A Case Study of Coding Rights: Should Freedom of Speech Be Instantiated in the Protocols and Standards Designed by the Internet Engineering Task Force?

Thesis for degree in Master of Science in Social Science of the Internet

Candidate: Corinne J.N. Cath -- corinnecath@gmail.com

Candidate number: 692683

College: St. Hilda

Oxford Internet Institute 10 August 2015

Word count: 14.998

Thesis submitted in partial fulfilment of the requirement for the degree of MSc in Social Science of the Internet at the Oxford Internet Institute at the University of Oxford.

Abstract

The Internet Engineering Task Force (IETF) is one of the most important players in maintaining the technical architecture of the Internet. It plays a crucial role in managing the logical layer of the Internet, and designing the standards and protocols that define how information flows across the network. Considering the increased public and academic focus on the importance of value-sensitive design after the Snowden revelations in 2013, the limited body of literature on what role societal values could and should have in the development of Internet protocols and standards is surprising. This research aims to fill this knowledge gap by presenting an in-depth ethnographic case study of the Internet Engineering Task Force.

I ask the question what the role is and *should* be of human rights – in particular the right to freedom of speech – in the development of IETF Internet protocols and standards.

The data I present in this research gives a window into the day-to-day workings of the IETF. Through qualitative interviews, discourse analysis and participant observation I show that particular social values are being instantiated in protocols, but only when these values have the necessary technical properties and if there is no strong commercial or political pushback. I explain how the IETF's unique position to influence the Internet's design comes with a moral obligation to ensure its work is aligned with fundamental human rights principles. I also argue that various political, practical and commercial realities create a situation in which it is currently not feasible – or wise – for the IETF to instantiate human rights *in* protocols. On the basis of these findings I present several policy recommendations that ensure the work of the IETF accounts for human rights, and I make various suggestions for further research.

Keywords: Article 19, Code, Ethics, Freedom of Speech, Human Rights, Internet Architecture Management, Internet Engineering Task Force, Internet Fragmentation, Privacy-by-design, Protocols, Standards, Standard Setting Bodies, Technical Engineering, United Nations Declaration of Human Rights, Value Sensitive Design.

Acknowledgments

I am deeply grateful for the support of a variety of people, who helped me throughout the research process. First, I want to thank the research participants without whom this thesis could not have come into being. Second, I want to thank my supervisor Professor Luciano Floridi. His excellent guidance, insights, endless patience, and brilliant squash analogies allowed me to 'keep my eyes on the ball' throughout the MSc program.

I am deeply indebted to the OII Faculty for supporting me to pursue this research. My MSc cohort played a crucial role in keeping my spirits lifted, the soccer matches friendly, and my cup of coffee filled to the brim.

A special thanks is reserved my grandmother Corinne De Beaufort, mother Inez de Beaufort, aunt Pauline van der Meer Mohr and sister Ernestine Cath. Your support and encouragement is, and always has been, crucial. I also want to thank the 'Prins Bernhard Cultuur Fonds' and the 'Genootschap Noorthey', without whose scholarships I would not have been able to come to Oxford.
There are a number of other people who deserve a special mention for providing me with advice, insights and excuses to leave Oxford, amongst whom are: Ian Brown, Laura Denardis, DKG, Joana Varon, Joe Hall, Niels ten Oever, Mor Rubinstein, Meredith Whittaker, Joss Wright, and Ben Zevenbergen.

Finally, I am deeply grateful to my family and friends for putting up with my ceaseless use of Internet lingo and 16-letter abbreviations. You helped me struggle through understanding the world and work of technical engineers, encouraging me whenever I no longer saw the light at the end of the [encrypted] tunnel, and providing me with invaluable feedback on my work. Last but not least, I want to thank my housemates Beth, Luca, and Nathan for giving me a sense of home and community in Oxford.

Table of Contents

List of Abbreviations

AD	Area Director
ACLU	American Civil Liberties Union
BCP	Best Current Practice
BOF	Birds of a Feather
CDT	Centre for Democracy and Technology
DNS	Domain Name System
DRM	Digital Rights Management
ETSi	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
HRPC	Human Rights Protocol Considerations
HTTP	Found Hypertext Transfer Protocol
IAB	Internet Architecture Board
ICANN	The Internet Corporation for Assigned Names and Numbers
ID	Internet Draft
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IM	Instant Messaging
IRTF	Internet Research Task Force
ISP	Internet Service Provider
ITU	International Telecommunication Union
NAT	Network Address Translator
OHCHR	United Nation's Office of the High Commissioner for Human Rights
OPES	Open Pluggable Edge Services
PM	Pervasive Monitoring
RFC	Requests for Comments
SDO	Standards Developing Organisation
SMTP	Simple Mail Transfer Protocol
SPUD	Session Protocol Underneath Datagrams
TLS	Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
UDHR	Universal Declaration of Human Rights
WG	Working Group
W3C	World Wide Web Consortium

Table of Figures

Chapter 1. Human Rights and Internet Architecture Management

> By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole. (...) The full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception, and that this principle should never be reversed. (United Nations Office of the High Commissioner for Human Rights 2011)

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. (United Nations Office of the High Commissioner for Human Rights 2015)

1.1 Introduction

The most recent report of the United Nation's Office of the High Commissioner for Human Rights (OHCHR) posits that there is a direct link between digital security, privacy on the Internet and maintaining freedom of speech. The report states that technological solutions, like banning the use of 'backdoors' by governments and encouraging encryption, are important steps to preserving freedom of speech. This argument is in line with academic theories on value-sensitive design, which suggest that particular societal values – like privacy – should be hard-coded into technology (Cavoukian 2009; Ceyhan 2008). This thesis builds upon this academic work and 'privacy in design' studies, which:

> raise[s] awareness about the processes through which values and norms become embedded in technological architecture and looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens (EGE 2014:32).

The growing impact of the Internet on the lives of individuals (Benkler 2006; Castells 2001; Mueller 2004; 2010) makes the architecture of the Internet, its standards and protocols, increasingly important to society (Davidson and Morris 2003). However, the logical layer of the Internet – where these standards and protocols reside – is often left out of the discussion on value-sensitive design. This is surprising as protocols and standards define how information travels across the net, and who is able to connect to whom and what. Internet standards and protocols are thus highly relevant to any discussion about how to protect human rights both online and offline (Anderson 2015; Busch 2011; Liddicoat and Doria 2012; Post 2015).

Questions at the intersection of human rights and Internet architecture management are particularly interesting as Internet Standard Setting Bodies (SDOs) are increasingly becoming arenas for tussles over value-sensitive design, and the moral (and 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). This thesis focuses on whether human rights – in particular the right to freedom of speech – should be instantiated in protocols and standards designed by the Internet Engineering Task Force (IETF).

Structure

This thesis is structured in six chapters. The first chapter presents an introduction and overview of the current academic debate on the intersection of human rights and Internet architecture management. The second chapter gives a detailed overview of the research design, methods, and limitations of this research. The findings are presented in three separate chapters, each corresponding to a specific research sub-question.

Chapter three describes how the different technical principles followed by IETF engineers indicate the existence of a shared normative understanding between them of what the Internet is.

Chapter four analyses five case studies with the aim of understanding how this conceptualisation of the Internet is maintained (or not) in its larger political and commercial context, and especially how different societal values are weighed, and eventually encoded.

Chapter five presents what the role of human rights is, and should be, in the process of Internet architecture management at the IETF. It identifies various difficulties involved in instantiating human rights in Internet protocols. Finally, chapter six synthesises the findings of the previous chapters, presents some conclusions, suggestions for further research, and policy recommendations.

Research Questions

This research addresses the following central question:

> *Should the right to freedom of speech be instantiated in the protocols and standards designed by the Internet Engineering Task Force?*

This overarching question is articulated into three sub-questions that overlap with chapter three, four and five:

> *a. What is the underlying normative framework that drives the technological design decisions made by engineers, and what role do the engineers' personal ethics play in this?*
>
> *b. How do values become instantiated in protocols, and how do contextual factors like political and market dynamics constrain (or enable) particular value-sensitive design decisions?*

c. What is the responsibility of the IETF towards human rights, and what obstacles does it encounter when trying to instantiate human rights in the Internet's architecture?

By answering such sub-questions, the thesis pursues three main goals. First, it provides an in-depth and emic analysis – using the data gathered through qualitative interviews, participant observation and discourse analysis – of the normative framework that shapes technical decisions of IETF engineers, how contextual factors like politics and market dynamics constrain or enable certain design decisions, and the responsibility of the IETF vis-à-vis human rights. Second and third, this research aims to add both to the academic discussion and the policy discussion on the role of Internet architecture management in implementing value-sensitive design aimed at upholding human rights principles.

1.2 Literature Review: to bake-in or not to bake-in, that is the question.

In the heyday of the Internet the people running, building, and maintaining it were academics (Abbate 2000:1). As such there has always been a lively academic debate surrounding Internet architecture management. 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 et al. 2005; Kurose and Ross 2007). These principles are at the base of the success of the Internet, as we know it. 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).

It is crucial to develop a better understanding of the normative frameworks underlying the design choices made by technical engineers. These decisions influence the creation of standards, which in turn determines how the Internet is experienced by end-users and to what extent it protects their fundamental human rights. Or as Brown et al. state:

> 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).

This thesis uses this statement as a point of departure, expanding Brown et al.'s point to include potential impacts on human rights.

In the early nineties, Internet architecture management was heavily influenced by cyber-utopians, who clung to the famous 'Declaration of Independence in Cyberspace' by John Perry Barlow (1996). Yet, non-technical actors and values consistently influenced architecture management, as such technology has never been neutral (Abbate 2000; Brown et al. 2010; Busch 2011; Denardis 2014; Franklin 1999; Galloway 2004; Winner 1977). Technical engineers' personal values – as well as larger societal values – get encoded into the technology they build (Abbate 2000; Denardis 2013; 2014).

The influence of commercial and political forces on Internet architecture management is well documented in the academic literature (Benkler 2006; Brown et al. 2010; Denardis 2014; Lessig 2006; Mueller 2004; Zittrain 2008). Lessig details how SDOs are increasingly influenced by 'the invisible hand of commerce' (2006:208). This leads SDOs to make decisions that, according to Davidson and Morris (2003:9), are not always in the best interest of end-users. Denardis (2013; 2014; 2015) on the other hand argues that the IETF consistently pushes back against developments that lead to the standardisation of surveillance and other issues that negatively influence end-users' experience of the Internet.

This research will shed further light on these theories, by detailing what conditions need to be present for the IETF to resist commercial and political developments that negatively impact end-users. In addition, the role that societal values – in particular human rights – can and should play in Internet architecture management warrants further academic exploration (Busch 2011; Post 2015). There are two main positions in the current academic debate over the role that societal values – especially human rights – should have in guiding protocol development. On the one hand, Clark et al. argue there is a 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).

Both positions are highly normative. Brown et al. and Clark et al. focus on the question whether particular societal values *should* be followed when designing protocols. The research questions posed in this thesis interrogate both the assertions made by Clark et al.'s (2005) 'tussle theory' and add further complexity to the position taken by Brown et al. (2010).

Currently, there are only a limited number of such case studies that examine their arguments in-depth (Denardis 2015; Thompson 2013; Rachovitsa 2015). This shortcoming is a direct motivation for this qualitative research, which presents an ethnographic case study on the question whether and how human rights should guide protocol development. Filling this knowledge gap is important not only because protocols and standards shape the Internet, but also because code – the software and hardware that defines the infrastructure of cyberspace – is increasingly perceived to have the same power in society as law (Lessig 2006).

Code is (Human Rights) Law

There is a direct link between the discussion on the role that values should play in the development of code (Brown et al. 2010 and Clark et al. 2005) and Lessig's position that 'code is law' (2006). Standards and protocols are code. Arguably, if code is law, then protocols and standards should be more in line with the existing bodies of law of the physical world (Brown et al. 2010; Liddicoat and Doria 2012; OHCHR 2015; UNESCO 2015).

Considering the global nature of the Internet and the many different contexts and cultures it exits in, the most relevant moral and legal framework to be upheld by those designing its structure is the United Nations Declaration of Human Rights (UDHR). The UDHR consists of thirty articles that cover the fundamental inalienable rights held by all human beings. Although the UDHR is not legally binding, it has been included in many national laws and constitutions since its adoption. It is the basis of a plethora of international, national, and regional laws aimed at protecting and promoting fundamental human rights. Several of these rights have clear online components, such as freedom of speech and assembly (Dutton 2011; UNESCO 2015).

As mentioned, this thesis will focus in particular on how the right to freedom of speech – also referred to as the right to freedom of opinion and expression – should guide Internet architecture management. This focus was chosen in light of the direct link between the Internet and freedom of speech (Deibert et al. 2008; Benkler 2006; Castells 2001; Morozov 2011). As well as the limited body of existing scholarship on freedom of speech and its intersections with Internet architecture management, and the importance of freedom of speech for 'the enjoyment of other human rights and freedoms that constitutes a fundamental pillar for building a democratic society and strengthening democracy'

(Human Rights Council resolution 25/2). Freedom of speech will be defined as outlined in article 19 of the UDHR, which states that:

> 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 Internet increasingly is one of these media. Hence it is not surprising that in the wake of the Snowden revelations – which revealed how certain actors are using the Internet's architecture in ways that infringe upon human rights – there has been an increased call for value-sensitive Internet design that takes into account freedom of speech (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. However, these calls mostly focus on privacy. The language remains vague, not specifying how value-sensitive design should enter the engineering process. This thesis will attempt to address this issue.

1.3 Setting the Stage: The Internet Engineering Task Force (IETF)

The IETF is a 'self-organised group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications'[1]. In many ways the IETF mirrors the Internet, as it is an informal 'decentralised confederation of equals' (Davidson et al. 2002:7). Its work revolves around 'the development and evolution of the core networking protocols (such as TCP/IP) and the basic Internet applications (e.g., SMTP for e-mail)' (Davidson et al. 2002:6). The IETF essentially creates voluntary standards that maintain the interoperability and usability of the Internet. It has no official membership[2]. The work is

[1] http://ietf.org/about/

[2] http://ietf.org/about/

mostly done over the publicly available email lists, and during three annual meetings. Decisions at the meetings are made on the basis of ‘rough consensus’ expressed by ‘humming’.

Over the past years the most prevalent human rights issues arising at the IETF were related to (unlawful) government or corporate surveillance of communications (Davidson and Morris 2003:11). However, in the past years more actors have been exploiting protocol weaknesses to control information, these attempts go beyond ‘simple’ surveillance and have a direct impact on human rights (Anderson 2015; Post 2015).

Protocols and Standards

Anyone who has ever used the Internet or any Internet-based service interacted with standards and protocols. Wi-Fi, exchanging songs over blue-tooth, and connecting to the Web are all made possible by Internet standards. Internet standards are ‘a numerical language that enables technical interoperability between and among heterogeneous technology products’ (Denardis 2013:6).

There is a difference between standards and protocols. Standards allow diverse systems to talk to each other; they enable 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). However, in this thesis, the terms ‘protocol’ and ‘standard’ will be used interchangeably because, for the purpose of understanding the (im)possibility of instantiating human rights in them, differentiating between the two is unnecessary.

Chapter 2. Methodology

> ‘Contemporary ethnographic endeavours must still walk a tightrope between “ethnographic thinness” and our desire to address political and economical practices.’
>
> Goldstein (2003:44)

2.1 Introduction

There is only a limited number of SDOs with an impact as wide as that of the IETF. The IETF is one of the few within that particular group that does not have any documents or organisational structures that explicitly take into account human rights principles. Yet, the IETF’s engineers encounter difficult dilemmas in this arena on a daily basis. In addition, there is limited ethnographic enquiry into the role that values (should) play in design decisions at the IETF. The combination of these factors motivated me to focus on the IETF.

Throughout this thesis I aim to walk the ethnographic tightrope. I try to balance giving an in-depth and emic analysis of the IETF’s work with contextualising the findings distilled from this ethnographic endeavour in their larger political, social and economic environment.

2.2 Research Design and Methods

This research had four stages. Initially, I gathered data from primary sources such as IETF mailinglists, Requests for Comments[3] (RFCs), video and audio content generated by the IETF. I also collected secondary sources such as popular and academic papers. In total I collected over 200 documents, and forty video and audio recordings. The amount of data gathered was substantial; hence I built a ‘lexical’ analysis tool in Python to facilitate the discourse analysis. The tool analysed all the data collected for a wide-array of concepts related to the research questions (Appendix A). The tool tracked the occurrence of a

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

keyword in a document and presented the sentence in which it occurred. This allowed me to focus in on particular documents, which indicated whether (and how) the IETF discusses human rights. The problem with Python-based lexical analysis is that it is unable to catch the 'latent meaning' (Denzin and Lincoln 2000) of words. This is where the second stage of the research started.

The Python data guided which texts to focus on. All of the data gathered was in the public domain and non-sensitive. Because it also included audio and video, I opted to use the qualitative analysis programme 'Dedoose' to perform the qualitative discourse analysis (Appendix B). For the analysis a mix of the coding, category handling, modelling and writing models as defined by Richards (2009:171) was used. 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 to update the keywords in the Python tool. This garnered additional sources to be included in the qualitative discourse analysis in Dedoose. After several cycles of discourse analysis a satisfactory level of 'saturation' (Babbie 2010) was reached and I fed the findings into the third phase of the research: ethnographic interviews and participant observation.

