Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft Article19
Intended status: Informational C. Cath
Expires: February 28, 2017 Oxford Internet Institute
August 27, 2016

Research into Human Rights Protocol Considerations
draft-tenoever-hrpc-research-05

Abstract

The proliferating convolution of Internet and society increases the impact of the Internet on the lives of individuals. Because of this, the design and development of the architecture of the Internet also has a growing impact on society. This has led to an broad recognition that human rights [UDHR] [ICCPR] [ICESCR] have a role in the development and management of the Internet [HRC2012] [UNGA2013] [NETmundial]. It has also been argued that the Internet should be strengthened as a human rights enabling environment [Brown].

This document provides a proposal for a vocabulary to discuss the relation between human rights and Internet protocols, an overview of the discussion in technical and academic literature and communities, a proposal for the mapping of the relation between human rights and technical concepts, and a proposal for guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations [RFC6973].

Discussion of this draft at: hrpc@irtf.org // https://www.irtf.org/mailman/listinfo/hrpc

Table of Contents

1. Introduction

"There's a freedom about the Internet: As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere."

[Berners-Lee]

This document aims to expose the relation between protocols and human rights, propose possible guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, in a manner similar to the work done for Privacy Considerations in [RFC6973], and to increase the awareness in both the human rights community and the technical community on the importance of the technical workings of the Internet and its impact on human rights.

Open, secure and reliable connectivity is necessary (although not sufficient) to excercise the human rights such as freedom of expression and freedom of association, as defined in the Universal Declaration of Human Rights [UDHR]. The Internet aims to be a global network of networks that provides unfettered connectivity to all users at all times and for any content [RFC1958]. This objective of stimulating global connectivity contributes to the Internet's role as an enabler of human rights. Next to that, the strong commitment to security [RFC1984] [RFC3365] and privacy [RFC6973] [RFC7258] in the Internet's architectural design contribute to the strengthening of the Internet as a human rights enabling environment. One could even argue 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. Internet connectivity increases the capacity for individuals to exercise their rights, the core of the Internet, its architectural design is therefore closely intertwined with the human rights framework [CathFloridi]. The quintessential link between the Internet's architecture and human rights has been argued by many. [Bless] for instance argues that, 'to a certain extent, the Internet and its protocols have already facilitated the realization of human rights, e.g., the freedom of assembly and expression. In contrast, measures of censorship and pervasive surveillance violate fundamental human rights.' [Denardis15] argues 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.' By doing so, the IETF enabled the manifestation of the right to privacy, through the Internet's architecture. Additionally, access to information gives people access to knowledge that enables them to help satisfy other

human rights, as such the Internet increasingly becoming a pre-condition for human rights rather than a supplement.

Openness of communications of the technical design fostered freedom of communication as a core value, however as the scale and the commercialization of the Internet grew, topics like access, rights and connectivity are forced to compete with other values. Therefore, important human rights enabling characteristics of the Internet might be degraded if they're not properly defined, described and protected as such. And, the other way around, not protecting human right enabling characteristics could also result in (partial) loss of functionality and connectivity, and other inherent parts of the Internet's architecture.New protocols, particularly those that upgrade the core infrastructure of the Net, should be designed to continue to enable fundamental human rights.

The IETF has produced guidelines and procedures to ensure and galvanize the privacy and security of the network in protocol development. This document aims to explore the possibility of the development of similar procedures for guidelines for human rights considerations to ensure that protocols developed in the IETF do not have an adverse impact on the realization of human rights on the Internet. By carefully considering the answers to the questions posed in the final part of this document, document authors should be able to produce a comprehensive analysis that can serve as the basis for discussion on whether the protocol adequately protects against human rights threats.

2. Vocabulary used

In the discussion of human rights and Internet architecture concepts developed in computer science, networking, law, policy-making and advocacy are coming together [Dutton],[Kaye], [Franklin]. The same concepts might have a very different meaning and implications in other areas of expertise. In order to foster a constructive interdisciplinary debate, and minimize differences in interpretation, the following glossary is provided.

Accessibility Full Internet Connectivity as described in [RFC4084] to provide unfettered access to the Internet

The design of protocols, services or implementation that provide an enabling environment for people with disabilities.

The ability to receive information available on the Internet

Anonymity The condition of an identity being unknown or concealed. [RFC4949]

Anonymous A state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals (the anonymity set). [RFC6973]

Authenticity The fact that the data does indeed come from the source it claims to come from. (It is strongly linked with Integrity, see below).

Censorship resistance Methods and measures to prevent Internet censorship.

Confidentiality The non-disclosure of information to any unintended person or host or party.

Connectivity The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958].

Content-agnosticism Treating network traffic identically regardless of content.

Debugging Debugging is a methodical process of finding and reducing the number of bugs, or defects, or malfunctions in a protocol or its implementation, thus making it behave as expected. It also includes analyzing the consequences that might have emanate from the error. Debugging tends to be harder when various subsystems are tightly coupled, as changes in one may cause bugs to emerge in another. [WP-Debugging]

The process through which people troubleshoot a technical issue, which may include inspection of program source code or device configurations. Can also include tracing or monitoring packet flow.

Decentralized Opportunity for implementation or deployment of standards, protocols or systems without one single point of control.

End-to-End The principal of extending characteristics of a protocol or system as far as possible within the system. technicall this means that intermediaries should not modify messages but simply route them to their desired end-points as capabilities should be given by the end-points, that the network then interconnects rather than controls. For example, end-to-end instant message encryption would conceal communications from one user's instant messaging application through any intermediate devices and servers all the way to the recipient's instant messaging application. If the message was decrypted at any intermediate point-for example at

a service provider-then the property of end-to-end encryption would not be present.

One of the key architectural guidelines of the Internet is the end-to-end principle in the papers by Saltzer, Reed, and Clark [Saltzer] [Clark]. The end-to-end principle was originally articulated as a question of where best not to put functions in a communication system. Yet, in the ensuing years, it has evolved to address concerns of maintaining openness, increasing reliability and robustness, and preserving the properties of user choice and ease of new service development as discussed by Blumenthal and Clark in [Blumenthal]; concerns that were not part of the original articulation of the end-to-end principle. [RFC3724]

Federation The possibility of connecting autonomous and possibly centralized systems into single system without a central authority.

Heterogenity The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and Internet service providers, each with their own separate policy concerns,there is a large heterogeneity of administrative domains and pricing structures. As a result, the heterogeneity principle proposed in [RFC1958] needs to be supported by design. [FIArch]

Integrity Maintenance and assurance of the accuracy and consistency of data to ensure it has not been (intentionally or unintentionally) altered.

Internet censorship Internet censorship is the intentional suppression of information originating, flowing or stored on systems connected to the Internet where that information is relevant for decision making to some entity. [Elahi]

Inter-operable A property of a documented standard or protocol which allows different independent implementations to work with each other without any restricted negotiation, access or functionality.

Internet Standards as an Arena for Conflict Pursuant to the principle of constant change, since the function and scope of the Internet evolves, so does the role of the IETF in developing

standards. Internet standards are adopted on the basis of a series of criteria, including high technical quality, support by community consensus, and their overall benefit to the Internet. The latter calls for an assessment of the interests of all affected parties and the specifications' impact on the Internet's users. In this respect, the effective exercise of the human rights of the Internet users is a relevant consideration that needs to be appreciated in the standardization process insofar as it is directly linked to the reliability and core values of the Internet. [RFC1958] [RFC0226] [RFC3724]

Internationalization (i18n) The practice of making protocols, standards, and implementations usable in different languages and scripts. (see Localization)

(cf [RFC6365]) In the IETF, "internationalization" means to add or improve the handling of non-ASCII text in a protocol. [RFC6365] A different perspective, more appropriate to protocols that are designed for global use from the beginning, is the definition used by W3C:

"Internationalization is the design and development of a product, application or document content that enables easy localization for target audiences that vary in culture, region, or language." [W3Ci18nDef]

Many protocols that handle text only handle one charset (US-ASCII), or leave the question of what CCS and encoding up to local guesswork (which leads, of course, to interoperability problems). If multiple charsets are permitted, they must be explicitly identified [RFC2277]. Adding non-ASCII text to a protocol allows the protocol to handle more scripts, hopefully all of the ones useful in the world. In today's world, that is normally best accomplished by allowing Unicode encoded in UTF-8 only, thereby shifting conversion issues away from individual choices.

Localization (l10n) The practice of translating an implementation to make it functional in a specific language or for users in a specific locale (see Internationalization).

