/mail-archive/web/hrpc/current/pdfRBnRYFeVsm.pdf.

Richards, L. (2009). *Handling qualitative data: A practical guide*. London: Sage.

Richie, J., & Lewis, J. (2003). *Qualitative research practice: A guide for social science students and researchers*. London: Sage.

Sweet, J., & Schneier, M. (2013). *Legal aspects of architecture, engineering and the construction process*. Cengage: Stamford.

Sweet, J., Schneier, M., & Wentz, B. (2015). *Construction managers and contractors*. Cengage: Stamford.

Thompson, M. (2013). *Evaluating neutrality in the information age: On the value of persons and access*. University of Oxford, Oxford. Retrieved March 16, 2015 from http://www.oii.ox.ac.uk/people/?id=86.

UNESCO. (2015). *Connecting the dots: Access to information and knowledge, freedom of expression, privacy and ethics on a global Internet*. Retrieved July 1, 2015, from http://unesdoc.unesco.org/images/0023/002325/232563E.pdf

UN Human Rights Council (OHCHR). (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. Retrieved February 27, 2015 from http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

UN Human Rights Council (OHCHR). (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*. Retrieved July 3, 2015, from http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

Winner, L. (1977). *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, MA: MIT Press.

Zittrain, J. (2008). *The future of the Internet—And how to stop it*. New Haven: Yale University Press.