On the basis of the initial discourse analysis, a list of interview questions was created (Appendix C) that provided guidance during the semi-structured interviews. This particular interview method was chosen, as there was only one moment to interview the participants (Babbie 2010). Doing semi-structured interviews allowed me to be both a data 'miner' and 'traveller' (Kvale 2006: 3-5); meaning that I was able to ensure that the topics central to my research were covered, whilst granting the participants the opportunity to bring up new issues and insights.

Because the questions were informed by the discourse analysis, they resonated with the interviewees creating the necessary 'rapport' (Geertz 1975) for the interviewees to feel comfortable enough to speak freely and comment critically on design decisions made in the IETF over the years. The ethnographic stage of the research allowed me to acquire the data necessary to 'provide a holistic understanding of research participants' views and actions' (Denzin and Lincoln 2000:7).

The data of the third stage was gathered between March and July of 2015. The research period was scheduled for that time in order to take advantage of two IETF meetings, the 92nd meeting in Dallas Texas in March of 2015 and the 93nd in Prague in July of 2015. During the meeting in Dallas, the HRPC group – of which I have been a member since December 2014 – conducted over 20 interviews with various IETF members. After this point in time I conducted an additional 10 interviews.

The participants were selected through purposive sampling (Babbie 2010:184), as I was interested in getting a wide variety of opinions on the role of human rights in guiding protocol development. I also wanted to ensure that the sample was made up of individuals with extensive experience of working at the IETF in various roles. The interviewees included individuals in leadership positions (Working Group (WG) chairs, Area Directors (ADs)), 'regular participants', individuals working for specific entities (corporate, civil society, political, academic) and represented various backgrounds, nationalities and genders. I stopped doing additional interviews and participant observation after new themes ceased to emerge (Babbie 2010; Lincoln and Guba 1985) (Appendix D).

The fourth and final stage was the 'writing-up' process. By steadily returning to the different sources of data, triangulating them and holding them up to the theoretical body of knowledge, several overarching themes emerged that presented a logical narrative. The findings are given in chapter three, four, and five and supported by direct quotes and excerpts from the interviews and discourse analysis[4]. Although the IETF is extraordinarily transparent for an SDO – all its work is published online – direct conversation and

[4] Direct quotes from the interviews, or discourse analysis are indented, separated, italic and spaced at 2.0. Direct quotes from the literature over two sentences are indented, separated, not italic and spaced at 1.15. This to make a clear difference between quotes that come from the data analysis and longer quotes that come directly from the literature.

participant observation wielded results that could not have been gathered solely through textual or statistical analysis of the secondary and primary sources.

Limitations

This research method and design has various limitations. I recognise that my research is limited by the biases of the interviewees, the researcher (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 the views of one engineer, the data was triangulated (Harvey 2011) with the findings of the discourse analysis, the literature review, and participant observation. According to Richards (2009), data triangulation mitigates some of the issues surrounding 'double hermeneutics', as well as purposive sampling, inherent to this research.

Throughout the research I was aware of the fact that my methods, design, and narrow focus meant that my findings are at best 'partial', and at worst 'partisan' (Denzin and Lincoln 2000). However, as Denzin and Lincoln (2000) 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.

Quantitative research – and its ability to generalise findings to a large population – would be a great asset to some of the knowledge gaps identified in the literature review of this research. However, such quantitative research is often built upon qualitative research (Richie and Lewis 2003). Or as Blee and Taylor (2002:109) explain: qualitative findings (like those presented in this research) are best seen as 'data enhancers' that bring new insights to the foreground, making it possible to detect aspects of the object of research that would otherwise be missed, and might spur additional qualitative and quantitative research.

The Role of the Researcher and Ethics

In qualitative research 'researchers are an intricate part of the creation of meaning' (Denzin and Lincoln 2000:3). They are not neutral vessels, but rather 'embodied beings' in the social space they research (Ahmed 1999; Butler 2013). In order to clarify how I influenced the research it is important to situate me within my larger context. I am part of a research group at the London-based NGO 'Article 19' working on human rights and the Internet. I am a white woman from a Northern European country with an educational background in anthropology and human rights. As an academic, with no training in technical engineering or experience with the IETF, the initial reaction of the engineers to my presence was not amicable. Some of this sentiment undoubtedly spilled over into the interviews. This hurdle was however quickly overcome by my participation in the IETF's work.

In order to gain access to (and a deeper understanding of) the work of the IETF, participating in the mailinglists and conferences proved imperative. I contributed to the IETF's work through my role as a participant in the HRPC group (Appendix E). Active participation turned out to be crucial not only for building rapport, but also for receiving on-going feedback from the community on my findings, ensuring that they were 'thick' (Geertz 1975), credible, trustworthy, and dependable (Babbie 2010; Lincoln and Guba 1985).

This research is in line with the ethical framework for research on human subjects as laid out by the Central University Research Ethics Committee (CUREC) of the University of Oxford. All participants were informed about the purpose and potential risks (Appendix F). As most interview participants preferred anonymous attribution, the decision was made to apply this to all the interview excerpts presented in this research (Appendix G).

As the work of the IETF is publicly available, the energetic reader could attempt to attribute quotes taken from the RFCs and mailinglists to the individuals who produced them. Given this situation, I ensured that quotes from the interviews could not be linked back to quotes from the RFCs, by not using the interview quotes that directly overlap with RFCs or gave other indications of the identity of the interviewee. Considering the fact that the IETF engineers are aware that all their work on mailinglists and RFCs is publicly available, using these primary sources did not raise additional ethical concerns.

Chapter 3. How Anarchy Works[5]

‘We reject kings, presidents and voting.
We believe in rough consensus and running code.’

(Clark 2010)

3.1 Introduction

This famous, and often repeated, statement represents one of the foundational beliefs of the Internet Engineering Task Force (IETF). The IETF tries to embody this principle, leading to – from an outsider’s perspective – somewhat anarchic working procedures. These idiosyncratic procedures make it hard to discern how values and norms become embedded in the Internet’s architecture or to discover the normative framework that underlies the design choices made at the IETF. Yet, this chapter will provide an answer to these questions by presenting the following two arguments.

First, the four architectural design principles on which the Internet is built are based upon a normative understanding of what the Internet is, and should do. Second, the particular make-up of the IETF participant base reinforces this normative understanding of the Internet. Jointly, these arguments showcase the normativity at the base of the creation of Internet protocols at the IETF and the overlap between protocols and human rights. These are crucial steps to answering questions about whether human rights should be instantiated in protocols.

3.2 Architectural Values?

The Internet was built on the basis of the following four key architectural principles: openness, interoperability, redundancy, and the end-to-end principle (Clark 1988). The IETF’s work is guided by these technical principles (Baran 1964; Clark et al. 2005;

[5] Title of the 1995 article in Wired “How Anarchy Works.” http://www.wired.com/wired/archive/3.10/ietf.html

Denardis 2014; Galloway 2004). Undoubtedly, there are other technical principles that could be named as crucial to the work of the IETF, and through which the same narrative about the underlying normative conceptualisation of the Internet could be shown. However, due to the historical importance of these principles to Internet architecture management the focus will be on these four. The following paragraphs will show how these architectural principles are maintained, operationalised, and challenged at the IETF.

Openness, Permissionless Innovation, and Content Agnosticism

Openness refers to the 'absence of centralised points of control – a feature that is assumed to make it easy for new users to join and new uses to unfold' (Brown and Ziewitz 2013:16). It is at the heart of the rapid expansion of the Internet (Mueller 2004; Benkler 2006; Zittrain 2008) and central to the work of the IETF (Denardis 2014; Rachovitsa 2015). One engineer describes the importance of permissionless innovation as follows:

> *I can work on my app and that does not have to affect your. You can work on yours independently, and we can both succeed. We are not tied together in what we do, and I do not have to have an agreement with the network that I have to have this particular application. I can run any kind of traffic over the network.*

Another said:

> *The overriding principle that I would want to raise here [as crucial to the work of the IETF] is permissionless innovation. That we can keep on building on top of the Internet (...) I think that is fundamental.*

A second way openness functions within the IETF is through content agnosticism. Content agnosticism is the principle that packages get transferred across the network, regardless of their content or destination. Although many consider it to be good engineering practice (Cooper 2013), content agnosticism is under pressure. The recent debates over net neutrality being but one example of dominant market forces, like Internet Service Providers (ISPs), not necessarily subscribing to the notion that 'all packets are equal' (Thompson 2013:113).

This suggests that the IETF is not a utopic SDO in which the four principles are adhered to religiously. In fact, there are many market incentives for the engineers to ignore these principles. One of the more worrying developments is the market's move towards a locked-in or 'walled garden' approach to software development (Benkler 2006; Zittrain 2008). As one engineer said:

> *If we can engineer the protocols and engineer the market so that we have a more level playing field, that is better for users. (...) The web unfortunately tends to push things into silos now.*

This commercial development is a challenge to the architectural principles and also influences the principle of interoperability.

Interoperability

The Internet is often mistakenly seen as one net, while in reality it consists of a large network of networks that interoperate (Force Hill 2013:10). Standards and protocols are key to interoperability, allowing different systems to talk to each other. Interoperability is at the core of the work of the IETF, as proposed Internet specifications will only become Internet standards if they contain interoperable implementations (Bradner 1999). The issue of interoperability is inherently linked to some of the concerns raised above about commercial pressures. The IETF attempts to stay politically neutral in such discussions that pit commercial developments against technical principles, by emphasising the importance of interoperability to the technical functioning of the Internet. Or in the words of one engineer:

> *The role of the IETF should be mostly focused on standards, or trying to harmonise technological practices in the Internet, to facilitate interoperability. I do not think the IETF itself should be the field for societal discussions at large.*

Yet, other IETF attendees acknowledge that their personal and political views are linked to their focus on maintaining certain technical principles, like interoperability. Or, as one interviewee representing civil society at the IETF said:

> *I am here at the IETF, to make sure that the protocols that we end up developing and that people will end up using actually embed some of the protections, like privacy and end-to-end encryption, that I want people to have when they communicate with each other online.*

Thus far the findings echo the literature review: commercial, political, technical and personal factors influence design decisions (Clark et al. 2005; Denardis 2013; 2014; Lessig 2006). But this chapter will show that both the technical and social values that guide IETF engineers are based on a shared conceptualisation of what they want the Internet to look like and be used for. This shared conceptualization of the Internet has underpinned engineering choices since its birth, as the following paragraph will show.

Redundancy and the Distributed Architecture

The development of the Internet as a distributed network is both the result of the technical strength derived from having a redundant number of nodes (Baran 1964), and the political view of its creators on the dangers of too much centralised control by any one entity (Abbate 2000; Clark 1988; Naughton 1999). Again, we see the confluence of technical design principles with socio-political values. In addition to seeing the technical importance of redundancy reflected in the Internet's architecture, and the IETF's RFCs, its social importance was also emphasised during the interviews:

> *It [redundancy] is very important because it is a very old law in political science that when someone has power they abuse it. (...) One of the best ways to limit this risk is to distribute the data, if you have many actors each having a little power it will be much more difficult for anyone to seize, or to watch, or to control the Internet.*

The concept of the distributed architecture is important to IETF engineers, from both a technical and social perspective. As another engineer explained:

> *If you have a totally centralised architecture and someone wants to take out your network, they take out the centre, and good luck to all of the rest of the nodes. Being decentralised in that sense – of not having one central point that can be taken down and cause a total collapse of the network – is obviously important.*

After the dragnet surveillance practices of various intelligence agencies became public in the summer of 2013, the IETF became more engaged with the discussion about its responsibility to use the four architectural principles to develop value-sensitive technology (Rachovitsa 2015). On this subject one technical engineer said:

> *The role of the IETF – formally – is only about defining the architecture and defining the technologies that are applied to achieve the architecture, and provide the global Internet. As long as the IETF adheres to these principles of decentralised and distributed control, the architecture and the technologies enabling it [the global Internet] will prevail.*

These statements indicate that the IETF follows the four fundamental principles both for their technical strength and because of its intentions to create a particular type of Internet. An Internet that is reliable, open and globally accessible. This will become even more evident when considering the IETF's commitment to the end-to-end principle.

The End-to-End Principle

The end-to-end principle is one of the most cited architectural principles of the Internet (Clark 1988; RFC 1958). It refers to the notion that:

> A mechanism should not be placed in the network if it can be placed at the end node, and that the core of the network should provide a general service, not one that is tailored to a specific application (Clark et al. 2005:7).

Or as one engineer explained it:

> *The idea of end-to-end connectivity is that if you are connected to the Internet, and someone else is connected to the Internet you can definitely communicate.*

The end-to-end principle is important for innovation and reliability. But like the other principles it is being eroded by commercial and political developments (Clark at all 2005; Force Hill 2013; Zittrain 2008). This was echoed in the interviews:

> *Some of the essential characteristics [of the Internet] have already been lost – so it is not a matter of preserving them, it is a matter of resurrecting them. End-to-end is a good example: it is already dead. It can be resurrected, it can be reinstated but in today's Internet you do not have end-to-end access most of the time.*

Yet, even in the face of pressures to move away from the end-to-end principle, the engineers emphasise its importance, and build technologies that maintain it:

> *Re-establishing end-to-end connectivity I think is a very important point. It is really key actually. The ability for any device to communicate with any device is a crucial aspect of the Internet's ability to continue to function as a platform for free speech.*

The findings presented suggest that IETF engineers conceptualise the Internet as a fundamentally open, accessible and free platform for unhindered connectivity. The four architectural design principles at the foundation of the Internet's standards and protocols are not solely technical. Rather they are rooted in a shared normative understanding amongst IETF engineers of what the Internet is. Looking at 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 holds 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 thus strives to create an Internet that is a global network of networks that provides unrestricted connectivity for all users and usages at any time. Or, in the words of one engineer:

> *In so far as there is any broader ethic in the Internet community it is that everyone should be able to talk to everyone freely. That one principle seems to be pretty well grounded, and for the most part has been upheld.*

This particular conceptualisation of the Internet can also be seen in the IETF's mission statement:

> *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 (RFC 1958).*

This statement clarifies how 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[6]), it becomes clear that the IETF is focused on creating a particular Internet, a network with the fundamental goal of connectivity.

[6] It would be a fundamentally different Internet, but that is precisely the point.

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 essential to basic human rights such as freedom of expression (Dutton 2011; UNESCO 2015). Assuming that connectivity is the ultimate underlying normative objective of the network means acknowledging there is a clear relationship between the architecture of the network and the right to freedom of speech. Clarifying the specific connection between the Internet's architecture and human rights is important, as it is crucial to understanding why – as will be argued in chapter five and six – the right to freedom of speech cannot be instantiated in protocols.

3.3 The Personal is Protocol

The previous paragraphs showed that design decisions are influenced by the four technical principles (openness, redundancy, interoperability, end-to-end) commercial forces, political pressures, and the engineers' shared conceptualisation of the Internet. But the personal ethics of the individuals participating in the IETF also colour standards and protocols (Abbate 2000; Denardis 2013; 2014; Naughton 1999). The interviewees readily acknowledge this:

> *You are getting the value system of the different participants. Every time you make a technical choice, there is a set of values. Who is allowed to do what when you are designing a network protocol? You have to make those decisions and you tilt the ability of the different players different ways by making them.*

Likewise, another engineer explained:

> *Formally, the decisions that people make in the IETF are based on their own considerations; think of their own morals or ethics. They figure that [their personal ethics] out and they express their technical preferences and that is what we use to do arguments. (…) In a perfect world, they bring their own ethics, they bring their own business motivations, they bring any other kind of motivations they have and they translate that into their technical comments and decisions.*

Personal values and ethics thus guide protocol development. It is clear that '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 of mostly male (figure 1), Western (figure 2 and 3), white (author's field notes) representatives of large companies (figure 4)[7] these personal ethics are often in line with the Western democratic popular understanding of the Internet as a democratising tool for freedom of speech.

[7] The figures are presented as they were found on the IETF website. There are many flaws in the data visualizations, but as the website states: 'The technical term that experts like to use for the level of quality achieved by this tool is "crap".' The point I am trying to make however does not need perfect data visualizations, as even these figures support my point that the IETF participant base is relatively homogenous.