(cf [RFC6365]): The process of adapting an internationalized application platform or application to a specific cultural environment. In localization, the same semantics are preserved while the syntax may be changed. [FRAMEWORK]

Localization is the act of tailoring an application for a different language or script or culture. Some internationalized applications can handle a wide variety of languages. Typical

users only understand a small number of languages, so the program must be tailored to interact with users in just the languages they know. The major work of localization is translating the user interface and documentation. Localization involves not only changing the language interaction, but also other relevant changes such as display of numbers, dates, currency, and so on. The better internationalized an application is, the easier it is to localize it for a particular language and character encoding scheme.

Open standards Conform [RFC2606]: Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be "open external standards" for the purposes of the Internet Standards Process.

Openness The quality of the unfiltered Internet that allows for free access to other hosts.

Absence of centralized points of control - a feature that is assumed to make it easy for new users to join and new uses to unfold [Brown].

Permissionless innovation The freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist.

Privacy The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. [RFC4949]

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privacy is a broad concept relating to the protection of individual or group autonomy and the relationship between an individual or group and society, including government, companies and private individuals. It is often summarized as "the right to be left alone" but it encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognized as a core right that underpins human dignity

and other values such as freedom of association and freedom of speech.

The right to privacy is also recognized in nearly every national constitution and in most international human rights treaties. It has been adjudicated upon both by international and regional bodies. The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.

Reliable Reliability ensures that a protocol will execute its function consistently and error resistant as described and function without unexpected result. A system that is reliable degenerates gracefully and will have a documented way to announce degradation. It also has mechanisms to recover from failure gracefully, and if applicable, allow for partial healing.

Resilience The maintaining of dependability and performance in the face of unanticipated changes and circumstances.

Robustness The resistance of protocols and their implementations to errors, and to involuntary, legal or malicious attempts to disrupt its mode of operations. [RFC0760] [RFC0791] [RFC0793] [RFC1122]. Or framed more positively, a system can provide functionality consistently and without errors despite involuntary, legal or malicious attempts to disrupt its mode of operations.

Scalable The ability to handle increased or decreased workloads predictably within defined expectations. There should be a clear definition of its scope and applicability. The limits of a systems scalability should be defined.

Stateless / stateful In computing, a stateless protocol is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol which requires keeping of the internal state on the server is known as a stateful protocol. [WP-Stateless]

Strong encryption / cryptography Used to describe a cryptographic algorithm that would require a large amount of computational power to defeat it. [RFC4949]

Transparent "transparency" refers to the original Internet concept of a single universal logical addressing scheme, and the

mechanisms by which packets may flow from source to destination essentially unaltered. [RFC2775]

The combination of reliability, confidentiality, integrity, anonymity, and authenticity is what makes up security on the Internet.

```
  (     Reliability          )
 (      Confidentiality       )
 (      Integrity             ) = communication and information security
 (      Authenticity          )
  (     Anonymity            )
```

The combination of the end-to-end principle, interoperability, resilience, reliability and robustness are the enableing factors that result in on the Internet.

```
    ( End-to-End      )
   (  Interoperability )
   (  Resilience       )
   (  Reliability      ) = connectivity
   (  Robustness       )
   (  Autonomy         )
    ( Simplicity      )
```

3. Research Questions

The Human Rights Protocol Considerations Research Group (hrpc) in the Internet Research Taskforce (IRTF) embarked on its mission to answer the following two questions which are also the main two questions which this documents seeks to answer:

1. How can Internet protocols and standards impact human rights, either by enabling them or by creating a restrictive environment?

2. Can guidelines be developed to improve informed and transparent decision making about potential human rights impact of protocols?

4. Literature and Discussion Review

Protocols and standards are regularly seen as merely performing technical functions. However, these protocols and standards do not exist outside of their technical context nor outside of their political, historical, economic, legal or cultural context. This is best exemplified by the way in which protocols have become part and parcel of political processes and public policies: one only has to look at the IANA transition, the RFC on pervasive monitoring or global innovation policy for concrete examples [Denardis15]. To

quote [Abbate]: "protocols are politics by other means". Since the late 1990's a burgeoning group of academics and practitioners researched questions surrounding the societal impact of protocols. These studies vary in focus and scope: some focus on specific standards [Davidsonetal] [Musiani], others look into the political, legal, commercial or social impact of protocols [BrownMarsden] [Lessig], [Mueller] and yet others look at how the engineers' personal set of values get translated into technology [Abbate],[CathFloridi] [Denardis15] [WynsbergheMoura].

Commercial and political influences on the management of the Internet's architecture are well-documented in the academic literature and will thus not be discussed here [Benkler] [Brownetal] [Denardis15] [Lessig] [Mueller] [Zittrain]. It is sufficient to say that the IETF community consistently tries to push back against the standardization of surveillance and certain other issues that negatively influence end-users' experience of and trust in the Internet [Denardis14]. The role human rights play in engineering, architecture and protocol design is much less clear.

It is very important to understand how protocols and standards impact human rights. In particular because Standard Developing Organizations (SDOs) are increasingly becoming venues where social values (like human rights) are discussed, although often from a technological point of view. These SDOs are becoming a new focal point for discussions about values-by-design, and the role of technical engineers in protecting or enabling human rights [Brownetal] [Clarketal] {[Denardis14}} [CathFloridi] [Lessig] [Rachovitsa].

In the academic literature five clear positions can be discerned, in relation to the role of human rights in protocol design and how to account for these human rights in protocol development: Clark et al. argue that 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 [Clarketal].' They hold that human rights should not be hard-coded into protocols because of four reasons: first, the rights in the UDHR are not absolute. Second, technology is not the only tool in the tussle over human rights. Third, there are inherent dangers to blunting the tools of enforcement and last but not least, it is dangerous to make promises that can't be kept. The open nature of the Internet will never, they argue, be enough to fully protect individuals' human rights.

Conversely, Brown et al. [Brownetal] state that 'some key, universal values - of which the UDHR is the most legitimate expression - should

be baked into the architecture at design time.' They argue that design choices have offline consequences, and are able shape the power positions of groups or individuals in society. As such, the individuals making these technical decisions have a moral obligation to take into account the impact of their decisions on society, and by extension human rights. Brown et al recognise that values and the implementation of human rights vary across the globe. Yet they argue that all members of the United Nations have found 'common agreement on the values proclaimed in the Universal Declaration of Human Rights. In looking for the most legitimate set of global values to embed in the future Internet architecture, the UDHR has the democratic assent of a significant fraction of the planet's population, through their elected representatives."

The main disagreement between these two academic positions lies mostly in the question on whether a particular value system should be embedded into the Internet's architecture or whether the architecture needs to account for a varying set of values.

A third position that is similar to that of Brown et al., is taken by [Broeders] who argues that 'we must find ways to continue guaranteeing the overall integrity and functionality of the public core of the Internet.' He argues that the best way to do this is by declaring the backbone of the Internet - which includes the TCP/IP protocol suite, numerous standards, the Domain Name System (DNS), and routing protocols - a common public good. This is a different approach than that of [Clarketal] and [Brownetal] because Broeders does not suggest that social values should (or should not) be explicitly coded into the Internet's architecture, but rather that the existing architecture should be seen as an entity of public value.

Bless and Orwat [Bless] represent a fourth position. They argue that it is to early to make any definitive claims, but that there is a need for more careful analysis of the impact of protocol design choices on human rights. They also argue that it is important to search for solutions that 'create awareness in the technical community about impact of design choices on social values. And work towards a methodology for co-design of technical and institutional systems.'

Berners-Lee and Halpin argue that the Internet could lead to even new capacities, and these capacities may over time be viewed as new kinds of rights. For example, Internet access may be viewed as a human right in of itself if it is taken to be a pre-condition for other rights, even if it could not have been predicted at the declaration of the UNHDR after the end of World War 2.[BernersLeeHalpin]. This

last position is interesting to keep in mind, but beyond the remit of this document.

It is important to give some background to the academic discussion on this issue. As it stems from the issues as they arise in the field of technical engineering. They also are important to document as they inform the position of the authors of this document. Our position is that hard-coding human rights into protocols is very complicated as each situation is dependent on its context. At this point is difficult to say whether hard-coding human rights into protocols is wise (or feasible). It is however important to make consicious and explicit design decisions that take into account the human rights protocol considerations guidelines developed below. This will ensure that the impact protocols can have on human rights is clear and explicit, both for developers and for users. In addition, it ensures that the impact of specific protocol on human rights is carefully considered and that concrete design decisions are documented in the protocol.

This document details the steps taken in theresearch into human rights protocol considerations by the HRPC group to clarify the relation between technical concepts used in the IETF and human rights. This document sets out some preliminary steps and considerations for engineers to take into account when developing standards and protocols.