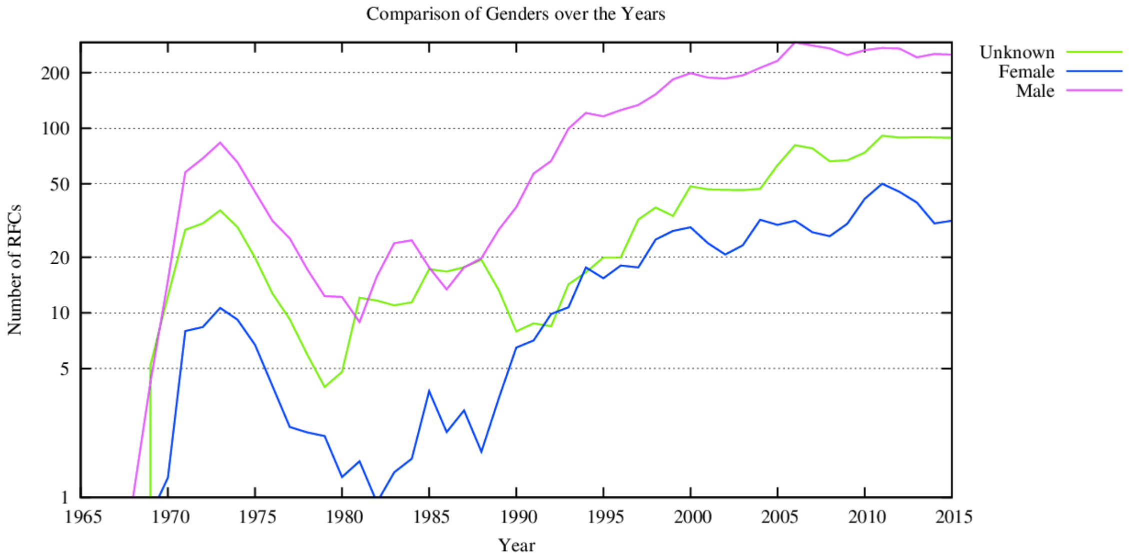


Figure 1. Authorship of RFCs, drafts, and other documents by gender over the years (Source: IETF website[8])

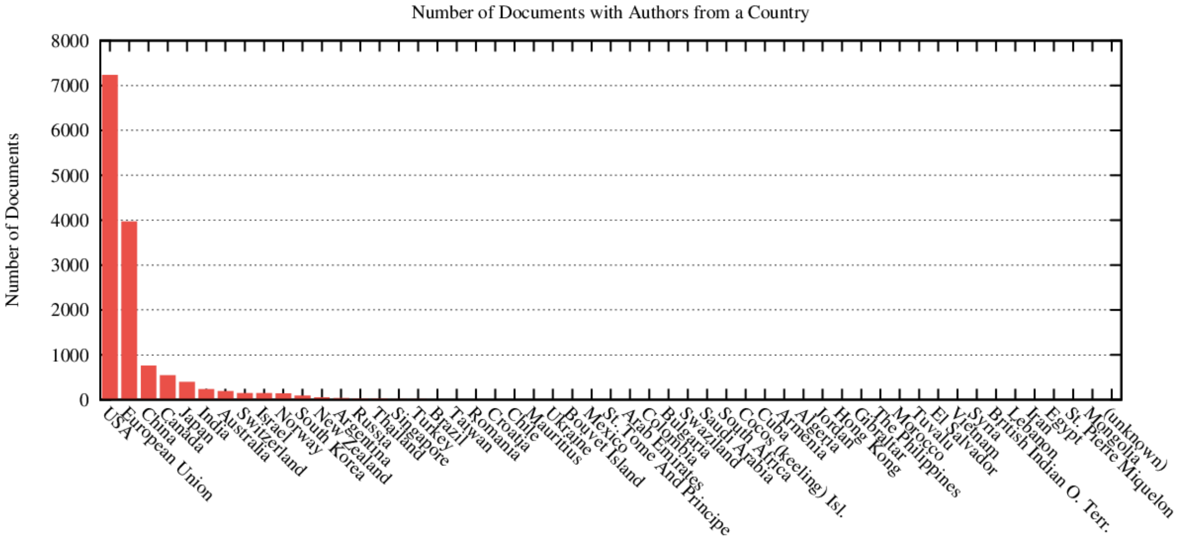


Figure 2. Distribution of documents according to the countries of their authors (Source: IETF website[9])

[8] This tracks publication of RFCs by authors of a given gender. Gender is based on the author's first name. Gender is determined either by knowing some individuals personally, or by testing the first name via genderchecker. The scale is logarithmic, normalized to 100%, representing all documents, and data has been smoothed using an exponential moving average with alpha = 0.40.

[9] Considering the EU as a country

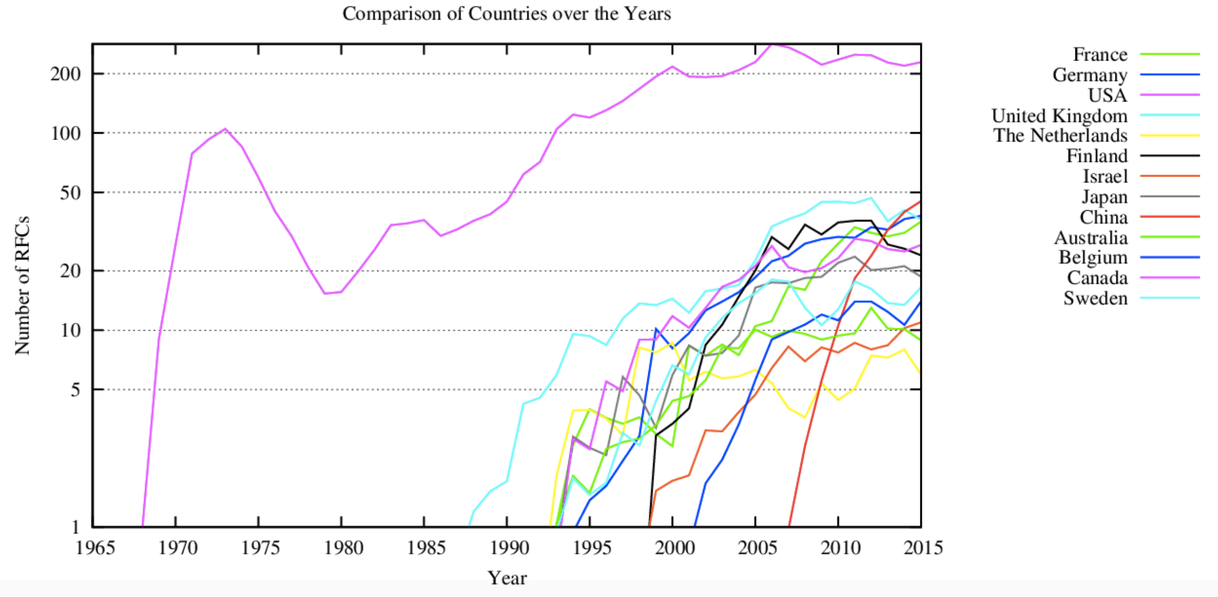


Figure 3. Distribution of countries of the authors of drafts, RFCs, and other documents plotted over the years (Source: IETF website[10])

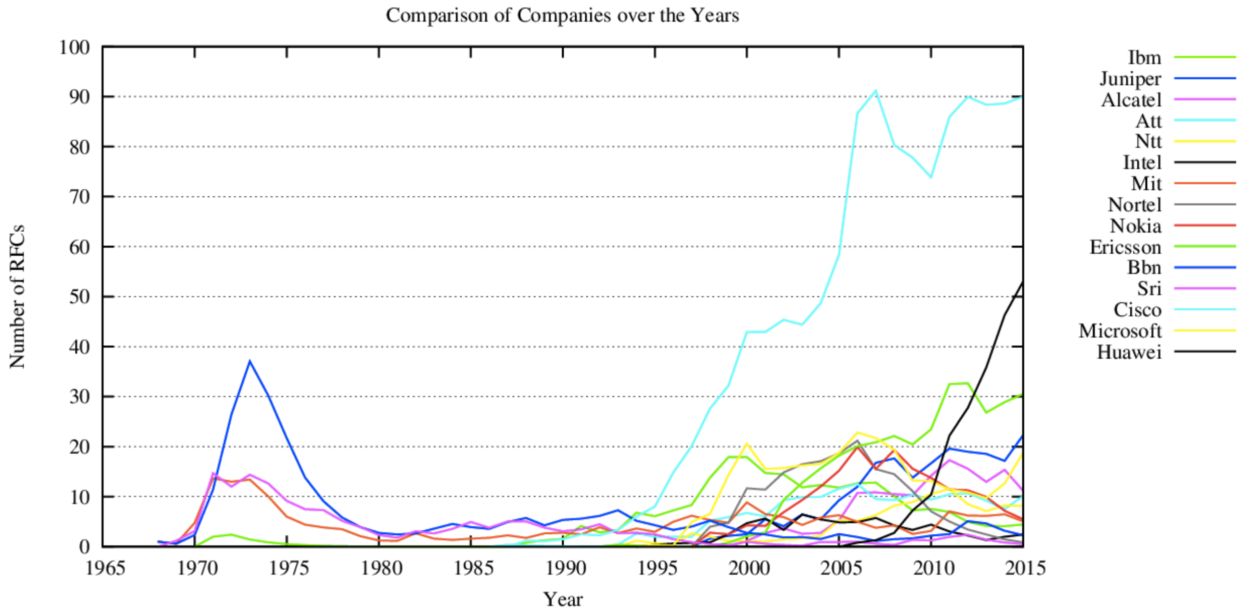


Figure 4. Companies contributing to RFCs measured over the years (Source: IETF website[11])

[10] Publication of RFCs by authors from a given country. Country data is calculated from the first occurrence of an author. The scale is logarithmic, normalized to 100% representing sum of the top countries, and data has been smoothed using an exponential moving average with alpha = 0.40.

[11] Publication of RFCs with authors from most active companies per year. Company data is calculated from the first occurrence of an author. For clarity, ISI has been excluded from this graph. The graph is normalized to 100% representing the sum of the top companies. The data has been smoothed using an exponential moving average with alpha = 0.40

In summation, although the architectural design principles are presented as technical considerations, it becomes clear that these principles are more than technical. They embody a socio-political conceptualisation of what a majority of technical engineers view the Internet to be: a connectivity-enabling platform for free speech. This conceptualisation is further reified by the fact that the IETF participants are a relatively non-diverse group with a largely shared set of 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 we decide. Politics is how that power is exercised, and by whom' (2006:59).

This chapter discussed the normative underlying framework that drives technological design decisions made by engineers, as well as the role technical and personal principles of the engineers, market, and political forces play in guiding protocol design decisions. The underlying normative framework became particularly visible in tensions and tussles between the aforementioned principles and forces influencing design decisions. Especially in those tensions arising from situations in which the engineers' conceptualization of the Internet is undermined by political or commercial developments. The next chapter will present five case studies that indicate how these tensions play out, how engineers weigh different factors and what the role should be of societal values – like human rights – in guiding protocol development.

Chapter 4. Values-by-Design: Case Studies

4.1 Introduction

This chapter will present several case studies with the aim of further understanding technical decisions made by IETF engineers, and how values become embedded in the architecture. This will be done by contextualising design decisions in their larger political and commercial environment; especially focusing on how different societal values are weighed, and eventually encoded. This research makes use of three prominent historic cases, and two contentious current cases. These cases were chosen, as they have been instrumental in shaping the debate on value-sensitive design in the IETF (Denardis 2014; 2010, Davidson and Morris 2003; Rachovitsa 2015). These cases will show that there are three conditions that need to be met for values to become encoded in protocols, and these findings will be discussed in light of the theoretical framework.

4.2 Historic Examples

The rapid expansion of the Internet and its ubiquitous presence brings new challenges to human rights, in particular the right to privacy. The rate at which individuals consume, produce, and share personal information without explicitly understanding, or consenting to, the process through which this occurs is concerning. So is the growing trend of commercial and governmental entities hovering up this data. There are many ways to protect freedom of speech online, one of which is to ensure that Internet protocols are encoded with privacy requirements (Dutton 2011; UNESCO 2015). The IETF has a long-standing history of taking privacy into account in protocol design, as discussed below.

Carnivores on the Wire

In the late 1990's the Federal Bureau of Investigation (FBI) created a computer surveillance system named 'Carnivore'. It monitored large amounts of Internet traffic, often capturing data not related to the target under investigation. This programme raised questions at the IETF of how it was inadvertently facilitating surveillance by designing protocols that are able to support (legal) interception of data flows. A mailing list was created and the following two questions were put to the community:

> *a.) Should the IETF develop new protocols or modify existing protocols to support mechanisms whose primary purpose is to support wiretapping or other law enforcement activities?*
>
> *b.) What should the IETF's position be on informational documents that explain how to perform message or data-stream interception without protocol modifications?*[12]

The debate on the mailing list was fierce[13] and revealed poignant divides in opinions. The debate did not only address the technical aspects of wiretapping but also included 'a number of normative concerns about engineering ethics, including the prospect of security engineers possibly designing something that diminishes the security of the system' (Denardis 2015:8). Several individuals who were active contributors on the Carnivore mailinglist were interviewed for this research. One engineer recalled the discussion by saying:

> *I opposed it then, and now, because it would have purposefully introduced security flaws into the system. It just sounded like bad engineering to me.*

[12] http://www.ietf.org/mail-archive/web/raven/current/msg00615.html

[13] http://www.ietf.org/mail-archive/web/raven/current/maillist.html

The issue was settled at the 1999 IETF meeting in Washington D.C. The IETF would not be including 'into IETF standards-track documents of functionality designed to facilitate wiretapping' (RFC 2804). Although the IETF refused to take an outright moral stance on the issue of wiretapping it did explicitly decide against standardising wiretapping capabilities into protocols. This illustrated that, on the issue of wiretapping, the value of privacy outweighed political pressuring by law enforcement agencies.

Doing privacy-by-design does not mean that individual companies cannot be forced to cooperate with wiretapping efforts of governments, or that surveillance on the network is impossible. However, the stance did highlight the IETF's reluctance to enable 'an industry wide standardisation effort to harmonise such capabilities' (Denardis 2015:8).

The IETF also decided not to leave room for 'tussle' (Clark et al. 2005), as it argued that there was sufficient (technical) reason and community consensus to take a definitive stance and code privacy into protocols. At the same time, the IETF steered away from explicitly mentioning privacy in the context of human rights, and firmly grounded its argumentation for non-cooperation with the FBI in technical jargon.

Pervasive Monitoring (PM)

A second example where privacy became hard-coded into the Internet's architecture is the recent debate at the IETF following the Snowden revelations about the dangers of 'Pervasive Monitoring' (PM). In the summer of 2013 various RFCs were drafted to deal with the impact of dragnet surveillance on the network. For instance, RFC 7258 'Pervasive Monitoring Is an Attack' held 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.*

This sentence 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. Revelations around the sheer scale of the monitoring, however, did deeply upset the IETF community:

> *When the NSA activities were revealed we got together to talk about it. (...) Everyone – well not everyone – what many people in the room were thinking: we built this thing to be safe, to be secure to deliver a service and what do you mean you are getting it and screwing it up? People were offended.*

The extent of the monitoring did not sit well with the community for two reasons: first, it presented a technical threat to the functioning of the network. And second, it undermined the IETF's conceptualisation of the Internet (as explained in the prior chapter) by breaking some of the fundamental architectural principles. Again, the IETF decided to encode a social value into the protocols.

But, the engineers approached the privacy breach as a technical attack that undermined trust in the network (RFC 7258), not a human rights issue. This technical approach to design decisions goes a long way to explaining why IETF engineers often do not feel a moral obligation to ensure their work does not negatively impact human rights, as will be further discussed in chapter five.

The OPES Working Group

The IETF functions by distributing tasks across different working groups. The Open Pluggable Edge Services (OPES) group developed a protocol in the early 2000s that raised policy and public interest concerns. This is the third example of how a value can get hard-coded into the Internet's architecture. Open pluggable devices are services that can be used as 'application intermediaries in the network' (RFC 3426), for instance as a web proxy cache between the original server and the client. They would be able to – with the consent of the end-user – change or filter the content passing through them. There are many legitimate technical and commercial reasons behind the development of this protocol.

Soon after the start of the OPES group, it surfaced that these devices would undermine the end-to-end principle by compromising the integrity (or the perception of integrity) of packets as they travelled over the Internet, posing serious privacy and security concerns. Various policy making organisations participated in the ensuing tussle over the work of OPES.

> In response to the concerns raised, in late 2001 the Internet Architecture Board (IAB) (which provides architectural guidance to the IETF) undertook an extensive review of the OPES proposals, and in November 2001, recommended that any work on OPES include strong protections for data security and privacy (Morris and Davidson 2003:6).

In this case, the IETF again took a stance on both the importance of security and privacy, which it favoured over particular commercial needs by mandating privacy and security to be hard-coded into technology (RFC 3238). But the IETF could not fully reverse – or even halt – the development of open pluggable devices, as the market incentive for their continued development was strong.

These various case studies indicate that the IETF, on a structural basis, goes beyond its technical mandate and gets involved in societal discussions. By taking strong stances on issues like privacy and security – values that have both technical and human rights properties – the IETF encodes values into protocols. But this is not to say that the IETF is always able to instantiate values in protocols. The IETF's ability to encode values is mediated by contextual factors like political and market dynamics. Sometimes these align with the IETF's view – and sometimes they diverge. If the IETF lacks a strong technical justification for instantiating a particular value in the protocol, it is often moved to follow the market or political dynamics.

4.3 Current Examples

The next paragraph will give two examples of on-going debates within the IETF on instantiating particular values in protocols, focusing specifically on how contextual factors like market dynamics can constrain (or enable) particular value-sensitive design decisions.

Middleboxes

On the current Internet, transparency on how packets reach a destination is no longer a given. This is due to the increased presence of firewalls, spam filters, and network address translators networks (NATs) – or middleboxes as these hosts are often called – that make use of higher-layer fields to function (Walfish et al. 2004).

This development is contentious. The debate also unfolded at the IETF, specifically at the Session Protocol Underneath Datagrams (SPUD) Birds of a Feather (BOF) meeting[14] held at the IETF conference in March 2015. The discussion at the BOF focused on questions about adding meta-data, or other information to traffic flows, to enable the sharing of information with middleboxes in that flow. During the sessions two competing arguments were distilled. On the one hand adding additional data would allow for network optimisation, and hence improve traffic carriage. On the other hand, there are risks of information leakage and other privacy and security concerns.

Repeatedly mentioned in the discussion was the danger of censorship that comes with middleboxes, and the IETF's role to prevent such censorship from happening. Or as one engineer emphasised:

[14] See https://www.ietf.org/proceedings/92/spud.html for the proceedings

> *We have to sometimes put tools in place that allow censorship; we do our best to design protocols that do not enable such features. And if problems like this arise we do try to put in additional protection for end-to-end security (...) It is a difficult problem. We do what we can.*

Middleboxes, and the protocols guiding them, influence individuals' ability to communicate online freely and privately. When asked what the IETF should do, the majority of engineers overwhelmingly answered in technical terms:

> *There are two things we can do; we can try to build protocols with end-to-end security so that the presence of middleboxes has less of an effect on user rights. We can try to build protocols that do not require the use of middleboxes. But there are a lot of real world realities that make it hard to deploy those [protocols that do not use middleboxes] right now.*

Middleboxes are becoming a proxy for the debate on the extent to which commercial interests are a valid reason to undermine the end-to-end principle. The potential for abuse and censoring, and thus ultimately the impact of middleboxes on the Internet as a place of unfiltered, unmonitored freedom of speech, is real. It is impossible to make any definitive statements about the direction the debate on middleboxes will take at the IETF. The opinions expressed in the SPUD BOF and by the various interviewees indicate that a majority of engineers are trying to mitigate the negative effects of middleboxes on freedom of speech, but their ability to act is limited by their larger commercial context that is expanding the use of middleboxes. These findings run counter to some of the established theories on how the IETF responds to protocol features that enable surveillance. Where Denardis (2015:10) holds that:

> Since the first hints of Internet commercialization and internationalization, the IETF has supported strong security in protocol design and has sometimes served as a force resisting protocol-enabled surveillance features.

This research indicates that the IETF indeed by-and-large resists efforts to standardize surveillance features into protocols when political actors drive this development. But there is much less resistance when increased surveillance is commercially motivated.

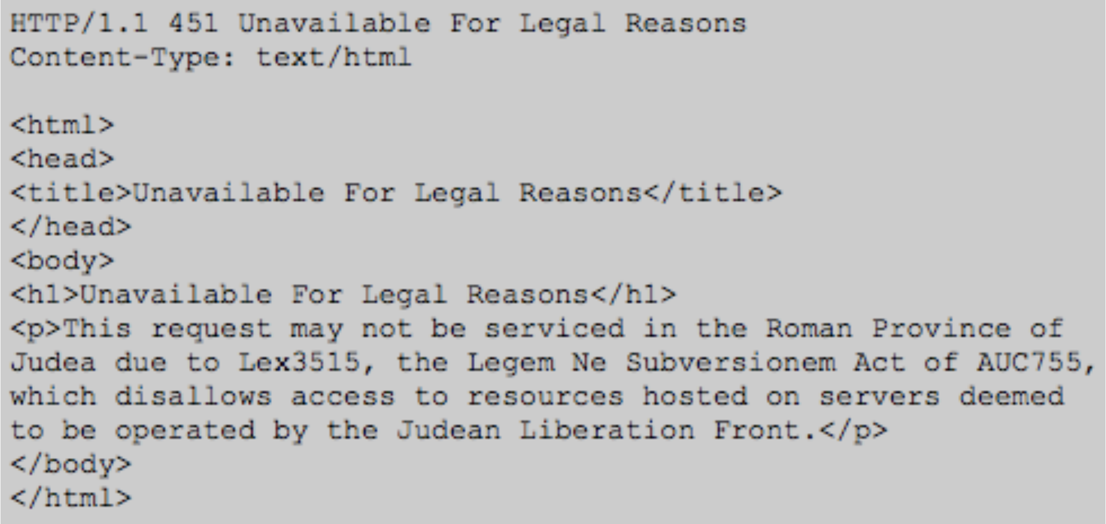
Status Code 451

Every Internet user has run into the '404 Not Found' Hypertext Transfer Protocol (HTTP) status code when trying, and failing, to access a particular website. It is a response status that the server sends to the browser, when the server cannot locate the URL. '403 Forbidden' is another example of this class of code signals that gives users information about what is going on. In the '403' case the server can be reached, but is blocking the request because the user is trying to access content forbidden to them. This can be because the specific user is not allowed access to the content (like a government employee trying to access pornography on a work-computer) or because access is restricted to all users (like social network sites in certain countries).

As surveillance and censorship of the Internet is becoming more commonplace, voices are being raised at the IETF to introduce a new status code that indicates when something is not available for 'legal reasons' (like censorship):

> The [451 status] code would allow server operators to operate with greater transparency in circumstances where issues of law or public policy affect their operation. This transparency may be beneficial both to these operators and to end-users (Bray 2012:3).

The status code would be named '451', a reference to Bradbury's famous novel on censorship. In practice the code would look like this:



```
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>
```

Figure 5. Status code 451 (Source: Website Bray, author of the 451-status code ID)

During the 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 heatedly debated. Some argued 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'[15]. Again others argued that it would be useful for individuals, or organisations like the 'Chilling Effects' project, crawling the web to get an indication of censorship (IETF discussion on '451' – author's field notes March 2015).

There was no outright objection during the Dallas meeting against moving forward on status code '451', and there will be a call for adoption in the upcoming months. What is interesting about this particular case is that not only technical arguments but also the status code's outright potential political use for civil society played a substantial role in shaping the discussion, and the decision to move forward with this technology.

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

4.4 Half-Baked

These case studies indicated that the IETF does hard-code particular values into protocols. It shows that there are three conditions that need to be met for values to becoming encoded in protocols. First, there needs to be a clear technical reason for encoding a particular value. Second, it can only be done when there is no strong commercial or, as the next chapter will show, political resistance to encoding the value in the protocols. Third, encoding the value needs to work towards maintaining the normative conceptualization of the Internet as presented in chapter three.

These findings are interesting as they put pressure on the ‘tussle theory’ argument made by Clark et al. (2005). In the cases presented, the IETF makes decisions that limit the space for tussle by elevating a particular societal value 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. first argue 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).

The cases studies indicated that the statement – that Clark et al. make later in the paper – that ‘there is no “final outcome” of these interactions, no stable point, and no acquiescence to a static architectural model’ (2005:2) is not always true. At the same time the IETF is not, as Brown et al. (2010:3) would like, purposefully ‘baking fundamental values into the architecture’. Neither of these theories fully map onto the findings presented in this chapter, and indicate the need for further theorizing in this debate.

Second, the case studies echo Lessig’s idea that:

> The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things (2006:51).

The design decision to encode particular societal values – like privacy or security – into protocols and standards have a permanent impact on the trajectory of technology, and how information flows across the networks. Decisions about information flows, in their turn, have a great impact on the shape of the technically mediated public sphere, especially the rights it protects and the practices it enables. By extension, this suggests that design decisions made at the IETF influence to what extent people are able to exercise fundamental rights like the right to freedom of speech.

Lastly, although the examples presented are by no means exhaustive they do indicate how particular values get baked into protocols. This is, however, not the same as arguing that the IETF *should* bake values into protocols. The next chapter will establish what exactly the moral responsibility is of the IETF vis-à-vis human rights and present some of the complications that emerge when trying to purposefully imbue protocols with human rights – especially freedom of speech.

Chapter 5. Human Rights-by-Design: Destroying Baghdad

5.1 Introduction

The argument that the IETF should be more cognizant of its impact on human rights is not new. It has been made by various individuals throughout its history, both within and outside of the IETF (Doria and Liddicoat 2012; Thompson 2013). Not only have several individuals argued that the IETF should take human rights into account, at different points of time the IETF has actually coded particular values - directly related to rights like freedom of speech – into protocols (as the previous chapters describe).

This chapter will give an overview of some of the challenges of trying to instantiate human rights – specifically freedom of speech – in protocols. These challenges are indicative of the larger issues surrounding value-sensitive design and largely fall under one of three different categories: philosophical, protocol-specific and practical. This chapter will also further clarify the source and type of moral obligation the IETF has to ensure its work is in line with the UDHR.

5.2 Philosophical Challenges

Many of the problems in trying to encode human rights into protocols are not technical, in the first instance, but philosophical. Attempting to do value-sensitive design, especially in reference to human rights, raises questions about technical feasibility (Clark et al. 2005) but also about the legitimacy the IETF has to act as a 'law-maker' (Lessig 2006), and the legitimacy of human rights more broadly.

Cultural Relativism and Institutional Legitimacy

Although human rights, as defined by the UDHR, are widely recognised in the Global

North they are not absolute in the legal sense of being ‘global black letter law’ (Forsythe 2006). As mentioned in the introduction of this thesis, the UDHR is part and parcel of most legal systems, but is interpreted locally. This presents some difficulties when trying to decide how to instantiate human rights’ principles in protocols and standards.

The process of encoding human rights becomes further convoluted by the fundamentally different approach governments take to defining important concepts. To interoperate and gain consensus governments need to define concepts like human rights broadly. Meanwhile, engineers define things strictly to interoperate. All of these issues are outside of the influence of the IETF, but do present real barriers to instantiating human rights in protocols. This is further complicated by the fact that the IETF does not, currently, have the legitimacy to make or protect laws (Denardis 2013). One engineer captured this perfectly by stating:

> *Asserting that IETF consensus is valid outside of the IETF context is dangerous. Because we do not speak for other people and I think it is much safer for us to live within that little bubble than it is to attempt to take on something that is really the domain of governments – who tend to speak for stakeholders that are not present at the table.*

Lessig is worried about the shift of power from legal systems to code (2006). He argues that when technological artefacts are constraining our behaviour the processes shaping these behaviours ought to be legitimised by the people subject to them. This is not currently the case for the IETF, and would be hard to achieve considering its non-formal status. Even if the IETF were to gain the legitimacy necessary to protect human rights, and encode these in its 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 (Force Hill 2013:36).

Several engineers echoed this sentiment, one argued that:

> *I do not think people appreciate how fragile the Internet and the web are. It really is just agreement that keeps it all together. If people are unhappy enough, or a jurisdiction is not happy enough with its lot, and what it gets out of the Internet and decides to go a different way, it can fall apart. It is a real threat.*

This leaves the IETF in a paradoxical situation. First, although it does not have the legitimacy to encode (and thus protect) human rights, it has in the past already made decisions, which effectively do so. Second, when the IETF does not emphasise the importance of human rights in its protocols it risks implicitly condoning political and economic developments geared towards a less open and accessible Internet. This would mean moving away from its conceptualisation of the Internet, as explained in chapter three. Yet, if the IETF does actively act upon its view of the Internet by hard-coding particular human rights' principles into the Internet, it will most likely lead to further Internet fragmentation. Such fragmentation undermines connectivity, the main goal of the IETF.

In response to these conundrums the IETF developed the aforementioned repertoire of responding to human rights and value-sensitive design questions in technical terms, and only takes up the discussion when there is limited commercial or political push-back. In doing so the IETF is implicitly suggesting that as it does not have the legitimacy to protect or encode human rights, it also cannot be held responsible for the negative repercussions of its work on human rights. This false line of argumentation will be addressed below.

Neutral or Dual Use Technology?

When analysing past and contemporary IETF debates two (slightly contradictory) lines of reasoning by IETF engineers for evading their responsibility vis-à-vis human rights become apparent. Engineers often repudiate responsibility for the potential impact of their work on human rights by arguing that the technology they build is neutral:

> *Protocols by themselves are neutral. The use of the protocols, what people do, is not. (...) In general, even things like nuclear weapons can be used for good in some cases. In general technology is neutral, the problem is that people are not neutral. And people are the ones that use technology.*

In order to deflect responsibility for how the technology is used, engineers separate their role in creating it from the technology's ability to be used for nefarious purposes. As demonstrated by this engineer:

> *For better or for worse, it [the Internet] can be used for both things [good and evil]. And it can be at the same time, a tool for expression but also potentially an instrument of state control or the control of other entities that mediate your experience there [on the Internet].*

The emphasis on the inherent neutrality of technology was also shown in the previous chapters that detailed the debate on PM, and wiretapping, in which the IETF explicitly refused to take a political stance. There is a large body of academic knowledge that argues that technology is by no means neutral because it is inherently connected to the practice of its use (Busch 2011; Franklin 1999; Galloway 2004; Winner 1977). This practice is embedded in culture, which means that technology cannot be detached from practice or the cultural context in which it is applied, and by extension, its moral and legal principles. Considering the global nature of the Internet and the many different contexts and cultures it crosses, the most relevant moral, ethical and legal framework to be upheld by those designing its nuts and bolts is the UDHR.

Following this line of reasoning, IETF engineers have a clear responsibility to ensure that human rights are accounted for in protocols. The question remains if instantiating human rights *in* protocols is the best way to achieve this goal. Clearly, the technical engineers disagree. On multiple occasions they expressed their preference for a 'technologically neutral' approach to engineering. 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 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.*

It is questionable to what extent it is possible to make this clinical separation between technology and its use (Franklin 1999). Especially, because it is precisely the ability to mediate the experience of individuals online that lies at the base of the IETF's responsibility to act in such a fashion that standards are in line with human rights. Or as Liddicoat and Doria (2012:15) argue:

> The technical community will not only be best placed but 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.

Many other international organisations that perform crucial technical maintenance work, such as ICANN, are developing methods for encoding human rights into its policies and work. SDOs like the European Telecommunications Standards Institute (ETSi) and the World Wide Web Consortium (W3C) are developing similar methods, yet the IETF seems to be trailing behind. Even though arguably its responsibility in relation to human rights is evident. Yet, there is another level of complication to address when it comes to instantiating human rights in protocols.

5.3 Protocol Specific

Engineering involves constantly balancing different priorities (Kurose and Ross 2007). The previous chapters indicated that it involves weighing shared normative conceptualisations, personal ethics, political and commercial pressures and technical principles. This process sometimes also involves balancing technical properties with protecting (particular) human rights. This paragraph will present some of the case studies discussed earlier in light of their relation to human rights, and how human rights factor into technical architecture management.

Privacy versus Security

In the post-Snowden era there is much societal debate about the need to give up the right to privacy for security. Although the debate has not settled it is clear that it is not a simple 'either/or' binary (Brown and Marsden 2013). In the case of engineering to preserve privacy and security, some technical complications arise, many related to the fact that some of the requirements to protect both properties simultaneously are contradictory. One engineer explained:

> *I talked about sourceless architecture where the packets do not carry the source of the network. It is very good for privacy but it can be a problem for security, because people could then run DDoS attacks leaving less traces. (…) Sometimes it can be difficult to have both privacy and protection against DDoS attacks. In that case there is a real trade-off, and trade-offs are complicated things.*

Another example mentioned in the interviews showed a similar technical trade-off:

> *One very good example is privacy in DDoS attacks, or the problem of spam. How to solve spam without limiting privacy? For instance, I tested bitmessage, which is a messaging system intended to be completely anonymous. A lot of effort was done to ensure there were no leaks, no meta-data available. Only ten minutes passed before I received my first spam. (…) Because of the complete lack of traceability it was impossible to defend in advance against the spam. This is a good example where you have a real trade-off to make, not the false trade-offs that the politicians suggest when they vote in the PATRIOT ACT or laws like that. But real technical trade-offs, where the solution is not obvious.*

Similar issues surrounding technical trade-offs between security, privacy, political, and commercial developments were demonstrated in the Carnivore and OPES case studies.

These cases were resolved as the IETF's approach to security and privacy was technical, and there was limited commercial pushback. The situation becomes more complicated when, in addition to these technical trade-offs, engineers are expected to weigh different rights against each other.

Freedom of Speech versus Hate Speech

The Internet is made such that it does not discriminate against particular kinds of content; this also means that it can be used for hate speech. Societies draw different lines between hate speech and freedom of speech. The ability of engineers to protect rights like freedom of speech by instantiating them in protocols is greatly complicated by the fact that different jurisdictions have different approaches to defining the boundaries between free speech and hate speech. As exemplified by this engineer's statement:

> *I come from a culture that has very particular ideas about freedom of speech. And I know that there are cultures that would consider my ideas about freedom of speech to be bad. This is a real good example of freedom of speech versus hate speech. I am not sure how I could write technology that could make censorship harder and makes monitoring harder, that does not make hate speech easier.*

Similar tensions can be seen in the debate on copyright, and restricting access to specific content for children (Brown and Marsden 2013; Castells 2001; Cavoukian 2009; Denardis 2014). The IETF is not set up to systematically weigh different technical properties that represent different degrees of protection for human rights, or even directly weigh human rights against each other. This would be a minimum requirement to instantiate human rights in protocols.

5.4 Practical Issues

Besides the philosophical and protocol specific issues there are some practical issues concerning the protection of freedom of speech by protocol design. This research identified three specific practical issues that inhibit the IETF from instantiating human rights in protocols: the protocol process is iterative, the standards are voluntary, and market forces are moving away from standardisation.

Trial and Error

The protocol creation process is iterative. Meaning that when engineers build protocols they do not always know what the protocols will be used for. The usual workflow involves building a protocol, and fixing any potential issues after the protocol is deployed. One engineer succinctly explained this situation as:

> *We know a problem arises when we are having it.*

This approach also means that it is difficult to anticipate the impact of a protocol on human rights. Some initial assessments can be made before deployment, as is currently done for privacy and security concerns, but essentially the IETF process is set up to fix problems after they occur. Not to pre-empt them. In the case of human rights, and freedom of speech in particular, estimating the potential negative impact is more complicated than with privacy, for instance. Privacy can be translated to be a technical property. Such a process does not (yet) exist for human rights. Additionally, even if it did, standards do not always get implemented according to the protocols' specifications, as will be demonstrated in the next paragraph.