5. Methodology

Mapping the relation between human rights, protocols and architectures is a new research challenge, which requires a good amount of interdisciplinary and cross organizational cooperation to develop a consistent methodology.

The methodological choices made in this document are based on the political science-based method of discourse analysis and ethnographic research methods [Cath]. This work departs from the assumption that language reflects the understanding of concepts. Or as [Jabri] holds, policy documents are 'social relations represented in texts where language is used to construct meaning and representation'. This process happens in 'the social space of society' [Schroeder] and manifests itself in institutions and organizations [King], exposed using the ethnographic methods of semi-structured interviews and participant observation. Or in non-academic language, the way the language in IETF/IRTF documents describes and approaches the issues they are trying to address is an indicator for the underlying social assumptions and relations of the engineers to their engineering. By reading and analyzing these documents, as well as interviewing engineers and participating in the IETF/IRTF working groups, it is

possible to distill the relation between human rights, protocols and the Internet's architecture.

The discourse analysis was operationalized using qualitative and quantitative means. The first step taken by the research group was reading RFCs and other official IETF documents. The second step was the use of a python-based analyzer, using the tool Big Bang, adapted by Nick Doty [Doty] to scan for the concepts that were identified as important architectural principles (distilled on the initial reading and supplemented by the interviews and participant observation). Such a quantitative method is very precise and speeds up the research process [Richie]. But this tool is unable to understand 'latent meaning' [Denzin]. In order to mitigate these issues of automated word-frequency based approaches, and to get a sense of the 'thick meaning' [Geertz] of the data, a second qualitative analysis of the data set was performed. These various rounds of discourse analysis were used to inform the interviews and further data analysis. As such the initial rounds of quantitative discourse analysis were used to inform the second rounds of qualitative analysis.The results from the qualitative interviews were again used to feed new concepts into the quantitative discourse analysis. As such the two methods continued to support and enrich each other.

The ethnographic methods of the data collection and processing allowed the research group to acquire the data necessary to 'provide a holistic understanding of research participants' views and actions' [Denzin] that highlighted ongoing issues and case studies where protocols impact human rights. The interview participants were selected through purposive sampling [Babbie], as the research group was interested in getting a wide variety of opinions on the role of human rights in guiding protocol development. This sampling method also ensured that individuals with extensive experience working at the IETF in various roles were targeted. 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.

5.1. Data Sources

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

5.1.1. Discourse analysis of RFCs

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

5.1.2. Interviews with members of the IETF community

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 was done at the IETF92 Dallas meeting in March 2015. To get an insider understanding of how they view the relationship (if any) between human rights and protocols to play out in their work.

5.1.3. Participant observation in Working Groups

By participating in various working groups, in person at IETF meetings and on mailinglists, information was gathered about the IETFs day-to-day workings. From which which general themes, technical concepts, and use-cases about human rights and protocols were extracted.

5.2. Data analysis strategies

The data above was processed using three consecutive strategies: mapping protocols related to human rights, extracting concepts from these protocols, and creation of a common glossary (detailed under "2.vocabulary used"). Before going over these strategies some elaboration on the process of identifying technical concepts as they relate to human rights needs to be given:

5.2.1. Identifying qualities of technical concepts that relate to human rights

5.2.1.1. Mapping protocols and standards related to human rights

By combining data from the three data sources named above, an extensive list of protocols and standards that potentially enable the Internet as a tool for freedom of expression and association was assembly. In order to determine the enabling (or inhibiting) features we relied on direct references of such impact in the RFCs, as well as input from the community. On the basis of this analysis a

list of RFCs that describe standards and protocols that are potentially closely related to human rights was compiled.

5.2.1.2. Extracting concepts from mapped RFCs

Mapping the protocols and standards that are related to human rights and create a human rights enabeling environment was the first step. For that we needed to focus on specific technical concepts that underlie these protocols and standards. On the basis of this list a number of technical concepts that appeared frequently was extracted, and used to create a second list of technical terms that, when combined, create an enabling environment for excercising human rights on the Internet.

5.2.1.3. Building a common vocabulary of technical concepts that impact human rights

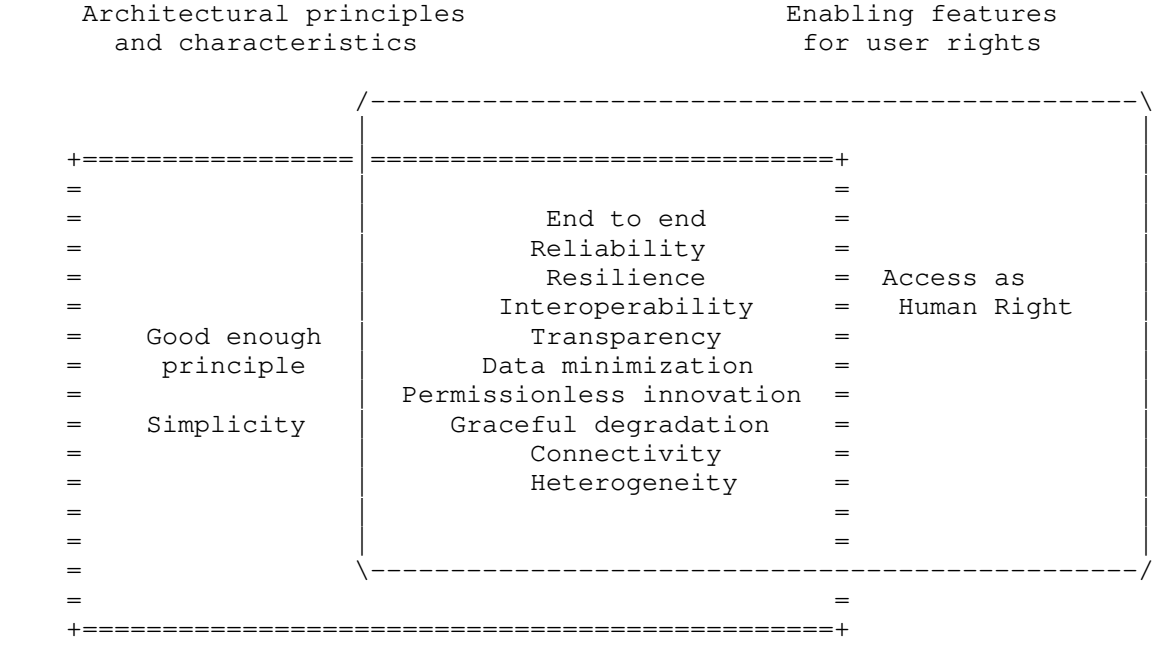
While interviewing experts, mapping RFCs and compiling technical definitions several concepts of convergence and divergence were identified. To ensure that the discussion was based on a common understanding of terms and vocabulary, a list of definitions was created. The definitions are based on the wording found in various IETF documents, and if these were unavailable definitions were taken from definitions from other Standards Developing Organizations or academic literature.

5.2.1.4. Translating Human Rights Concept into Technical Definitions

The previous steps allowed for the clarification of relation between human rights and technical concepts. The steps taken show how the research process zoomed in, from compiling a broad lists of protocols and standards that relate to human rights to extracting the precise technical concepts that make up these protocols and standards, in order to understand the relationship between the two. This sub-section presents the next step: translating human rights to technical concepts by matching the individuals components of the rights to the accompanying technical concepts, allowing for the creation of a list of technical concepts that when combined create an enabling environment for human rights.

5.2.1.5. List technical terms that combined create enabling environment for human rights

On the basis of the prior steps the following list of technical terms, that when combined create an enabling environment for human rights, such a freedom of expression and freedom of association, was drafted.