Voted off the Island of Voluntary Standards

IETF standards are voluntary. Meaning that adherence to standards cannot be enforced. This complicates the ability of IETF engineers to protect any social value, including human rights. Or in the words of one engineer:

> *Traditionally the IETF's role has been to document the practices that people who are interconnecting their networks use. So that traffic from one network can flow to another network. The IETF has no concrete authority to wield. We are not going to arrest anybody for not following our protocols. We are not going to "vote them off the island". We do not have any way to force anybody to do this stuff.*

In addition, when it comes to deployment of their protocols, engineers are bound by market forces that dictate which particular protocols (and what specific parts of the spec) will be used:

> *The role of the IETF is to make protocols. (...) We specify that end-to-end is a good thing, the industry ignores us and deploys middleboxes. We say that IPv6 is a good thing, and most ISPs do not deploy it.*

On a similar note, another technical engineer argued:

> *We produce paper. Bites that get printed on paper in the IETF. And then other people implement things, and deploy things. (...) It is the implementation and the deployment, how you implement, why you implement, and whether you try and capture users, or whether you let them interoperate with anybody that*

> *creates the impact.*

The growing importance of market incentives for protocol development, also identified in the previous chapters, is problematic, especially in relationship to the IETF's ability to do value-sensitive design:

> While many private-sector participants make high-quality contributions to standards, the extent to which participants can be expected to agree about the network's architecture is diminished because of diverging market interests. Because of these changes, there is a growing risk that the public interest in standards – an ethos for many of the leading Internet standard bodies – could fade into the background of discussion among private interests. (Davidson and Morris 2003:4)

The increased lock-in of users also reduces the necessity of standardisation for companies. This commercial development in combination with the political developments laid out by Force Hill (2013) greatly reduce the ability of the IETF to uphold its conceptualisation of the open Internet, let alone instantiate human rights in protocols. The next and final chapter will provide a discussion of findings, several policy recommendations and conclusions that will clarify why the right to freedom of speech *should not* be instantiated in IETF protocols and standards.

Chapter 6. Discussion, Conclusion and Policy Recommendations

> ***SHOULD*** *This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course (RFC 2119).*

6.1 Introduction

RFC 2119 defines how words in RFCs 'should be interpreted'. The word 'should' is approached as a recommendation, not a hard requirement. Throughout this research the word 'should' played an important role. In this research it is not approached as a mere recommendation – it represents a call to action for the IETF. It refers to the necessity for the IETF to recognise its moral responsibility to ensure its work is in line with the UDHR principles. Before giving a definitive answer to the research question:

> *Should the right to freedom of speech be instantiated in the protocols and standards designed by the Internet Engineering Task Force?*

A short discussion of the findings will be given.

6.2 Discussion of the Findings

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 – openness, interoperability, redundancy and end-to-end – are presented as strictly technical, it was illustrated that these principles represent a socio-political conceptualisation of what technical engineers view the Internet to be: a medium for connectivity and by extension freedom of speech. This underlying normative framework drives technological design decisions by IETF engineers, and is reinforced by the particular make-up of the IETF participant base.

The five case studies clarified that the IETF has a clear moral obligation to ensure its work is in line with the UDHR principles. This thesis identified three particular factors as crucial to understanding situations where the IETF decided it could, and should, encode a particular social value into the Internet's architecture. First, there needs to be a clear technical reason for encoding a particular value. Second, it only happens when there is no strong commercial or political resistance to encoding the value in the protocols. Third, encoding the value needs to work towards maintaining the engineers' shared normative conceptualization of the Internet.

The case studies also clarified that commercial and political contextual factors strongly influence design decisions. In a situation where the interests of the IETF and a commercial or political player diverge, the IETF needs the aforementioned conditions to be present to be able to encode a certain value. These findings also have ramifications for the theories put forward by Lessig and Denardis, which will be discussed later. But do these findings mean the IETF *should* only encode values when it perceives it *can* do so?

This research walked a fine line between answering the question of whether human rights *can* be instantiated in protocols and whether human rights *should* be instantiated in protocols.

The debate on PM, OPES, and Carnivore, indicate that the IETF is not inclined to entertain the question if it *should* encode values when it perceives the aforementioned three basic conditions necessary so it *can* encode values, to be lacking. The current examples of the debate on middleboxes and status code '451' indicate that there is a cultural shift going on within the IETF where the first condition (a strictly technical reason for encoding a social value) is no longer an absolute requirement, but this development is in its early days.

It was argued that for various philosophical, protocol, political, and practical reasons it is – currently – not feasible or wise for the IETF to instantiate human rights in its protocols. And it is here that the reasons why the IETF could not, and should not, instantiate human rights in protocols start to overlap. It was illustrated that the IETF enables individuals to exercise their right to freedom of speech by maintaining a network of unfettered connectivity. Directly instantiating the right to freedom of speech in protocols – considering the current political and commercial climate – is likely to be counterproductive to the IETF's overarching goal of maintaining connectivity. It will lead to important market and political stakeholders opting out of the IETF, with large players like China already having made statements to that effect were the IETF to encode protocols with human rights. This would effectively create a rift in the Internet's logical layer.

When instantiating human rights – specifically the right to freedom of speech – in protocols *directly* leads to Internet fragmentation[16] it should not be done. As Internet fragmentation undermines connectivity and thereby the central freedom of speech enabling properties of the network.

Yet, the merits of attempting to make the work of the IETF more in line with the UDHR's article 19 should not be entirely dismissed, difficult as it might be. Given that, regardless of the IETF's stance on human rights, and the commercial and political context it finds itself in, its technical decisions will impact human rights. Hence, an attempt should be made to ensure that human rights become a structural part of the IETF's work. The following paragraph will give three policy recommendations on how the IETF can ensure protocol development is guided *by* human rights principles, without instantiating them *in* protocols.

[16] A careful reader will remark that if the IETF does not instantiate human rights in protocols some of the commercial and political developments mentioned in chapter four will also lead to Internet fragmentation. Although these developments are worrying and need to be addressed, the immediacy of the Internet fragmentation brought on by instantiating human rights in protocols (currently) outweighs the gradual threat presented by not instantiating human rights in protocols.

6.3 Policy Recommendations

On the basis of the findings presented in this thesis three mutually compatible approaches are identified, through which the IETF could align its work with the UDHR, without directly instantiating human rights in protocols.

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 society. This does not mean turning it into another ICANN or ITU. Rather it means finding novel ways to have human rights guide protocol development. The IETF's Internet Research Task Force's (IRTF) research group on human rights is currently spearheading this attempt. The group is creating an RFC with 'Human Rights Protocol Considerations'[17]. These considerations are modelled on the protocol considerations for privacy (RFC 6973) and security (RFC 3532), but with a specific focus on human rights. This particular format fits the IETF's structure: it is a procedure that engineers are accustomed to and it leaves enough flexibility to circumvent issues raised by Internet fragmentation or active resistance of large market players.

A second approach would be to increase the number of technical engineers that act as custodians for human rights at the IETF. Over the past twenty years technical engineers from the Centre for Democracy and Technology (CDT) and the American Civil Liberties Union (ACLU) actively participated in specific IETF working groups they identified as having a potential impact on human rights. The recent development of the RFC on privacy considerations is an example of such a procedure in which they played an important role. Both these suggestions however run the same risk that security and privacy considerations suffer from: faulty implementation or partial deployment of RFCs. Which is why these two approaches need to happen conjointly with the third strategy.

A third approach would be to emphasise the importance of the four key architectural principles as laid out by Clark et al. (2005) in protocol design. This would evade several of

[17] See https://datatracker.ietf.org/rg/hrpc/charter/

the problems of Internet fragmentation and the tendency amongst operators and implementers to ignore (from their perspective unnecessary) parts of the RFCs' specifications. This does not directly instantiate human rights in protocols but does strengthen the basic make-up of the Internet that has led to it become a crucial media for exercising the right to freedom of speech in the first place. These three options present realistic and technically feasible ways to ensure that human rights concerns are addressed within the IETF.

6.4 Discussion of Theoretical Contribution

This thesis has made three main theoretical points. First, it sheds further light on the theories put forward by Denardis (2013; 2014; 2015) and Lessig (2006). Lessig's theory on the negative influence of the market on protocol development – specifically the willingness of SDOs to take into account public interest issues, like keeping the Internet open and accessible for all – is elaborated on by the findings presented. The findings give an in-depth and detailed picture of precisely how commercial factors influence protocols and what potential negative influence this has on the Internet.

On that same note, these findings nuanced Denardis's statements on the IETF's ability, and willingness, to resist attempts by political and commercial actors to increase surveillance on the network. It was shown that, although in most cases where there is political pressure to add surveillance capabilities to the protocols the IETF actively resists such attempts; this resistance is less strong when it comes to commercial players.

The influence of the three aforementioned conditions for the IETF to encode a value, in combination with the voluntary nature of protocols, and the prerogative implementers and deployers of protocols have to ignore parts of the RFC specifications also have ramifications for the debate on the role of SDOs in developing value-sensitive design. More specifically, although the IETF has a clear moral obligation to ensure its work is in line with human rights principles building these into the design is not necessarily the most effective way to uphold these principles. These findings also have consequences for Lessig's assertion that code is law (2006).

The second theoretical contribution of this research is that Lessig's theory on the strength of 'code as law' needs further development. The case studies presented in chapter four seemed to echo Lessig's assertions about the regulatory power of code. However, the findings presented in chapter five nuanced this assertion. Although code is a strong regulator, it is not created in a social vacuum. The example was given that all current RFCs have privacy considerations, encoding privacy into the protocols and standards. Yet, due to market pressures the implementers and deployers do not always follow the RFCs' specifications, often leaving out these crucial privacy and security considerations. This research showed that currently – even when code is designed to protect a value – the influence of commercial, political, and personal interests can prevent that code from being implemented such that the protections are upheld.

This suggests that Lessig's statement that 'code is law' presents an oversimplified view of reality because it overemphasises the influence of technology on society, ignoring the socially constructed dialectic relationship between them. These findings call for additional research that further untangles the relation between technology and society, in particular as it pertains to the debate on value-sensitive design and the power of code-makers (like the IETF) to protect social values.

Third, this thesis presented the two main positions in the contemporary academic discussion on the role that human rights should play in guiding protocol development. Clark et al. (2005) argued human rights should not be hard coded into the design, as designs need room for 'tussle' to survive. Conversely, Brown et al. (2010) argued that the UDHR principles should be baked into the design.

This research showed that particular values do get baked into the design, without undermining it. This factual evidence does not refute the normative point made by Clark et al.'s tussle theory, but it does represent a problem for it to solve. At the same time, the IETF only selectively encodes values, and this represents a difficulty for Brown et al.'s suggestion in favour of UDHR principles. Neither of the theories presented thus map onto the case study of the IETF. These finding suggests there is a need for furthering theorising in this debate. Or perhaps the development of a hybrid of the two theories, that also accounts for the practical realities that encourage or inhibit human rights principles from guiding design decisions.

Overall, in this thesis it was argued that the design decisions made by 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 get encoded, when and why various commercial, political, 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 freedom of speech. Yet, it is also indispensable because this particular case study showed how the confluence of these various factors created a situation in which it is currently unfeasible – and unwise – for the IETF to directly instantiate human rights in protocols.

These insights are valuable to the technical engineers; human rights activists, policy makers, and academics interested in moving forward the debate on how human rights should (and can) become part of the work of the IETF and other standards bodies.

Works Cited

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

Ahmed, S. (1999). *Differences that Matter: Feminist Theory and Postmodernism*. Cambridge: Cambridge University Press.

Anderson, C. (2015). *The need for democratization of digital security solutions to ensure the right to freedom of expression*. Retrieved May 27, 2015, from https://citizenlab.org/wp-content/uploads/2015/02/SR-FOE-submission.pdf

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.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved May 12, 2015, from https://projects.eff.org/ barlow/Declaration-Final.html

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

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.

Bradner, S. (1999). Open Sources: Voices from the Open Source Revolution. Retrieved February 21, 2015, from http://www.oreilly.com/openbook/opensources/book/ietf.html

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

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/conext/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf

Brown, I., & Marsden, C. (2013). *Regulating Code: good governance and better regulation in the information age*. Boston: MIT Press.

Brown, I., & Ziewitz, M. (2013). A Prehistory of Internet Governance. *In Ian Brown (ed.) Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar.

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

Butler, J. (2013). *Dispossession: The Performative in the Political*. Cambridge: Polity Press.

Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

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

Centre for democracy and technology (CDT). (2000). OPES debate. Retrieved January 8, 2015, from https://www.cdt.org/files/standards/bulletin/1.02.shtml

Ceyhan, A. (2008). Technologization of Security. *Surveillance and Society*, *5*(2), 116 – 131.

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. (2010). Characterizing cyberspace: past, present and future. Retrieved May 4, 2015, from https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf on 26-05-2015

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.

Cooper, A. (2013). *How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom*. Retrieved March 1, 2015, from http://www.alissacooper.com/phd-thesis/

Creswell, J. W. (2013). Five qualitative approaches to inquiry. In *Creswell J. W, editor. 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

Davidson, A., Morris, J., & Courtney, R. (2002). *Strangers in a Strange Land: Public Interest Advocacy and Internet Standards*. Retrieved March 10, 2015 from http://link.springer.com/article/10.1007%2Fs12130-004-1027-y

Deibert, R., Palfrey, J., Rohonzinski, R., Zittrain, J., & Stein, J. (2008). *Access Denied: The practice and policy of global Internet Filtering*. Boston: MIT Press.

Demmers, J. (2012). *Theories of Violent Conflict: an introduction*. NYC: Routledge.

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

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.

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

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

European Group on Ethics and New Technology. (2014). *Ethics of Security and Surveillance Technologies*. Retrieved March 15, 2015 from http://surprise-project.eu/wp-content/uploads/2014/11/Recommendations-of-the-EGE-on-the-ethics-of-surveillance-

and-security-technologies_Kinderlerer.pptx.pdf

Force Hill, J. (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/

Forsythe, D. P. (2006). *Human Rights in International Relations*. Cambridge: Cambridge University Press.

Franklin, U. M. (1999). *The Real World of Technology*. Toronto: Toronto University Press.

Frerks, G. (2007). Conflict, Development and Discourse. In *Frerks, G. and B. Klein Goldewijk (eds.) Human Security and International Security*. (pp. 45–63). Wageningen: Wageningen Academic Publishers.

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

Geertz, C. (1975). *Kinship in Bali*. Chicago: University of Chicago Press.

Goffman, E. (1981). *Forms of Talk*. Philadelphia: University of Pennsylvania Press.

Goldstein, D. M. (2003). *Laughter out of place: Race, Class, Violence, and Sexuality in a Rio Shanty Town*. Berkeley: University of California 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

Hoffman, P. (2012). The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force. Retrieved March 5, 2015, from http://www.ietf.org/tao.html

Internet Architecture Board. (2002). RFC 3238 IAB Architectural and Policy Considerations for Open Pluggable Edge Services (OPES). Retrieved March 15, 2015, from http://www.ietf.org/rfc/rfc3238.txt

Internet Engineering Task Force. (1996a). BPC The Internet Standards Process – Revision 3. Retrieved March 13, 2015, from https://www.ietf.org/rfc/rfc2026.txt

Internet Engineering Task Force. (1996b). 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. (1999). Raven Debate The IETF's position on technology to support legal intercept. Retrieved April 3, 2015, from http://www.ietf.org/mail-archive/web/raven/current/msg00000.html

Internet Engineering Task Force. (2000a). Crypto Forum Research Group (CFRG). Retrieved May 9, 2015, from https://irtf.org/cfrg

Internet Engineering Task Force. (2000b). RFC 2804 IETF policy on Wiretapping. Retrieved June 17, 2015, from http://tools.ietf.org/html/rfc2804

Internet Engineering Task Force. (2002a). RFC 3233 Defining the IETF. Retrieved March 23, 2015, from https://tools.ietf.org/html/rfc3233

Internet Engineering Task Force. (2002b). 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

Internet Society. (2015). Definition of Internet standards. Retrieved July 4, 2015, from www.internetsociety.org/what-we- do/internet-technology- matters/open- internet-standards

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

Kaplan, B., & Maxwell, J. (1994). Qualitative research methods for evaluating computer information systems. In *Evaluating Health Care Information Systems: Methods and Applications* (pp. 45–68). Thousand Oaks CA: Sage.

Kurose, J., & Ross, K. W. (2007). *Computer Networking: A Top-Down Approach* (4th ed.). Boston: Addison-Wesley.

Kvale, S. (2006). *Dominance Through Interviews and Dialogues*. Retrieved December 21, 2014 from https://www.sfu.ca/cmns/courses/2012/801/1Readings/Kvale_dominance%20through%20interviews.pdf

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_prot ocols-_comparing_processes_and_principles28129.pdf

Lincoln, Y., & Guba, E. (1985). *Naturalistic Inquiry*. NYC: Sage.

Morozov, E. (2011). *The Net Delusion: How Not to Liberate the World*. London: Penguin.

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.

Naughton, J. (1999). *A Brief History of the Future: The Origins of the Internet*. London: Weidenfeld & Nicolson.

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/

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.

Taddeo, M. (2009). Defining trust and e-trust: Old theories and new problems. *Journal of Technology and Human Interaction*, *5*(2), 23–35.

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. (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. (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

Walfish, M., Stribling, J., Krohn, M., Balakrishnan, H., Morris, R., & Shenker, S. (2004).

Middleboxes No Longer Considered Harmful. Retrieved May 24, 2015, from http://nms.csail.mit.edu/doa

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.

Appendix A: Keywords and concepts tracked by Python lexical analyser

Round 1:

- Human Rights
- Universal Declaration of Human Rights
- Jurisdiction
- Article 19
- Freedom of Speech

Round 2:

- Human Rights
- Universal Declaration of Human Rights
- Jurisdiction
- Article 19
- Freedom of Speech
- Censoring
- Back-door
- Encryption
- Security
- Privacy
- Pervasive Monitoring
- Filtering

Round 3:

- Human Rights
- Universal Declaration of Human Rights
- Jurisdiction
- Article 19
- Freedom of Speech
- Censoring
- Filtering
- Pervasive Monitoring
- Security
- Back-door
- Openness
- Redundancy
- End-to-end

-Security considerations
- Privacy considerations
- Content agnosticism
- Open Source
- Open Standards
- Middleboxes
- Privacy
- Interoperability
- Encryption
- Lock-in
-Architectural principles
- Walled Garden

Appendix B: Coding tree Dedoose qualitative discourse analysis

Cases that put each document in the correct 'case':

1. Does the text mention human rights (explicitly or implicitly)?
   a. Yes
   b. No

2. How is the Internet conceptualised in the text?
   a. Positively
      - Enabler of Connectivity
      - Medium for Communication
      - Positive influence on Society
      - Global Connectivity
      - Public Network
      - Global Network
   b. Negatively [none found]
   c. Neutral
      - Network of Networks
      - The Architecture

3. What Architectural technical principles are mentioned as guiding design decisions?
   a. Interoperability
   b. Openness
   c. Redundancy
   d. End-to-end Principles
   e. Constant Change
   f. Internet networking layer
   g. Decentralised control
   h. Scalability
   i. Modularity
   j. Dumb Network

4. Which external factors are mentioned as influencing the design decisions?
   a. Commerce

b. Politics

c. Civil Society

5. Which concepts related to human rights are mentioned?

a. Privacy

b. Security

c. Surveillance

d. Connectivity

e. Filtering

f. Censoring

h. Monitoring

i. Attack on the Network

Appendix C: List of interview questions

Question 1: Please state your name and your current/past role in the IETF and/or surrounding environment?

Question 2: Do you think the RFCs you co-authored could impact human rights in either a positive or a negative way?

Question 3: How useful do you think security considerations are in RFCs? And why (not)?

Question 4: How useful do you think privacy considerations are in RFCs? And why (not)?

Question 6: Would you say that the decisions reached in the IETF are based on some sort of values? If so, which are these values? If not, why not?

Question 7: What are the essential characteristics of the Internet today that should be preserved in new protocol development?

Question 8: Do you believe it is possible to translate the right to freedom of expression to technical terms? If so, using which terms? If not, why not?

Question 9: Which architectural principles are crucial to the functioning of the Internet?

Question 10: What is the specific role of the IETF in the development of the Internet and how could that role evolve?

Question 11: How do you believe commercial interests influence the protocol creation process?

Question 12: How do you believe political interests influence the protocol creation process?

Questions 13: How do you believe societal interests influence the protocol creation process?

Question 14: Is there anything I did not ask that you expected me to ask?

Appendix D: Coding tree Dedoose qualitative analysis interviews and participant observation*

<u>Cases that put each document in the correct 'case' (Richards 2009)</u>

1. Does the interview/observation pertain to technical architectural principles?
   a. Yes
   b. No

   If yes, which principles were named?

   i. Openness
   ii. Permissionless Innovation
   iii. Content Agnosticism
   iv. Interoperability
   v. Connectivity
   vi. Redundancy
   vii. Distributed Architecture
   viii. End-to-end argument

2. Does the interview/observation excerpt pertain to personal ethics?
   a. Yes
   b. No

   If yes, which were named?

   i. Democracy
   ii. Cyber-utopianism
   iii. Laissez-faire
   iv. Stay of my turf
   v. Liberalism
   vi. Libertarianism

3. Does the interview/observation excerpt pertain to commercial influences?
   a. Yes
   b. No

   If yes, which were named?

   i. Market liberalism
   ii. Copyright

iii. The Big Five
iv. Network effect
v. Lock-in
vi. Walled Garden
vii. Silo-ing
viii. Generative Internet
ix. Open source movement
x. Intellectual property
xi. DRM
xii. Net neutrality
xiii. ISPs
xiv. Internet fragmentation

4. Does the interview/observation excerpt pertain to political influences?

a. Yes
b. No

If yes, which were named?

i. DRM/Copyright
ii. Surveillance
iii. Snowden
iv. NSA
v. National legislatures
vi. UN
vii. ICANN
viii. IANA
ix. US Congress

5. Does the interview/observation excerpt pertain to human rights?

a. Yes
b. No

If yes, which were named?

i. Privacy
ii. Security
iii. Pervasive Monitoring

iv. Surveillance

v. Censorship

vi. Monitoring

vii. Internet Fragmentation

* This appendix gives an overview of the initial decisions made on classifying the data within different cases. The full coding tree for the entire research includes additional codes and sub-codes for each case. The decision was made not to give the full final coding tree but present a small excerpt below for chapter 5 to show the granularity of the coding process.

Chapter 5. Destroying Baghdad [Example Coding Tree]

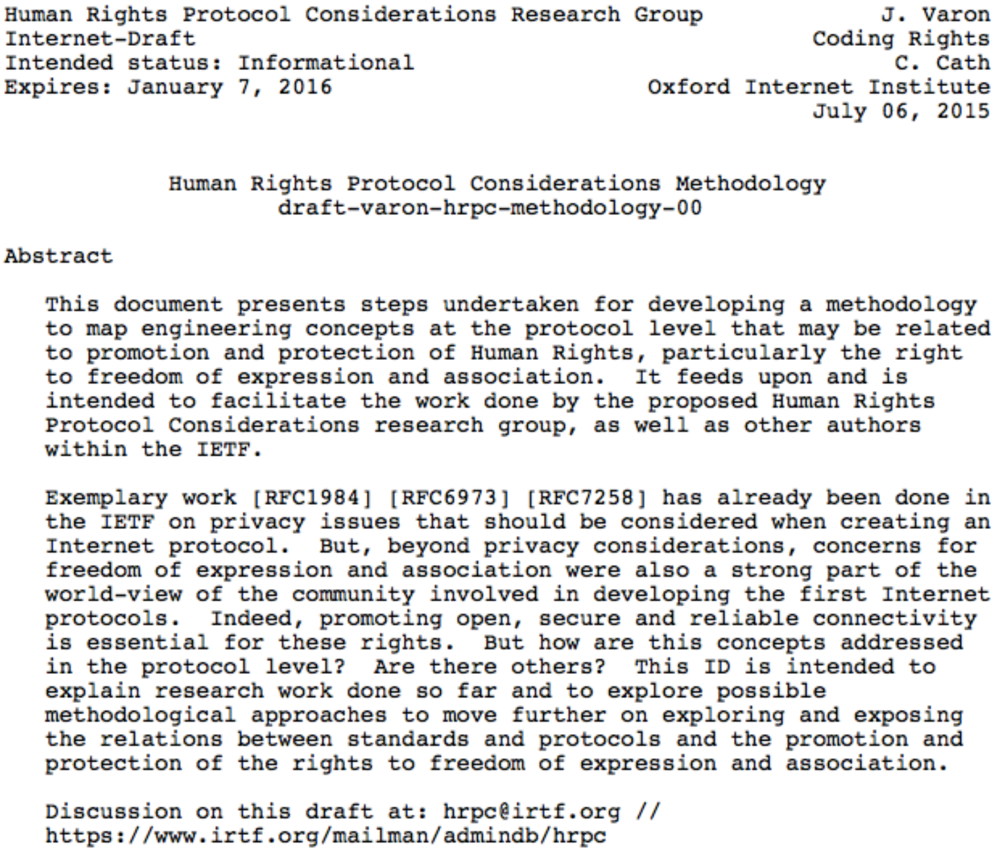
Does the interview/observation excerpt pertain to human rights?

1. Does it identify challenges surrounding instantiation human rights in code?
    a. yes
    b. no
    If yes, which?
        i. Philosophical
            - Cultural relativism
            - Legitimacy of the UDHR?
            - Legitimacy of IETF as lawmaker
            - Tech-neutral
            - Dual Use [aka Hammers and Nails]

        ii. Related to Protocols
            - Technical operationalisation of contradictory properties
            - Privacy
            - Security
            - Freedom of Speech
            - Hate speech
            - Cross-jurisdictional differences
            - Copyright
            - Rights of children online
            - Lack of procedures and processes in the IETF

        iii. Practical Issues
            - Internet is happy accident
            - Trial and error
            - Iterative process
            - Inherited systems/ legacy systems
            - Standards cannot be enforced
            - Deployers not in line with IETF
            - Market forces

Appendix E: Internet Draft by author and HRPC group member



```
Human Rights Protocol Considerations Research Group           J. Varon
Internet-Draft                                           Coding Rights
Intended status: Informational                                 C. Cath
Expires: January 7, 2016                     Oxford Internet Institute
                                                         July 06, 2015
```

Human Rights Protocol Considerations Methodology
draft-varon-hrpc-methodology-00

Abstract

This document presents steps undertaken for developing a methodology to map engineering concepts at the protocol level that may be related to promotion and protection of Human Rights, particularly the right to freedom of expression and association. It feeds upon and is intended to facilitate the work done by the proposed Human Rights Protocol Considerations research group, as well as other authors within the IETF.

Exemplary work [RFC1984] [RFC6973] [RFC7258] has already been done in the IETF on privacy issues that should be considered when creating an Internet protocol. But, beyond privacy considerations, concerns for freedom of expression and association were also a strong part of the world-view of the community involved in developing the first Internet protocols. Indeed, promoting open, secure and reliable connectivity is essential for these rights. But how are this concepts addressed in the protocol level? Are there others? This ID is intended to explain research work done so far and to explore possible methodological approaches to move further on exploring and exposing the relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

Discussion on this draft at: hrpc@irtf.org //
https://www.irtf.org/mailman/admindb/hrpc

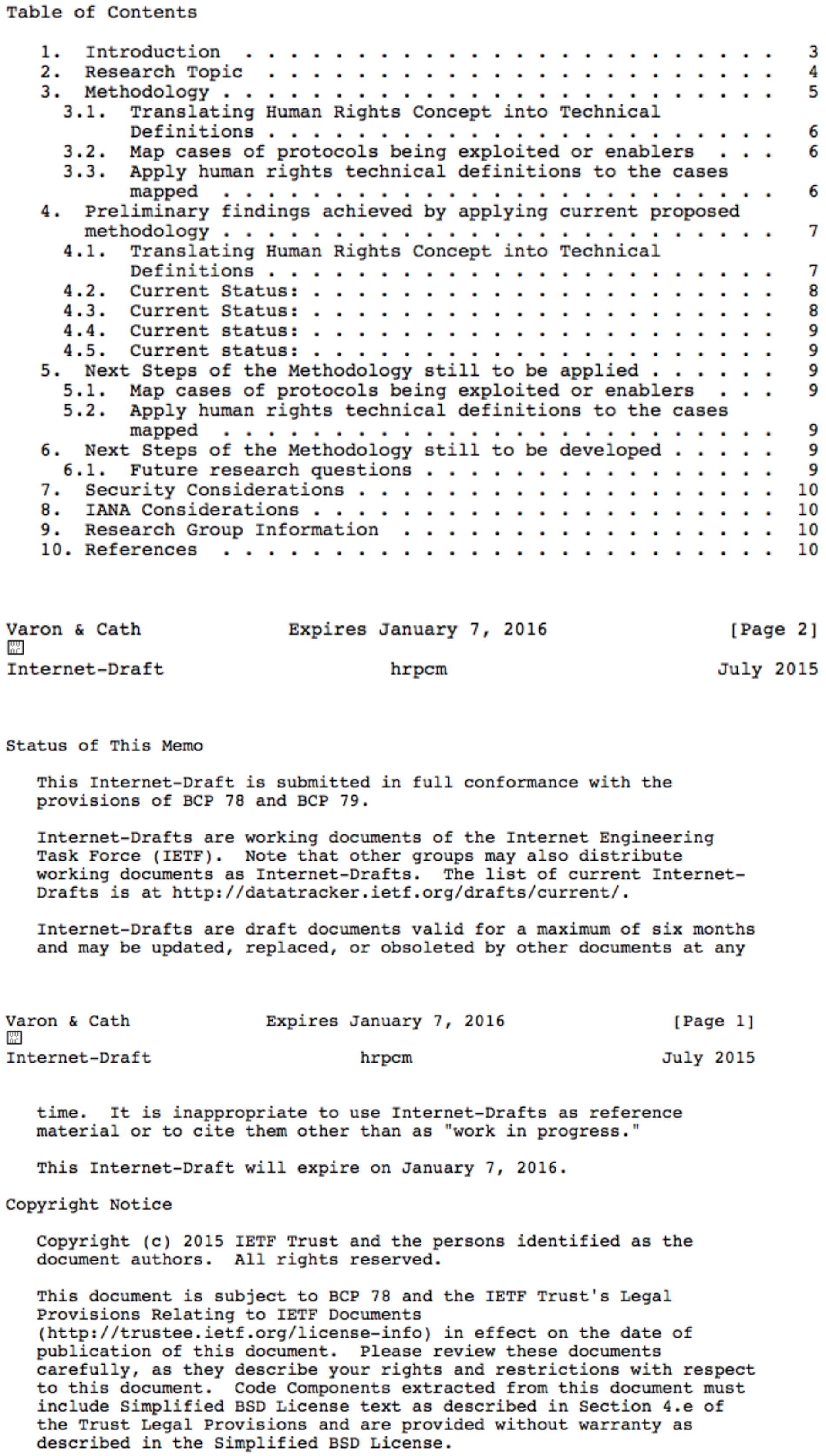


Table of Contents

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

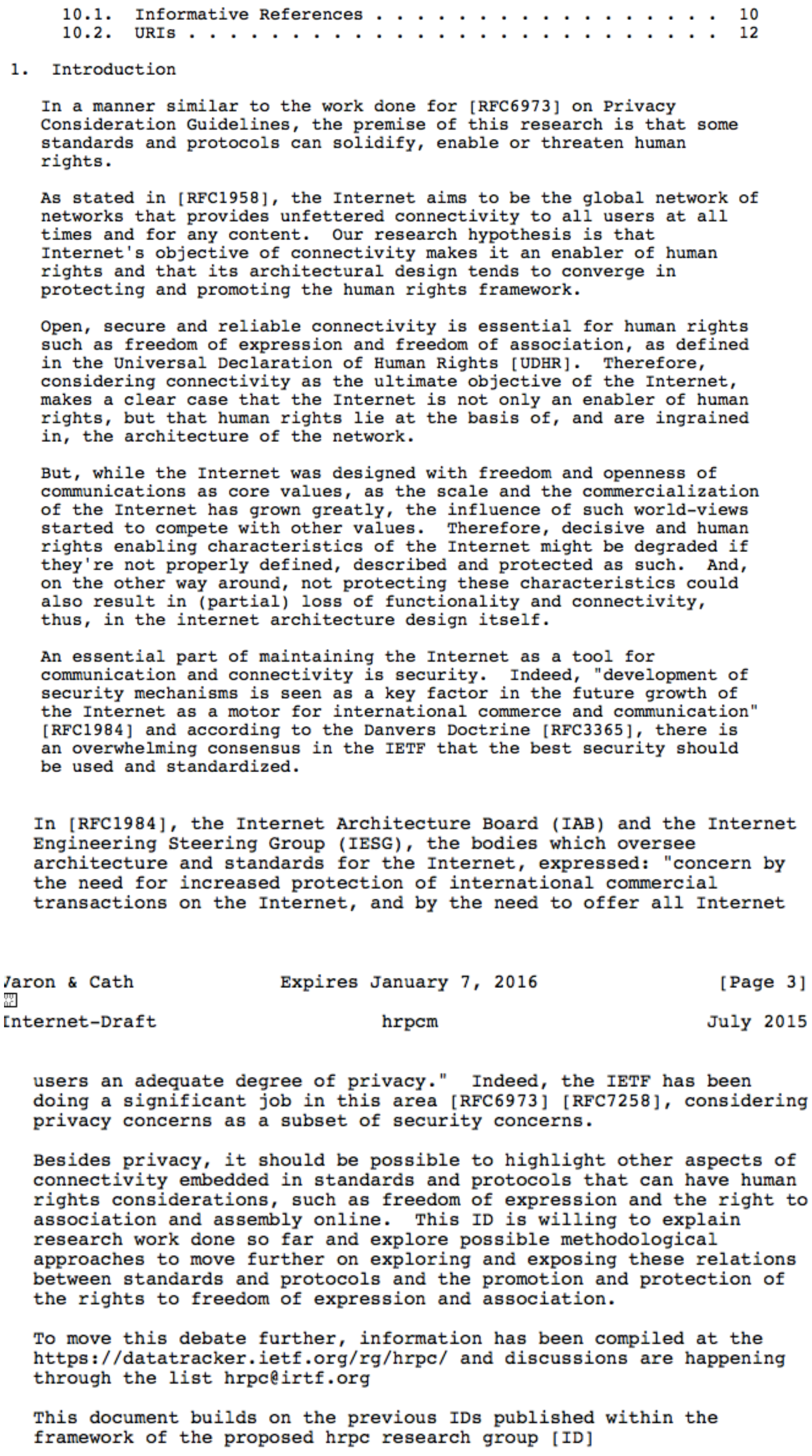
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 7, 2016.