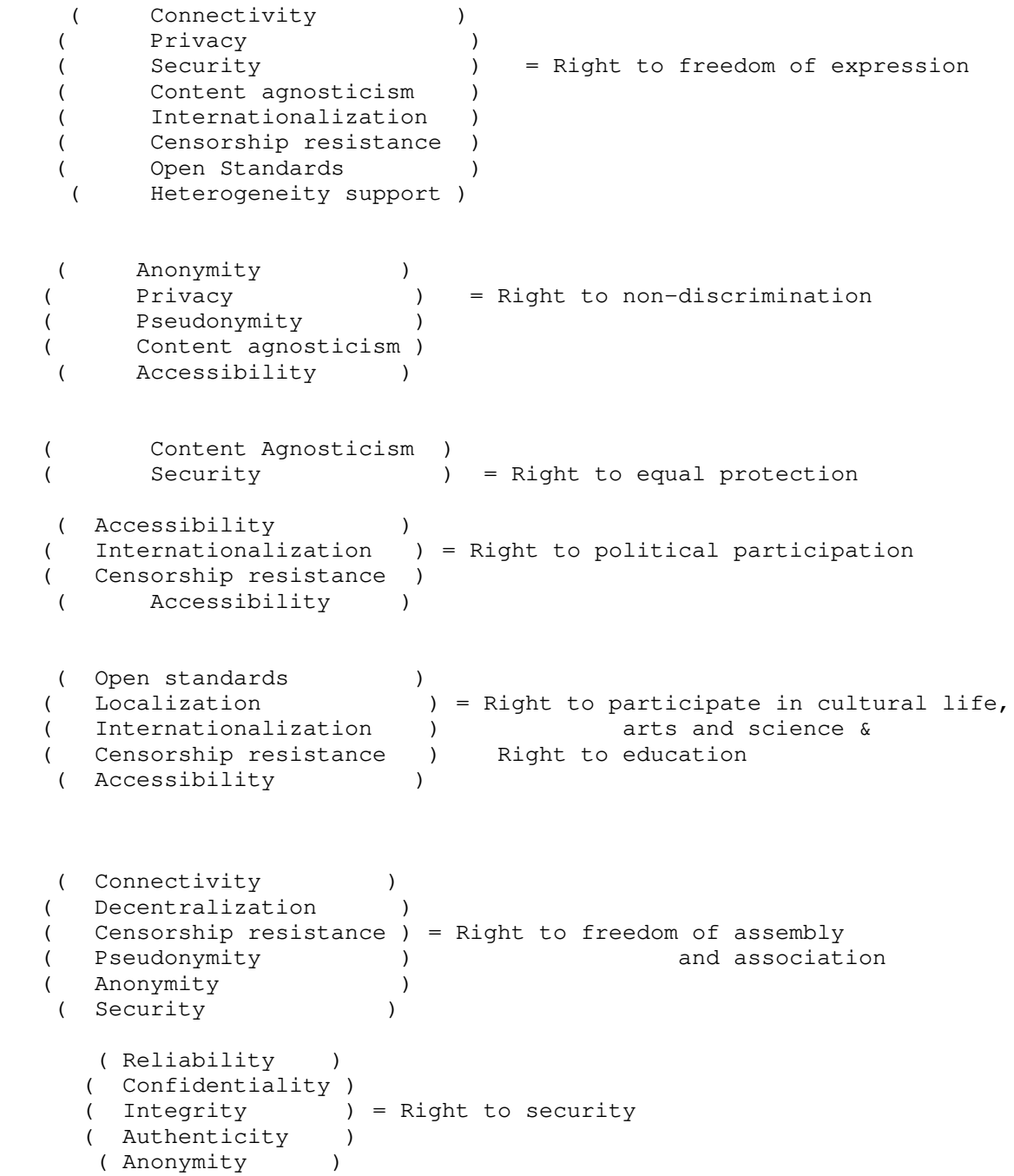


5.2.2. Translation human rights to technical terms

The combination of the technical concepts that have been gathered the steps above have been grouped according to their impact on specific rights as they have been mentioned in the interviews done at IETF92 as well as study of literature (see literature and discussion review above).

This analysis aims to assist protocol developers by understanding better understanding the roles specific technical concepts with regards to the possibility to exercise human rights on the Internet.

This analysis does not claim to be an complete or exhaustive mapping of all possible ways in which a protocols could potentially impact human rights, but it presents an initial combined concept mapping based on interviews and literature and discussion review.


(Connectivity)
(Privacy)
(Security) = Right to freedom of expression
(Content agnosticism)
(Internationalization)
(Censorship resistance)
(Open Standards)
(Heterogeneity support)
(Anonymity)
(Privacy) = Right to non-discrimination
(Pseudonymity)
(Content agnosticism)
(Accessibility)
(Content Agnosticism)
(Security) = Right to equal protection
(Accessibility)
(Internationalization) = Right to political participation
(Censorship resistance)
(Accessibility)
(Open standards)
(Localization) = Right to participate in cultural life,
(Internationalization) arts and science &
(Censorship resistance) Right to education
(Accessibility)
(Connectivity)
(Decentralization)
(Censorship resistance) = Right to freedom of assembly
(Pseudonymity) and association
(Anonymity)
(Security)
(Reliability)
(Confidentiality)
(Integrity) = Right to security
(Authenticity)
(Anonymity)

5.2.2.1. Map cases of protocols that adversely impact human rights or are enablers thereof

Given the information above, the following list of cases of protocols that adversely impact or enable human rights was formed.

5.2.3. IPv4

The Internet Protocol version 4 (IPv4), also known as 'layer 3' of the Internet, and specified as a common encapsulation and protocol header, is defined in [RFC0791]. The evolution of Internet communications led to continued development in this area, encapsulated in the development of version 6 (IPv6) of the protocol in [RFC2460]. In spite of this updated protocol, we find that 25 years after the specification of version 6 of the protocol, the older v4 standard continues to account for a sizeable majority of Internet traffic, and most (if not all) of the issues discussed here are valid for IPv4 as well as IPv6.

The Internet was designed as a platform for free and open communication, most notably encoded in the end-to-end principle, and that philosophy is also present in the technical implementation of the Internet Protocol. [RFC3724] While the protocol was designed to exist in an environment where intelligence is at the end hosts, it has proven to provide sufficient information that a more intelligent network core can make policy decisions and enforce policy shaping and restricting the communications of end hosts. These capabilities for network control and limitations of the freedom of expression by end hosts can be traced back to the IPv4 design, helping us understand which technical protocol decisions have led to harm of this human rights. A feature that can harm freedom of expression as well as the right to privacy through misuse of the Internet Protocol is the exploitation of the public visibility of the host pairs for all communications, and the corresponding ability to discriminate and block traffic as a result of that metadata.

5.2.3.1. Network visibility of Source and Destination

The IPv4 protocol header contains fixed location fields for both the source and destination IP addresses [RFC0791]. These addresses identify both the host sending and receiving each message, and allow the core network to understand who is talking to whom, and to practically limit communication selectively between pairs of hosts. Blocking of communication based on the pair of source and destination is one of the most common limitations on the ability for hosts to communicate today, [caida] and can be seen as a restriction of the ability for those hosts to assemble or to consensually express themselves.

Inclusion of an Internet-wide identified source in the IP header is not the only possible design, especially since the protocol is most commonly implemented over Ethernet networks exposing only link-local identifiers. [RFC0894] A variety of alternative designs including source routing, which would allow for the sender to choose a per defined (safe) route, and spoofing of the source IP address are technically supported by the protocol, but neither are considered good practice on the Internet. While projects like [torproject] provide an alternative implementation of anonymity in connections, they have been developed in spite of the IPv4 protocol design.

5.2.3.2. Protocols

The other major feature of the IP protocol header is that it specifies the protocol encapsulated in each message in an easily observable form, and does not encourage a design where the encapsulated protocol is not available to a network observer. This design has resulted in a proliferation of routers which inspect the inner protocol, and also led to a stagnation where only the TCP and UDP protocols are widely supported across the Internet. While the IP protocol was designed as the entire set of metadata needed for routing, subsequent enhanced routers have found value on making policy decisions based on the contents of TCP and UDP headers as well, and are encoded with the assumption that only these protocols will be used for data transfer. [spdy] [RFC4303] defines an encrypted encapsulation of additional protocols, but lacks widespread deployment and faces the same challenge as any other protocol of providing sufficient metadata with each message for routers to make positive policy decisions. Protocols like [RFC4906] have seen limited wide-area uptake, and these alternate designs are frequently re-implemented on top of UDP. [quic]

5.2.3.3. Address Translation and Mobility

A major structural shift in the Internet which undermined the protocol design of IPv4, and significantly reduced the freedom of end users to communicate and assemble is the introduction of network address translation. [RFC1631] Network address translation is a process whereby organizations and autonomous systems connect two networks by translating the IPv4 source and destination addresses between the two. This process puts the router performing the translation into a privileged position, where it can decide which subset of communications are worthy of translation, and whether an unknown request for communication will be correctly forwarded to a host on the other network.

This process of translation has widespread adoption despite promoting a process that goes against the stated end-to-end process of the

underlying protocol [natusage]. In contrast, the proposed mechanism to provide support for mobility and forwarding to clients which may move, encoded instead as an option in the IP protocol in [RFC5944], has failed to gain traction. In this situation the compromise made in the design of the protocol resulted in a technology that is not coherent with the end-to-end principles and thus creates and extra possible hurdle for freedom of expression in its design, even though a viable alternative that would do this exists. There is a particular problem surrounding NATs and VPN (as well as other connections used for privacy purposes) as they sometimes cause these not to work.