Copyright Notice



1. Introduction

In a manner similar to the work done for [RFC6973] on Privacy Consideration Guidelines, the premise of this research is that some standards and protocols can solidify, enable or threaten human rights.

As stated in [RFC1958], the Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. Our research hypothesis is that Internet's objective of connectivity makes it an enabler of human rights and that its architectural design tends to converge in protecting and promoting the human rights framework.

Open, secure and reliable connectivity is essential for human rights such as freedom of expression and freedom of association, as defined in the Universal Declaration of Human Rights [UDHR]. Therefore, considering connectivity as the ultimate objective of the Internet, makes a clear case that the Internet is not only an enabler of human rights, but that human rights lie at the basis of, and are ingrained in, the architecture of the network.

But, while the Internet was designed with freedom and openness of communications as core values, as the scale and the commercialization of the Internet has grown greatly, the influence of such world-views started to compete with other values. Therefore, decisive and human rights enabling characteristics of the Internet might be degraded if they're not properly defined, described and protected as such. And, on the other way around, not protecting these characteristics could also result in (partial) loss of functionality and connectivity, thus, in the internet architecture design itself.

An essential part of maintaining the Internet as a tool for communication and connectivity is security. Indeed, "development of security mechanisms is seen as a key factor in the future growth of the Internet as a motor for international commerce and communication" [RFC1984] and according to the Danvers Doctrine [RFC3365], there is an overwhelming consensus in the IETF that the best security should be used and standardized.

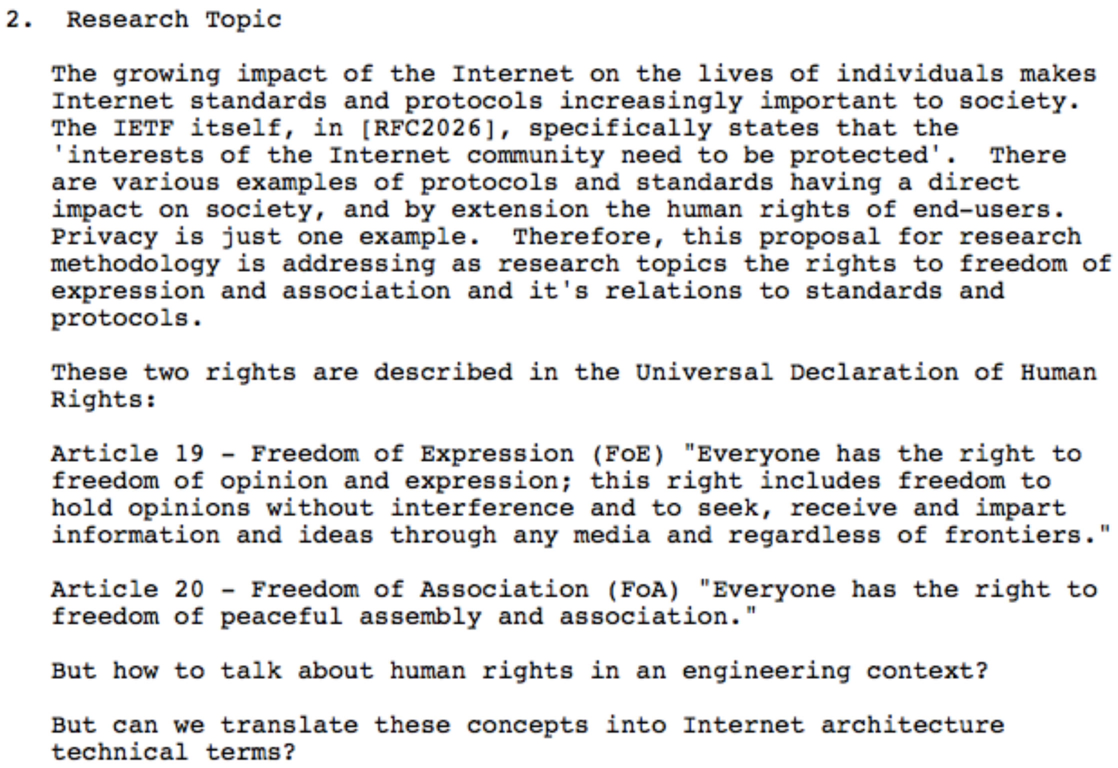
In [RFC1984], the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, expressed: "concern by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet

users an adequate degree of privacy." Indeed, the IETF has been doing a significant job in this area [RFC6973] [RFC7258], considering privacy concerns as a subset of security concerns.

Besides privacy, it should be possible to highlight other aspects of connectivity embedded in standards and protocols that can have human rights considerations, such as freedom of expression and the right to association and assembly online. This ID is willing to explain research work done so far and explore possible methodological approaches to move further on exploring and exposing these relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

To move this debate further, information has been compiled at the https://datatracker.ietf.org/rg/hrpc/ and discussions are happening through the list hrpc@irtf.org

This document builds on the previous IDs published within the framework of the proposed hrpc research group [ID]



2. Research Topic

The growing impact of the Internet on the lives of individuals makes Internet standards and protocols increasingly important to society. The IETF itself, in [RFC2026], specifically states that the 'interests of the Internet community need to be protected'. There are various examples of protocols and standards having a direct impact on society, and by extension the human rights of end-users. Privacy is just one example. Therefore, this proposal for research methodology is addressing as research topics the rights to freedom of expression and association and it's relations to standards and protocols.

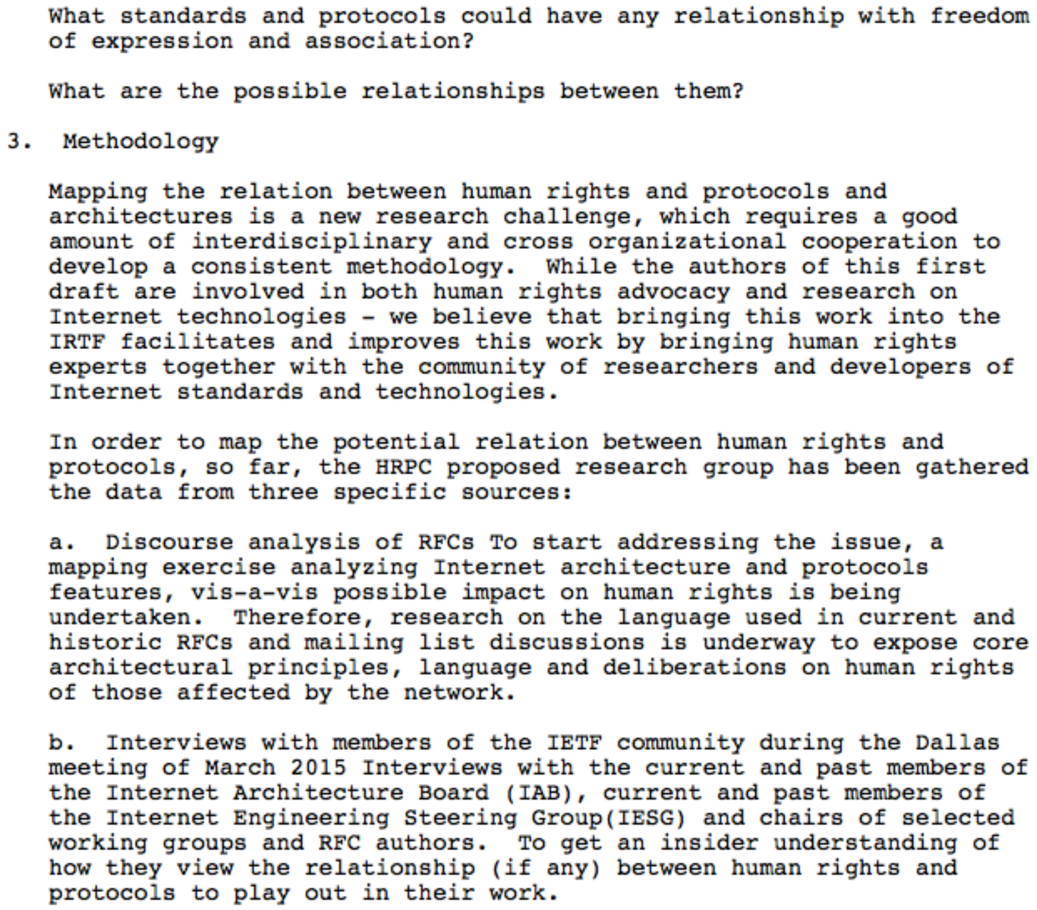
These two rights are described in the Universal Declaration of Human Rights:

Article 19 - Freedom of Expression (FoE) "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."

Article 20 - Freedom of Association (FoA) "Everyone has the right to freedom of peaceful assembly and association."

But how to talk about human rights in an engineering context?

But can we translate these concepts into Internet architecture technical terms?



What standards and protocols could have any relationship with freedom of expression and association?

What are the possible relationships between them?

3. Methodology

Mapping the relation between human rights and protocols and architectures is a new research challenge, which requires a good amount of interdisciplinary and cross organizational cooperation to develop a consistent methodology. While the authors of this first draft are involved in both human rights advocacy and research on Internet technologies - we believe that bringing this work into the IRTF facilitates and improves this work by bringing human rights experts together with the community of researchers and developers of Internet standards and technologies.

In order to map the potential relation between human rights and protocols, so far, the HRPC proposed research group has been gathered the data from three specific sources:

a. Discourse analysis of RFCs To start addressing the issue, a mapping exercise analyzing Internet architecture and protocols features, vis-a-vis possible impact on human rights is being undertaken. Therefore, research on the language used in current and historic RFCs and mailing list discussions is underway to expose core architectural principles, language and deliberations on human rights of those affected by the network.

b. Interviews with members of the IETF community during the Dallas meeting of March 2015 Interviews with the current and past members of the Internet Architecture Board (IAB), current and past members of the Internet Engineering Steering Group(IESG) and chairs of selected working groups and RFC authors. To get an insider understanding of how they view the relationship (if any) between human rights and protocols to play out in their work.

c. Participant observation in Working Groups By participating in various working groups information was gathered about the IETFs day-to-day work. From which which general themes and use-cases about human rights and protocols were extracted.

All this data was then processed using the following three consecutive strategies:

3.1. Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA Activity: Mapping of protocols and standards that potentially enable the internet as a tool for freedom of expression Expected Outcome: list of RFCs that describe standards and protocols that are potentially more closely related to FoE and FoA.

Step 1.2 - Extracting concepts from mapped RFCs Activity: Read the selected RFCs to highlight central design and technical concepts which impact human rights. Expected Outcome 1: a list of technical terms that combined create the enabling environment for freedom of expression and freedom of association. Expected Outcome 2: Possible translations of human rights concepts to technical terms.

Step 1.3 - Building a common glossary In the analysis of existing RFCs, central design and technical concepts shall be found which impact human rights. Expected Outcome: a Glossary for human rights protocol considerations with a list of concepts and definitions of technical concepts

3.2. Map cases of protocols being exploited or enablers

Step 1.1 - Cases of protocols being exploited Activity 1: Map cases in which users rights have been exploited, violated or compromised, analyze which protocols or vulnerabilities in protocols are invovled with this. Activity 2: Understand technical rational for the use of particular protocols that undermine human rights. Expected Outcome: list of protocols that have been exploited to expose users to rights violation and rationale.

Step 1.2 - Cases of protocols being enablers Activity: Map cases in which users rights have been enabled, promoted and protected and analyze which characteristics in the protocols are involved with this. Expected Outcome: list of characteristics in the protocols that have been key to promote and protect the rights to freedom of expression and association that could be added to our glossary

3.3. Apply human rights technical definitions to the cases mapped

Step 1 - Glossary and Cases Activity: Investigate alternative technical options from within list of technical design principle (see [HRPC-GLOSSARY]) that could have been applied in the mapped cases to strengthen our technical definition of FoE and FoA, and hence human rights and connectivity of the network.

Expected Outcome: Identify best (and worst) current practices. Develop procedures to systematically evaluate protocols for potential human rights impact.

4. Preliminary findings achieved by applying current proposed methodology

4.1. Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA

Below are some examples of these protocols and standards that might be related to FoE and FoA and FoE:

HTTP Websites made it extremely easy for individuals to publish their ideas, opinions and thoughts. Never before has the world seen an infrastructure that made it this easy to share information and ideas with such a large group of other people. The HTTP architecture and standards, including [RFC7230], [RFC7231], [RFC7232], [RFC7234], [RFC7235], [RFC7236], and [RFC7237], are essential for the publishing of information. The HTTP protocol, therefore, forms an crucial enabler for freedom of expression, but also for the right to freely participate in the culture life of the community (Article 27) [UDHR], to enjoy the arts and to share in scientific advancement and its benefits.

Real time communications through XMPP and WebRTC Collaborations and cooperation via the Internet have take a large step forward with the progress of chat and other other real time communications protocols. The work on XMPP [RFC6162] has enabled new methods of global interactions, cooperation and human right advocacy. The WebRTC work being done to standardize the API and protocol elements to support real-time communications for browsers, mobile applications and IoT by the World Wide Consortium (W3C) and the IETF is another artifact enabling human rights globally on the Internet.

Mailing lists Collaboration and cooperation have been part of the Internet since its early beginning, one of the instruments of facilitating working together in groups are mailing lists (as described in [RFC2639], [RFC2919], and [RFC6783]. Mailing lists are critical instruments and enablers for group communication and organization, and therefore form early artifacts of the (standardized) ability of Internet standards to enable the right to freedom of assembly and association.

IDNs English has been the lingua franca of the Internet, but for many Internet user English is not their first language. To have a true global Internet, one that serves the whole world, it would need to

reflect the languages of these different communities. The Internationalized Domain Names IDNA2008 ([RFC5890], [RFC5891], [RFC5892], and [RFC5893]), describes standards for the use of a broad range of strings and characters (some also written from right to left). This enables users who use other characters than the standard LDH ascii typeset to have their own URLs. This shows the ambition of the Internet community to reflect the diversity of users and to be in line with Article 2 of the Universal Declaration of Human Rights which clearly stipulates that "everyone is entitles to all rights and freedoms "[...]", without distinction of any kind, such as "[...]" language "[...]"." [UDHR]

4.2. Current Status:

Based on these standards and protocols, a raw list of RFCs that describe standards and protocols that are potentially related to FoE and FoA is available here: https://github.com/nllz/IRTF-HRPC/blob/master/RFC%20overview.ods

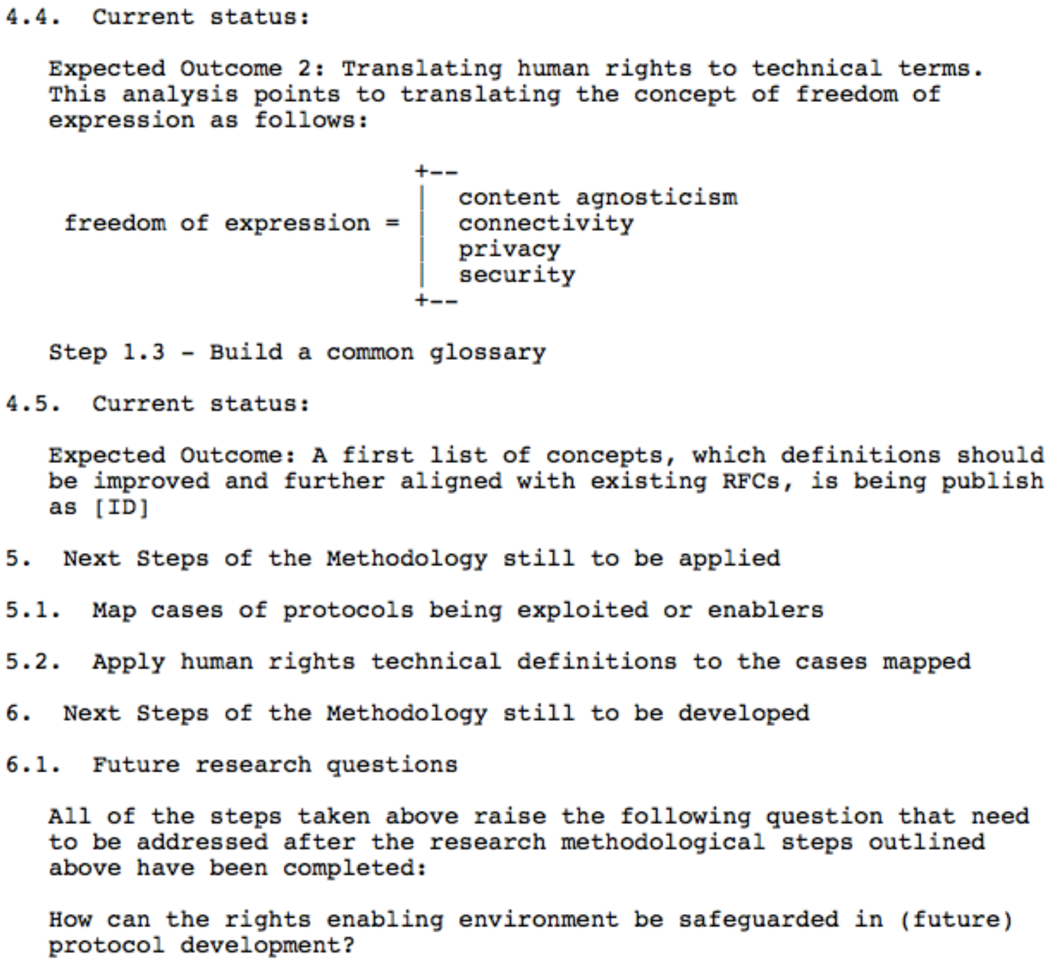
Step 1.2 - Extracting concepts from mapped RFCs The list of RFCs compiled above has used to extract our key concepts.

4.3. Current Status:

Expected Outcome 1: a list of technical terms that combined create the enabling environment for human rights, such a freedom of expression and freedom of association.

```
  Architectural principles                    Enabling features
    and characteristics                         for user rights

                     /------------------------------------------------\
                     |                                                |
+=================== |============================+                   |
=                    |                            =                   |
=                    |         End to end         =                   |
=                    |         Reliability        =                   |
=                    |         Resilience         =  Access as        |
=                    |      Interoperability      =   Human Right     |
=    Good enough     |        Transparency        =                   |
=     principle      |      Data minimization     =                   |
=                    |  Permissionless innovation =                   |
=                    |     Graceful degradation   =                   |
=                    |         Connectivity       =                   |
=                    |                            =                   |
=                    \------------------------------------------------/
=                                                 =
+=================================================+
```



4.4. Current status:

Expected Outcome 2: Translating human rights to technical terms. This analysis points to translating the concept of freedom of expression as follows:

```
                          +--
                          |  content agnosticism
 freedom of expression =  |  connectivity
                          |  privacy
                          |  security
                          +--
```

Step 1.3 - Build a common glossary

4.5. Current status:

Expected Outcome: A first list of concepts, which definitions should be improved and further aligned with existing RFCs, is being publish as [ID]

5. Next Steps of the Methodology still to be applied

5.1. Map cases of protocols being exploited or enablers

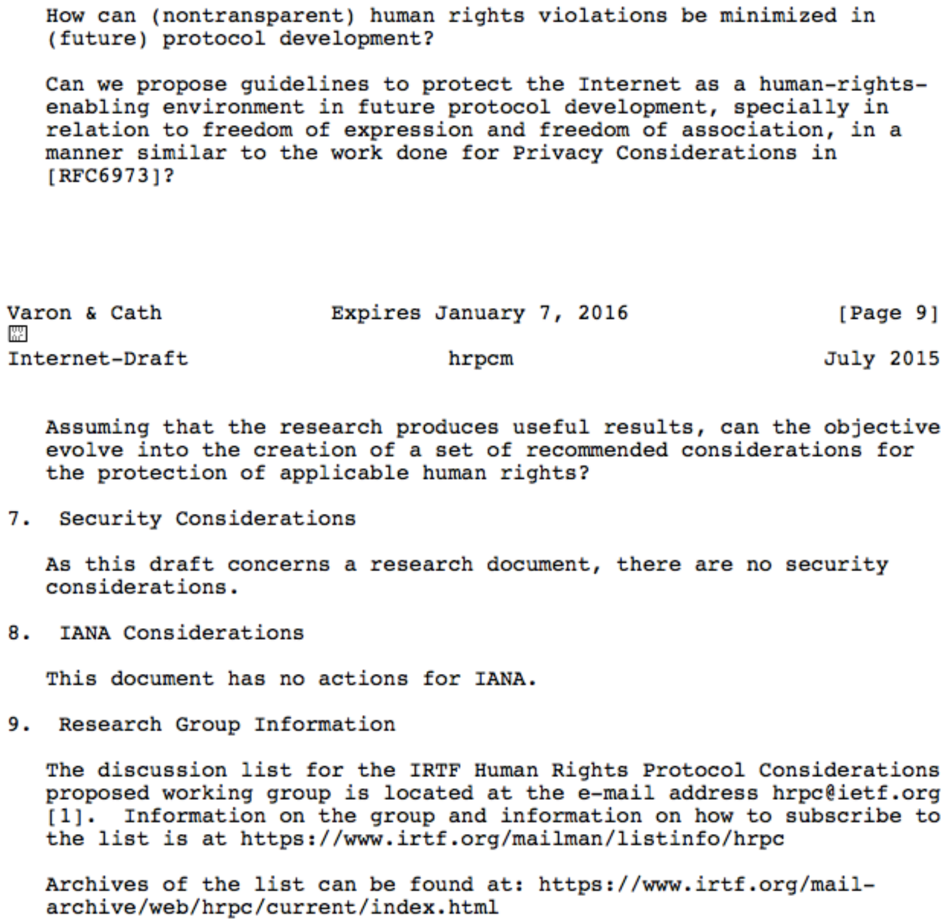
5.2. Apply human rights technical definitions to the cases mapped

6. Next Steps of the Methodology still to be developed

6.1. Future research questions

All of the steps taken above raise the following question that need to be addressed after the research methodological steps outlined above have been completed:

How can the rights enabling environment be safeguarded in (future) protocol development?



How can (nontransparent) human rights violations be minimized in (future) protocol development?

Can we propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, specially in relation to freedom of expression and freedom of association, in a manner similar to the work done for Privacy Considerations in [RFC6973]?

Varon & Cath Expires January 7, 2016 [Page 9]

Internet-Draft hrpcm July 2015

Assuming that the research produces useful results, can the objective evolve into the creation of a set of recommended considerations for the protection of applicable human rights?

7. Security Considerations

As this draft concerns a research document, there are no security considerations.

8. IANA Considerations

This document has no actions for IANA.

9. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hrpc

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hrpc/current/index.html

(Source: https://tools.ietf.org/html/draft-varon-hrpc-methodology-00)

Appendix F: Participant Information Sheet

Invitation

We would like to learn about your experiences of being involved in the IETF process and your opinion on the (im)possibility of encoding human rights into Internet protocols and standards. The following information is for helping you decide whether this is something you would be willing to do - please read it carefully. And please do ask if there are any aspects of the project that are unclear or if you would like more information about it before deciding whether or not you would like to take part in this research. If you have any questions please contact the researcher [name taken out for hand-in thesis]

What is the purpose of the study?

This study aims to fill a gap in current knowledge about the intersection between Internet Governance, Internet architecture management and human rights, in the wake of the Snowden revelations and the Council of Europe's report on ICANN's corporate social responsibilities to uphold human rights. To fill this gap, the study will collect interviews from 20-30 experts closely involved in the debate about coding societal values and/or human rights into IETF protocols, in 2014 and 2015. By using these interviews alongside discourse analysis of various IETF working groups, this project hopes to create a more in-depth understanding of changes in the approach of the IETF towards human rights proofing protocols, and thereby adding to the larger body of knowledge on the relationship between law and the Internet in general, and Internet protocols and human rights in particular.

What will I have to do?

If you would like to participate in the study we will get in touch to set up a time to talk, in person, via Skype or a secure VoIP of your choice at a time convenient to you. In order not to miss any information, if you permit it we will record the conversation, which will last no more than 40 minutes. Everything you say will be kept confidential and anonymous. You can decide which questions you are willing to answer. It is your decision to take part in this study and you can decide to stop participating at any time. The project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.

What will happen to the results of this research?

If you agree to participate in this project, the research will be written up as a master thesis. All participants are able to request a summary of the research findings should they wish to by contacting the researcher. On successful submission of the thesis, it will deposited both in print and online in the University of Oxford, to facilitate its use in future research. The digital online copy of the thesis will be deposited with the Oxford University Research Archive (ORA) and will be published with open access, meaning that it will be available to all Internet users.

We will change all the names and details of everyone we speak to – so no one apart from the researcher you speak to and the research team will know who took part in the study or what they said, unless the participants explicitly waiver this. All the data will be stored very securely on a password-protected computer, where possible with the use of encryption software. The Interviewees will be given the opportunity to see the research before publication. Once the analysis is complete the data will be deleted. All data will be held in accordance with the 1998 Data Protection Act.

Some results may be reported at academic conferences and/or published in academic journals but you will not be identifiable from these outputs. If you wish to obtain a copy of the published results, please let us know and we will send you copies as and when we write them.

Complaints:

If you have a concern about any aspect of this project, please speak to the researcher (contact details below) who will do her best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how she intends to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the chair of the Research Ethics Committee at the University of Oxford (Chair, Social Sciences & Humanities Inter- Divisional Research Ethics Committee; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD). The chair will seek to resolve the matter in a reasonably expeditious manner.

Who is organising and funding this research?

The research is organised and funded by the University of Oxford.

Should you have any questions, comments, or further information, your inquiries are most welcome at any time.

THANK YOU FOR TAKING THE TIME TO READ THIS INFORMATION

Appendix G: Snapshots of Interviews

In order to give the reader an idea of the content of the interviews below several snapshots of the interviews are presented. Some of these are part of the thesis, others informed the research but were not directly quoted.

Excerpt #1:

I had been working on technologies for what we called active emails. You could get an email with a program embedded in it but it was a program designed to be safe even if you did not trust the sender. So it was anticipating some of the problems we have now with, viruses and such made obsolete mostly by the web. In a paper that I wrote about it, I was illustrating the difference that this kind of language made by saying that you could have in any language a 'destroy Baghdad' procedures, it was about the time of the first Golf War but that in the language that had this kind of safety net around it, it would not do anything. Whereas in a normal language it could do something horrible. And then I put in a footnote after that, which has became highly quoted and is: 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.

Excerpt #2:

I do [believe that protocols impact human rights], I think that basically that our infrastructure that we use shapes the space of what is possible socially, and as a result what is possible socially impacts what people can and cannot do. And the kinds of relationships they can have with each other. I like to make an analogy with things that people can touch and experience more directly than Internet protocols, just as a Segway into this idea. I like to remind people that the way we shape public space has an effect on the kinds of rights people have and the kinds of lives people lead. For example if you design your city in a way that it has no side walks, it makes it very difficult for people who have no cars to get around and if you design your cities so that it has sidewalks everybody that can walk can get around, but maybe you design you city with sidewalks without curb cuts and people who can not walk, need to be in a wheelchair or have other mobility issues have other difficulties in getting around. The way that our infrastructure is shaped actually has an affect on the lives people lead and the kind of principles that we as a society subscribe to. So, I see our communications protocols as a similar scenario. We can set up communications protocols that anyone can use but if anyone can use them and by using them you are effectively surveilled or you can be impersonated, or you can be censored. If those protocols leave those options open than our society basically is saying we are okay with those outcomes.

Excerpt #3:

Some [shared values] are written down in documents like the IETF mission statement, which is in RFC… I don't remember. Some are explicit like in documents like RFC 1984 about surveillance and things like that. Or RFC 7258, which says that PM as done by the NSA is an attack on the Internet – so there are some values, which are somehow clearly related to human rights. For instance the right to privacy is clearly understood as an important thing for the users otherwise we wouldn't make things like privacy considerations sections.

Excerpt #4:

IP is a little trickier, no matter how well you do it with privacy preserving or privacy protecting; there will always be some leakage. And at IP level it is not too bad, for mail it is horrible. You have a whole bunch of mail headers that are at it, that for example have the sender's IP, various receive lines, message ID, subject those things do disclose information and in ways that are privacy unfriendly. How you get from there to human rights is another question, but they are privacy unfriendly. And probably mostly that because when we started doing that to mail it is because it was forty years ago; this was not really an issue. The problem is that we have had decades of deployment of things like mail and people have found good and less good uses of those headers. The impact of the kind of privacy unfriendliness of mail probably has both good effects and bad effects. The good effect is that people can use all sorts of aspects of mail to do spam filtering. The bad impacts is that people can also build business models that are not particularly privacy friendly, or they can and I am not sure this is actually happening, but governments could look at mail headers. And for some surveillance use, I am not sure there is but I do not know. But in theory you could do that.

Excerpt #5:

At the IETF we have a role in creating protocols, and we do our best to have those be end-to-end, but middleboxes are popping up. There is nothing that makes folks follow the IETF standards. So, we can go as far as we can, but then other things will happen. Governments will put policies in place; they will use things in ways that were unintended. And we do try to think through those scenarios, especially if they had not been thought through before IESG reviews; hopefully one of us picks up on those kinds of concerns. We might be highlighting it more in terms privacy, or the ability to access anything, and I have not really heard anyone think about it in terms of human rights. Unless it is something that really calls that out. If there is some obvious way for us to pick out that human rights concern, and understand what we should be looking for than we do call those out. And address those concerns. But sometimes we may just have a protocol that does not appear to affect privacy, or human rights or even help a government policy, but it could get plugged to be used that way. And some of that is out of our control.

Appendix H: Compressed coding and data handling log

Date	Data	Observation	Follow-up
February 1 – 14 2015	Literature review part I	There is not a lot of non-technical academic literature pertaining to the IETF. Moral question of the role of values/ human rights seems unanswered. Work with tussle theory (Clark et al. 2005)	Continue literature review in second week of February. Find focus and niche for the research.
February 15 – 28 2015	Literature review part II + Development methodology and research design	Interesting tension Clark et al. & Brown et al. (2010). Also identified Denardis (2013, 2014, 2015), Galloway (2004) and Busch (2011) as important sources. Decided to do combination of ethnographic interviews, participant observation and discourse analysis as outlined by Jabri (1996) and Demmers (2012). Textual analysis presents good addition to interviews, as texts can represent social relations. For qualitative coding will apply methods of Richards (2009).	Niche found in questions surrounding tussle within protocols, role of societal values, and questions surrounding how personal values factor into design decisions. Need to mitigate limitations of design and methodology. Sub-scribed to various IETF mailinglists.
March 1 – 14 2015	Started collecting primary and secondary sources about the IETF	Plethora of primary and secondary resources about the IETF. Need to find a way to scan them without having to	Built Python lexical analyser. Did four rounds of scanning and updating key

	Resolved practical issues: CUREC form, travel scholarship for fieldwork.	read hundreds of documents manually. Need to decide on platform for doing qualitative analysis after Python rounds.	words. Generated focused and limited body of primary and secondary sources to analyse.
March 15 – 31 2015	Have large body of qualitative data analysed. Moment has come to go into next phase of research: qualitative interviews and participant observation. Practical: last week of March is the IETF conference = first leg of data collection through interviews etc.	Will use Dedoose to do qualitative analysis of data, as it is non-sensitive and contains video + audio content. Data gathered through this analysis is used to inform research questions. First round of interviews went well. Questions resonated with the participants.	Update interview questions with new themes as they emerged during the interview process. Going to California for second and third rounds of interviews.
April 1 – 14 2015	Second and third rounds of interviews. Continuous analysis of additional primary and secondary sources, as these are mentioned in the interviews.	Themes continue to emerge. Met with Professor Denardis who provided me with valuable feedback on the data, and theoretical framework. Must ensure to make clear that the IETF takes up values, if there are also technical reasons.	Need for more interviews, no saturation yet. Started adding participant observation gathered from the mailinglists.

April 15 – 30 2015	Another round of interviews. Present on preliminary findings during OII lecture.	Feedback from OII community, valuable as pointed out the need to further contextualising design decisions in larger political and economic context. Ethnographic endeavour can't just stand on its own but needs to resonate in its larger political context.	Feed findings back to IETF community to get continues comments on development of research and if it's in line with the requirements for 'good' ethnographic research as laid out by Lincoln and Guba (1985) Transcribed all interviews. Now for several rounds of coding.
May 1 – 14 2015	Full Blown analysis of interviews started.	Slowly starting to see some cases and themes emerge. Still hesitant about putting them in definitive places. Coding tree is still very cluttered.	Continue to look for new cases and codes. Be open reshuffling the deck and being surprised about my own findings.

Date	**Data**	**Observation**	**Follow-up**
May 15 – 31 2015	Presented research at RIPE NCC conference in Amsterdam. See: https://ripe70.ripe.net/archives/video/108/ Reading and rereading transcribed	Presenting and getting direct feedback from the technical	All interviews are coded. First rounds fully done. Found additional cases, and also reordered data into coherent narrative,

	interviews, trying to get a better feel for the data.	community on both content and methodology is very useful. Realised that I should not wait feeding findings back to the IETF – as their comments upon my interpretation also present valuable data.	which includes a build up of three steps: 1. Values in the IETF 2. Case studies 3.Challenges to encoding human rights.
June 1 – 14 2015	So much data. There are many different narratives that could be written with the findings. How do I find the right fit?	Must ensure not to get lost in the data-forest. Went back to literature review and analysis done on secondary and primary sources,	In case of doubt: ask another researcher. Or some friends who are also anthropologists/sociologists to get some 'intercoder reliability'. Reached out to former professor at alma mater and a friend who is doing a PhD at Berkeley.

		triangulated these with my own findings to regain sense of the narrative of the research. Right now doubting coding decisions. Should I start over?	88% overlap between their coding and mine, some improvements clearly need to be made. But for now faith in my coding tree is restored.
June 15 – 30 2015	Level of saturation reached. Stopped data collection. Starting writing process.	Triangulating findings with other sources (literature and discourse analysis). The data are all assigned to their respective cases and the different categories and sub-codes.	The next step is to understand how the different sub-codes relate to each other, and to categories and see how these relations are reflected in the data. This is the moment the definitive narrative will emerge.

July 1 – 14 2015	Moving from codes to categories and back to codes. Writing large chucks of text, and reordering them continuously.	A narrative (although cluttered) is starting to emerge.	Write, rewrite, get feedback, rewrite again. T-Day is approaching.
July 15 – 31 2015	Followed discussion of IETF conference in Prague. No need for additional interviews at this point	Narrative is lined up. Feedback is collected and integrated.	Hand in the thesis.