5.2.4. DNS

The Domain Name System (DNS) [RFC1035], provides service discovery capabilities, and provides a mechanism to associate human readable names with services. The DNS system is organized around a set of independently operated 'Root Servers' run by organizations around the web which enact ICANN's policy by answering queries for which organizations have been delegated to manage registration under each Top Level Domain (TLD). The DNS is centralized, and this brings up political and social concerns over control. Top Level domains are maintained and determined by ICANN. These namespaces encompass several classes of services. The initial name spaces including '.Com' and '.Net', provide common spaces for expression of ideas, though their policies are enacted through US based companies. Other name spaces are delegated to specific nationalities, and may impose limits designed to focus speech in those forums both to promote speech from that nationality, and to comply with local limits on expression and social norms. Finally, the system has recently been expanded with additional generic and sponsored name spaces, for instance '.travel' and '.ninja', which are operated by a range of organizations which may independently determine their registration policies. This new development has both positive and negative implications in terms of enabling human rights. Some individuals argue that it undermines the right to freedom of expression because some of these new gtlds have restricted policies on registration and particular rules on hate speech content. Others argue that precisely these properties are positive because they enable certain (mostly minority) communities to build safer spaces for association, thereby enabling their right to freedom of association. An often mentioned example is an application like .gay.

DNS has significant privacy issues per [RFC7626]. Most notable the lack of encryption to limit the visibility of requests for domain resolution from intermediary parties, and a limited deployment of DNSSEC to provide authentication, allowing the client to know that they received a correct, "authoritative", answer to a query. In

response to the privacy issues, the IETF DNS PRIVate Exchange (DPRIVE) Working Group is developing mechanisms to provide confidentiality to DNS transactions, to address concerns surrounding pervasive monitoring [RFC7258].

Authentication through DNSSEC creates a validation path for records. This authentication protects against forged or manipulated DNS data. As such DNSSEC protects the directory look-up and makes hijacking of a session harder. This is important because currently interference with the operation of the DNS is becoming one of the central mechanisms used to block access to websites. This interference limits both the freedom of expression of the publisher to offer their content, and the freedom of assembly for clients to congregate in a shared virtual space. Even though DNSSEC doesn't prevent censorship, it makes it clear that the returned information is not the information that was requested, which contributes to the right to security and increases trust in the network. It is however important to note that DNSSEC is currently not widely supported or deployed by domain name registrars, making it difficult to authenticate and use correctly.

5.2.4.1. Removal of records

There have been a number of cases where the records for a domain are removed from the name system due to real-world events. Examples of this removal includes the 'seizure' of wikileaks [bbc-wikileaks] and the names of illegally operating gambling operations by the United States ICE unit, which compelled the US-based registry in charge of the .com TLD to hand ownership of those domains over to the US government. The same technique has been used in Libya to remove sites in violation of "our Country's Law and Morality (which) do not allow any kind of pornography or its promotion." [techyum]

At a protocol level, there is no technical auditing for name ownership, as in alternate systems like [namecoin]. As a result, there is no ability for users to differentiate seizure from the legitimate transfer of name ownership, which is purely a policy decision of registrars. While DNSSEC addresses network distortion events described below, it does not tackle this problem.

5.2.4.2. Distortion of records

The most common mechanism by which the DNS system is abused to limit freedom of expression is through manipulation of protocol messages by the network. One form occurs at an organizational level, where client computers are instructed to use a local DNS resolver controlled by the organization. The DNS resolver will then selectively distort responses rather than request the authoritative

lookup from the upstream system. The second form occurs through the use of deep packet inspection, where all DNS protocol messages are inspected by the network, and objectionable content is distorted, as in [turkey].

A notable instance of distortion occurred in Greece [ververis], where a study found evidence of both of deep packet inspection to distort DNS replies, and overblocking of content. ISPs prevented clients from resolving the names of domains which they were instructed to do through a governmental order, prompting this particular blocking systems there.

At a protocol level, the effectiveness of these attacks is made possible by a lack of authentication in the DNS protocol. DNSSEC provides the ability to determine authenticity of responses when used, but it is not regularly checked by resolvers. DNSSEC is not effective when the local resolver for a network is complicit in the distortion, for instance when the resolver assigned for use by an ISP is the source of injection. Selective distortion of records is also been made possible by the predictable structure of DNS messages, which make it computationally easy for a network device to watch all passing messages even at high speeds, and the lack of encryption, which allows the network to distort only an objectionable subset of protocol messages. Specific distortion mechanisms are discussed further in [hall].

5.2.4.3. Injection of records

Responding incorrectly to requests for name lookups is the most common mechanism that in-network devices use to limit the ability of end users to discover services. A deviation, which accomplishes a similar objective may be seen as different from a freedom of expression perspective, is the injection of incorrect responses to queries. The most prominent example of this behavior occurs in China, where requests for lookups of sites deemed inappropriate will trigger the network to respond with a false response, causing the client to ignore the real response when it subsequently arrives. [greatfirewall] Unlike the other forms of discussion mentioned above, injection does not stifle the ability of a server to announce it's name, it instead provides another voice which answers sooner. This is effective because without DNSSEC, the protocol will respond to whichever answer is received first, without listening for subsequent answers.

5.2.5. HTTP

The Hypertext Transfer Protocol (HTTP), described in its version 1.1 in RFC 7230 to 7237, is a request-response application protocol developed throughout the 1990s, and factually contributed to the exponential growth of the Internet and the inter-connection of populations around the world. Because of its simple design, HTTP has become the foundation of most modern Internet platforms and communication systems, from websites, to chat systems, and computer-to-computer applications. In its manifestation with the World Wide Web, HTTP radically revolutionized the course of technological development and the ways people interact with online content and with each other.

However, HTTP is also a fundamentally insecure protocol, that doesn't natively provide encryption properties. While the definition of the Secure Sockets Layer (SSL), and later of Transport Layer Security (TLS), also happened during the 1990s, the fact that HTTP doesn't mandate the use of such encryption layers to developers and service providers, caused a very late adoption of encryption. Only in the middle of the 2000s did we observed big Internet service providers, such as Google, starting to provide encrypted access to their web services.

The lack of sensitivity and understanding of the critical importance of securing web traffic incentivized malicious and offensive actors to develop, deploy and utilize at large interception systems and later active injection attacks, in order to swipe large amounts of data, compromise Internet-enabled devices. The commercial availability of systems and tools to perform these types of attacks also led to a number of human rights abuses that have been discovered and reported over the years.

Generally we can identify in Traffic Interception and Traffic Manipulation the two most problematic attacks that can be performed against applications employing a clear-text HTTP transport layer. That being said, the IETF and especially the General Area Review Team (Gen-ART), is taking steady steps to move to the encrypted version of HTTP, HTTPSecure (HTTPS).

5.2.5.1. Traffic Interception

While we are seeing an increasing trend in the last couple of years to employ SSL/TLS as a secure traffic layer for HTTP-based applications, we are still far from seeing an ubiquitous use of encryption on the World Wide Web. It is important to consider that the adoption of SSL/TLS is also a relatively recent phenomena. E-mail providers such as riseup.net provided SSL on by default as on

of the first. Google introduced an option for its GMail users to navigate with SSL only in 2008 [Rideout], and turned SSL on by default later in 2010 [Schillace]. It took an increasing amount of security breaches and revelations on global surveillance from Edward Snowden to have other Internet service providers to follow Google's lead. For example, Yahoo enabled SSL/TLS by default on its webmail services only towards the end of 2013 [Peterson].

TLS itself has been subject to many attacks and bugs which can be attributed to some fundamental design weaknesses such as lack of a state machine, which opens a vulnerability for a Triple Handshake Attack, and flaws caused by early U.S. government restrictions on cryptography, leading to cipher-suite downgrade attacks (Logjam attack). These vulnerabilities have been corrected in TLS1.3. [Bhargavan] [Adrian]

HTTP upgrading to HTTPS is also vulnerable to having an attacker remove the "S" in any links to HTTPS URIs from a web-page transferred in cleartext over HTTP, an attack called "SSL Stripping" [sslstrip]. Thus, for high security use of HTTPS IETF standards such as HSTS [RFC6797] and certificate pinning should be used [RFC7469].

As we learned through the Snowden's revelations, intelligence agencies have been intercepting and collecting unencrypted traffic at large for many years. There are documented examples of such mass surveillance programs with GCHQ's TEMPORA and NSA's XKEYSCORE. Through these programs NSA/GCHQ have been able to swipe large amounts of data including email and instant messaging communications which have been transported by the respective providers in clear for years, unsuspecting of the pervasiveness and scale of governments' efforts and investment into global mass surveillance capabilities.

However, similar mass interception of unencrypted HTTP communications is also often employed at a nation-level by less democratic countries by exercising control over state-owned Internet Service Providers (ISP) and through the use of commercially available monitoring, collection, and censorship equipment. Over the last few years a lot of information has come to public attention on the role and scale of a surveillance industry dedicated to develop interception gear of different types, making use of known and unknown weaknesses in existing protocols [RFC7258]. We have several records of such equipment being sold and utilized by oppressive regimes in order to monitor entire segments of population especially at times of social and political distress, uncovering massive human rights abuses. For example, in 2013 the group Telecomix revealed that the Syrian regime was making use of BlueCoat products in order to intercept clear-text traffic as well as to enforce censorship of unwanted content [RSF]. Similarly in 2012 it was found that the French Amesys provided the

Gaddafi's government with equipment able to intercept emails, Facebook traffic, and chat messages ad a country level. The use of such systems, especially in the context of the Arab Spring and of civil uprisings against the dictatorships, has caused serious concerns of significant human rights abuses in Libya.

5.2.5.2. Traffic Manipulation

The lack of a secure transport layer under HTTP connections not only exposes the users to interception of the content of their communications, but is more and more commonly abused as a vehicle for active compromises of computers and mobile devices. If an HTTP session travels in clear over the network, any node positioned at any point in the network is able to perform man-in-the-middle attacks and observe, manipulate, and hijack the session and modify the content of the communication in order to trigger unexpected behavior by the application generating the traffic. For example, in the case of a browser the attacker would be able to inject malicious code in order to exploit vulnerabilities in the browser or any of its plugins. Similarly, the attacker would be able to intercept, trojanize, and repackage binary software updates that are very commonly downloaded in clear by applications such as word processors and media players. If the HTTP session would be encrypted, the tampering of the content would not be possible, and these network injection attacks would not be successful.

While traffic manipulation attacks have been long known, documented, and prototyped especially in the context of WiFi and LAN networks, in the last few years we observed an increasing investment into the production and sale of network injection equipment both available commercially as well as deployed at scale by intelligence agencies.

For example we learned from some of the documents provided by Edward Snowden to the press, that the NSA has constructed a global network injection infrastructure, called QUANTUM, able to leverage mass surveillance in order to identify targets of interests and subsequently task man-on-the-side attacks to ultimately compromise a selected device. Among other attacks, NSA makes use of an attack called QUANTUMINSERT [Haagsma] which intercepts and hijacks an unencrypted HTTP communication and forces the requesting browser to redirect to a host controlled by NSA instead of the intended website. Normally, the new destination would be an exploitation service, referred in Snowden documents as FOXACID, which would attempt at executing malicious code in the context of the target's browser. The Guardian reported in 2013 that NSA has for example been using these techniques to target users of the popular anonymity service Tor [Schneier]. The German NDR reported in 2014 that NSA has also been

using its mass surveillance capabilities to identify Tor users at large [Appelbaum].

Recently similar capabilities of Chinese authorities have been reported as well in what has been informally called the "Great Cannon" [Marcak], which raised numerous concerns on the potential curb on human rights and freedom of speech due to the increasing tighter control of Chinese Internet communications and access to information.

Network injection attacks are also made widely available to state actors around the world through the commercialization of similar, smaller scale equipment that can be easily acquired and deployed at a country-wide level. Companies like FinFisher and HackingTeam are known to have network injection gear within their products portfolio, respectively called FinFly ISP and RCS Network Injector [Marquis-Boire]. The technology devised and produced by HackingTeam to perform network traffic manipulation attacks on HTTP communications is even the subject of a patent application in the United States [Googlepatent]. Access to offensive technologies available on the commercial lawful interception market has been largely documented to have lead to human rights abuses and illegitimate surveillance of journalists, human rights defenders, and political activists in many countries around the world. Companies like FinFisher and HackingTeam have been found selling their products to oppressive regimes with little concern for bad human rights records [Collins]. While network injection attacks haven't been the subject of much attention, they do enable even unskilled attackers to perform silent and very resilient compromises, and unencrypted HTTP remains one of the main vehicles.

There is a new version of HTTP, called HTTP/2, which was published as [RFC7540] and which aimed to be largely backwards compatible but also offer new option such as data compression of HTTP headers and pipelining of request and multiplexing multiple requests over a single TCP connection. Except for decreasing latency to improve page loading speeds it also facilitates more efficient use of connectivity in low-bandwith environments, which is an enabler for freedom of expression, the right to assembly, right to political participation and the right to participate in cultural life, art and science. [RFC7540] does not mandate Transport Layer Security or any other form of encryption, is also does not support opportunistic encryption, so the vulnerabilities listed above for HTTP/1 are also valid for HTTP/2 as defined in [RFC7540].

5.2.6. XMPP

The Extensible Messaging and Presence Protocol (XMPP), specified in [RFC6120], provides a standard for interactive chat messaging, and has evolved to encompass interoperable text, voice, and video chat. The protocol is structured as a federated network of servers, similar to email, where users register with a local server which acts one their behalf to cache and relay messages. This protocol design has many advantages, allowing servers to shield clients from denial of service and other forms of retribution for their expression, and designed to avoid central entities which could control the ability to communicate or assemble using the protocol.

None-the-less, there are plenty of aspects of the protocol design of XMPP which shape the ability for users to communicate freely, and to assembly through the protocol. The protocol also has facets that may stifle speech as users self-censor for fear of surveillance, or find themselves unable to express themselves freely.

5.2.6.1. User Identification

The XMPP specification dictates that clients are identified with a resource (node@domain/home [1] / node@domain/work [2]) to distinguish the conversations to specific devices. While the protocol does not specify that the resource must be exposed by the client's server to remote users, in practice this has become the default behavior. In doing so, users can be tracked by remote friends and their servers, who are able to monitor presence not just of the user, but of each individual device the user logs in with. This has proven to be misleading to many users, [pidgin] since many clients only expose user level rather than device level presence. Likewise, user invisibility so that communication can occur while users don't notify all buddies and other servers of their availability is not part of the formal protocol, and has only been added as an extension within the XML stream rather than enforced by the protocol.

5.2.6.2. Surveillance of Communication

The XMPP protocol specifies the standard by which communication of channels may be encrypted, but it does not provide visibility to clients of whether their communications are encrypted on each link. In particular, even when both clients ensure that they have an encrypted connection to their XMPP server to ensure that their local network is unable to read or disrupt the messages they send, the protocol does not provide visibility into the encryption status between the two servers. As such, clients may be subject to selective disruption of communications by an intermediate network which disrupts communications based on keywords found through Deep

Packet Inspection. While many operators have commited to only establishing encrypted links from their servers in recognition of this vulnerability, it remains impossible for users to audit this behavior and encrypted connections are not required by the protocol itself [xmppmanifesto].

In particular, section 13.14 of the protocol specification [RFC6120] explicitly acknowledges the existence of a downgrade attack where an adversary controlling an intermediate network can force the inter domain federation between servers to revert to a non-encrypted protocol were selective messages can then be disrupted.

5.2.6.3. Group Chat Limitations

Group chat in the XMPP protocol is defined as an extension within the XML specification of the XMPP protocol (https://xmpp.org/extensions/xep-0045.html). However, it is not encoded or required at a protocol level, and not uniformly implemented by clients.

The design of multi-user chat in the XMPP protocol suffers from extending a protocol that was not designed with assembly of many users in mind. In particular, in the federated protocol provided by XMPP, multi-user communities are implemented with a distinguished 'owner', who is granted control over the participants and structure of the conversation.

Multi-user chat rooms are identified by a name specified on a specific server, so that while the overall protocol may be federated, the ability for users to assemble in a given community is moderated by a single server. That server may block the room and prevent assembly unilaterally, even between two users neither of whom trust or use that server directly.

5.2.7. Peer to Peer

Peer-to-Peer (P2P) is a network architecture in which all the participant nodes can be responsible for the storage and dissemination of information from any other node (defined in [RFC7574], an IETF standard that used a P2P architecture). A P2P network is a logical overlay that lives on top of the physical network, and allows nodes (or "peers") participating to it to establish contact and exchange information directly from one to each other. The implementation of a P2P network may very widely: it may be structured or unstructured, and it may implement stronger or weaker cryptographic and anonymity properties. While its most common application has traditionally been file-sharing (and other types of content delivery systems), P2P is increasingly becoming a popular architecture for networks and applications that require (or

encourage) decentralization. A prime example is Bitcoin (and similar cryptocurrencies), as well as Skype, Spotify and other proprietary multimedia applications.

In a time of heavily centralized online services, peer-to-peer is often seen as an alternative, more democratic, and resistant architecture that displaces structures of control over data and communications and delegates all peers equally to be responsible for the functioning, integrity, and security of the data. While in principle peer-to-peer remains critical to the design and development of future content distribution, messaging, and publishing systems, it poses numerous security and privacy challenges which are mostly delegated to individual developers to recognize, analyze, and solve in each implementation of a given P2P network.

5.2.7.1. Network Poisoning

Since content, and in some occasions peer lists, are safeguarded and distributed by its members, P2P networks are prone to what are generally defined as "poisoning attacks". Poisoning attacks might be directed directly at the data that is being distributed, for example by intentionally corrupting it, or at the index tables used to instruct the peers where to fetch the data, or at routing tables, with the attempt of providing connecting peers with lists of rogue or non-existing peers, with the intention to effectively cause a Denial of Service on the network.

5.2.7.2. Throttling

Peer-to-Peer traffic (and BitTorrent in particular) represents a high percentage of global Internet traffic and it has become increasingly popular for Internet Service Providers to perform throttling of customers lines in order to limit bandwidth usage [torrentfreak1] and sometimes probably as an effect of the ongoing conflict between copyright holders and file-sharing communities [wikileaks]. Such throtteling undermines the end-to-end principle.

Throttling the peer-to-peer traffic makes some uses of P2P networks ineffective and it might be coupled with stricter inspection of users' Internet traffic through Deep Packet Inspection techniques which might pose additional security and privacy risks.

5.2.7.3. Tracking and Identification

One of the fundamental and most problematic issues with traditional peer-to-peer networks is a complete lack of anonymization of its users. For example, in the case of BitTorrent, all peers' IP addresses are openly available to the other peers. This has lead to

an ever-increasing tracking of peer-to-peer and file-sharing users [ars]. As the geographical location of the user is directly exposed, and so could be his identity, the user might become target of additional harassment and attacks, being of physical or legal nature. For example, it is known that in Germany law firms have made extensive use of peer-to-peer and file-sharing tracking systems in order to identify downloaders and initiate legal actions looking for compensations [torrentfreak2].

It is worth noting that there are varieties of P2P networks that implement cryptographic practices and that introduce anonymization of its users. Such implementations may be proved to be successful in resisting censorship of content, and tracking of the network peers. A primary example is FreeNet [freenet1], a free software application designed to significantly increase the difficulty of users and content identification, and dedicated to foster freedom of speech online [freenet2].

5.2.7.4. Sybil Attacks

In open-membership P2P networks, a single attacker can pretend to be many participants, typically by creating multiple fake identities of whatever kind the P2P network uses [Douceur]. Attackers can use Sybil attacks to bias choices the P2P network makes collectively toward the attacker's advantage, e.g., by making it more likely that a particular data item (or some threshold of the replicas or shares of a data item) are assigned to attacker-controlled participants. If the P2P network implements any voting, moderation, or peer review-like functionality, Sybil attacks may be used to "stuff the ballots" toward the attacker's benefit. Companies and governments can use Sybil attacks on discussion-oriented P2P systems for "astroturfing" or creating the appearance of mass grassroots support for some position where there is none in reality. It is important to know that there are no known solutions to Sybil attacks, and routing via 'friends' allows users to be de-anonymized via their social graph.

5.2.7.5. Conclusions

Encrypted P2P and Anonymous P2P networks already emerged and provided viable platforms for sharing material [tribler], publish content anonymously, and communicate securely [bitmessage].These platforms are not perfect, and more research needs to be done. If adopted at large, well-designed and resistant P2P networks might represent a critical component of a future secure and distributed Internet, enabling freedom of speech and freedom of information at scale.

5.2.8. Virtual Private Network

5.2.8.1. Introduction

A Virtual Private Network (VPN) is a point-to-point connection that enables two computers to communicate over an encrypted tunnel. There are multiple implementations and protocols used in provisioning a VPN, and they generally diversify by encryption protocol or particular requirements, most commonly in proprietary and enterprise solutions. VPNs are used commonly either to enable some devices to communicate through peculiar network configurations, or in order to use some privacy and security properties in order to protect the traffic generated by the end user; or both. VPNs have also become a very popular technology among human rights defenders, dissidents, and journalists worldwide to avoid local illegitimate wiretapping and eventually also to circumvent censorship. Among human rights defenders VPNs are often debated as a potential alternative to Tor or other anonymous networks. Such comparison is misleading, as some of the privacy and security properties of VPNs are often misunderstood by less tech-savvy users, which could ultimately lead to unintended problems.

As VPNs increased in popularity, commercial VPN providers have started growing in business and are very commonly picked by human rights defenders and people at risk, as they are normally provided with an easy-to-use service and sometimes even custom applications to establish the VPN tunnel. Not being able to control the configuration of the network, and even less so the security of the application, assessing the general privacy and security state of common VPNs is very hard. Often such services have been discovered leaking information, and their custom applications have been found flawed. While Tor and similar networks receive a lot of scrutiny from the public and the academic community, commercial or non-commercial VPN networks are way less analyzed and understood, and it might be valuable to establish some standards to guarantee a minimal level of privacy and security to those who need them the most.

5.2.8.2. No anonymity against VPN provider

One of the common misconception among users of VPNs is the level of anonymity VPN can provide. This sense of anonymity can be betrayed by a number of attacks or misconfigurations of the VPN provider. It is important to remember that, contrarily to Tor and similar systems, VPN was not designed to provide anonymity properties. From a technical point of view, the VPN might leak identifiable information, or might be subject of correlation attacks that could expose the originating address of the connecting user. Most importantly, it is vital to understand that commercial and non-commercial VPN providers

are bound by the law of the jurisdiction they reside in or in which their infrastructure is located, and they might be legally forced to turn over data of specific users if legal investigations or intelligence requirements dictate so. In such cases, if the VPN providers retain logs, it is possible that the information of the user is provided to the user's adversary and leads to his or her identification.

5.2.8.3. Logging

With VPN being point-to-point connections, the service providers are in fact able to observe the original location of the connecting users and they are able to track at what time they started their session and eventually also to which destinations they're trying to connect to. If the VPN providers retain logs for long enough, they might be forced to turn over the relevant data or they might be otherwise compromised, leading to the same data getting exposed. A clear log retaining policy could be enforced, but considering that countries enforce very different levels of data retention policies, VPN providers should at least be transparent on what information do they store and for how long is being kept.

5.2.8.4. 3rd Party Hosting

VPN providers very commonly rely on 3rd parties to provision the infrastructure that is later going to be used to run VPN endpoints. For example, they might rely on external dedicated server hosting providers, or on uplink providers. In those cases, even if the VPN provider itself isn't retaining any significant logs, the information on the connecting users might be retained by those 3rd parties instead, introducing an additional collection point for the adversary.

5.2.8.5. IPv6 Leakage

Some studies proved that several commercial VPN providers and applications suffer of critical leakage of information through IPv6 due to improper support and configuration [PETS2015VPN]. This is generally caused by a lack of proper configuration of the client's IPv6 routing tables. Considering that most popular browsers and similar applications have been supporting IPv6 by default, if the host is provided with a functional IPv6 configuration, the traffic that is generated might be leaked if the VPN application isn't designed to manipulate such traffic properly.

5.2.8.6. DNS Leakage

Similarly, VPN services that aren't handling DNS requests and are not running DNS servers of their own, might be prone to DNS leaking which might not only expose sensitive information on the activity of the user, but could also potentially lead to DNS hijacking attacks and following compromises.

5.2.8.7. Traffic Correlation

As revelations of mass surveillance have been growing in the press, additional details on attacks on secure Internet communications have come to the public's attention. Among these, VPN appeared to be a very interesting target for attacks and collection efforts. Some implementations of VPN appear to be particularly vulnerable to identification and collection of key exchanges which, some Snowden documents revealed, are systematically collected and stored for future reference. The ability of an adversary to monitor network connections at many different points over the Internet, can allow them to perform traffic correlation attacks and identify the origin of certain VPN traffic by cross referencing the connection time of the user to the endpoint and the connection time of the endpoint to the final destination. These types of attacks, although very expensive and normally only performed by very resourceful adversaries, have been documented [spiegel] to be already in practice and could completely vanify the use of a VPN and ultimately expose the activity and the identity of a user at risk.

5.2.9. HTTP 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 [Cath]. 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 were 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].

The status code is named '451', a reference to Bradbury's famous novel on censorship, and the temperature (in Fahrenheit) at which bookpaper autoignites.

During the IETF92 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'. Again others argued that it would be useful for individuals, or organizations 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 on December 18, 2015 the Internet Engineering Steering Group approved publication of 'An HTTP Status Code to Report Legal Obstacles'. It is now an IETF approved HTTP status code to signal when resource access is denied as a consequence of legal demands [RFC7725].

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.

It is however important to note that 451 is not a solution to detect all occasions of censorship. A large swath of Internet filtering occurs in the network rather than the server itself. For these forms of censorship 451 plays a limited role, as the servers will not be able to send the code, because they haven't received the requests (as is the case with servers with resources blocked by the Chinese Golden shield). Such filtering regimes are unlikely to voluntarily inject a 451 status code. The use of 451 is most likely to apply in the case of cooperative, legal versions of content removal resulting from requests to providers. One can think of content that is removed or blocked for legal reasons, like copyright infringement, gambling laws, child abuse, et cetera. The major use case is thus clearly on the Web server itself, not the network. Large Internet companies and search engines are constantly asked to censor content in various jurisdictions. 451 allows this to be easily discovered, for instance by initiatives like the Lumen Database. In the case of adversarial

blocking done by a filtering entity on the network 451 is less useful.

Overall, the strength of 451 lies in its ability to provide transparency by giving the reason for blocking, and giving the end-user the ability to file a complaint. It allows organizations to easily measure censorship in an automated way, and prompts the user to access the content via another path (e.g. TOR, VPNs) when (s)he encounters the 451 status code.

Status code 451 impact human rights by making censorship more transparent and measurable. The status code increases transparency both by signaling the existence of censorship (instead of a much more broad HTTP error message like HTTP status code 404) as well as providing details of the legal restriction, which legal authority is imposing it, and what class of resources it applies to. This empowers the user to seek redress.

5.2.10. 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]. 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 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 optimization, and hence improve traffic carriage. On the other hand, there are risks of information leakage and other privacy and security concerns.

Middleboxes, and the protocols guiding them, influence individuals' ability to communicate online freely and privately. 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. Middleboxes essentially undermine the end-to-end principle by inserting themselves in the network, and acting as intermediaries. Although there are many advantages, such as increased security and network performance, to having middleboxes they also have downsides. They are known to limit the choice of transport protocols and drop packets that don't conform. As such, limiting both freedom of expression online and undermining the end-to-end principle.

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.

5.2.11. DDOS attacks

Many individuals, not excluding IETF engineers, have argued that DDoS attacks are fundamentally against freedom of speech. Technically DDoS attacks are when one or multiple host overload the bandwidth or resources of another host by flooding it with traffic, causing it to temporarily stop being available to users. One can roughly differentiate three types of DDoS attacks: Volume Based Attacked (This attack aims to make the host unreachable by using up all it's bandwith, often used techniques are: UDP floods and ICMP floods), Protocol Attacks (This attacks aims to use up actual server resources, often used techniques are SYN floods, fragmented packet attacks, and Ping of Death [RFC4949]) and Application Layer Attacks (this attack aims to bring down a server, such as the webserver).

In their 2010 report Zuckerman et al argue that DDoS attacks are a bad thing because they are increasingly used by governments to attack and silence critics. Their research demonstrates that in many countries independent media outlets and human rights organizations are the victim of DDoS attacks, which are directly or indirectly linked to their governments. These types of attacks are particularly complicated because attribution is difficult, creating a situation in which governments can effectively censor content, while being able to deny involvement in the attacks [Zuckerman]. DDoS attacks can thus stifle freedom of expression, complicate the ability of independent media and human rights organizations to exercise their right to (online) freedom of association, while facilitating the ability of governments to censor dissent. When it comes to comparing DDoS attacks to protests in offline life, it is important to remember that only a limited number of DDoS attacks involved solely willing participants. In most cases, the clients are hacked computers of unrelated parties that have not consented to being part of a DDoS (for exceptions see Operation Abibil [Abibil] or the Iranian Green Movement DDoS [GreenMovement]).

In addition, DDoS attacks are increasingly used as an extortion tactic, with criminals flooding a website - rendering it inaccessible - until the owner pays them a certain amount of money to stop the attack. The costs of mitigating such attacks, either by improving security to prevent them or paying off the attackers, ends up being paid by the consumer.

All of these issues seem to suggest that the IETF should try to ensure that their protocols cannot be used for DDoS attacks. Decreasing the number of vulnerabilities in the network stacks of routers or computers, reducing flaws in HTTPS implementations, and depreciating non-secure HTTP protocols could address this issue. The IETF can clearly play a role in bringing about some of these changes, and has indicated in [RFC7258] its commitment to mitigating 'pervasive monitoring (...) in the design of IETF protocols, where possible.' This means the use of encryption should become standard. Effectively, for the web this means standardized use of HTTPS. The IETF could redirect its work such that HTPPS becomes part-and-parcel of its standards. However, next to the various technical trade-offs that this might lead to it is important to consider that DDoS attacks are sometimes seen as a method for exercising freedom of speech [Sauter].

There is a need for the IETF to be consistent in the face of attacks (an attack is an attack is an attack) to maintain the viability of the network. Arguing that some DDoS attacks should be allowed, based on the motivation of the attackers complicates the work of the IETF. Because it approaches PM regardless of the motivation of the attackers (see [RFC7258]) for reasoning), taking the motivation of the attackers into account for DDoS would indirectly undermine the ability of the IETF to protect the right to privacy because it introduces an element of inconsistency into how the IETF deals with attacks.

David Clark recently published a paper warning that the future of the Internet is in danger. He argues that the private sector control over the Internet is too strong, limiting the myriad of ways in which it can be used [Daedalus], including for freedom of speech. But just because freedom of speech, dissent, and protest are human rights, and DDoS is a potential expression of those rights, doesn't mean that DDoS in and of itself is a right. To widen the analogy, just because the Internet is a medium through which the right to freedom of expression can be exercised does not make access to the Internet or specific ICTs or NCTs a human right. Uses of DDoS might or might not be legitimate for political reasons, but the IETF has no means or methods to assess this, and in general enabling DDoS would mean a deterioration of the network and thus freedom of expression.

In summation, the IETF cannot be expected to take a moral stance on DDoS attacks, or create protocols to enable some attacks and inhibit others. But what it can do is critically reflect on its role in creating a commercialized Internet without a defacto public space or inherent protections for freedom of speech.

5.3. Model for developing human rights protocol considerations

Having established how human rights relate to standards and protocols, a common vocabulary of technical concepts that impact human rights and how these technical concept can be combined to ensure that the Internet remains an enabling environment for human rights means the contours of a model for developing human rights protocol considerations has taken shape. This subsection provides the last step by detailing how the technical concepts identified above relate to human rights, and what questions engineers should ask themselves when developing or improving protocols. In short, it presents a set of human rights protocol considerations.

5.3.1. Human rights threats

Human rights threats on the Internet come in a myriad of forms. Protocols and standards can harm or enable the right to freedom of expression, right to non-discrimination, right to equal protection, right to participate in cultural life, arts and science, right to freedom of assembly and association, and the right to security. An end-user who is denied access to certain services, data or websites may be unable to disclose vital information about the malpractices of a government or other authority. A person whose communications are monitored may be prevented from exercising their right to freedom of association or participate in political processes [Penney]. In a worst-case scenario, protocols that leak information can lead to physical danger. A realistic example to consider is when opposition group members (or those identified as such) in totalitarian regimes are subjected to torture on the basis of information gathered by the regime through information leakage in protocols.

This sections details several 'common' threats to human rights, indicating how each of these can lead to human rights violations/ harms and present several examples of how these threats to human rights materialize on the Internet. This threat modeling is inspired by [RFC6973] Privacy Considerations for Internet Protocols, which is based on the security threat analysis. This method is by no means a perfect solution for assessing human rights risks in Internet protocols and systems; it is however the best approach currently available. Certain specific human rights threats are indirectly considered in Internet protocols as part of the security considerations [RFC3552], but privacy guidelines [RFC6973] or

reviews, let alone human rights impact assessments of protocols are not standardized or implemented.

Many threats, enablers and risks are linked to different rights. This is not unsurprising if one takes into account that human rights are interrelated, interdependent and indivisible. Here however we're not discussing all human rights because not all human rights are relevant to ICTs in general and protocols and standards in particular [Bless]. This is by no means an attempt to cherry picks rights, if other rights seem relevant, please contact the authors and/or the hrpc mailinglist.

5.3.2. Guidelines for human rights considerations

This section provides guidance for document authors in the form of a questionnaire about protocols being designed. The questionnaire may be useful at any point in the design process, particularly after document authors have developed a high-level protocol model as described in [RFC4101].

There should be some discussion of potential human rights risks arising from potential misapplications of the protocol or technology described in the RFC. This might be coupled with an Applicability Statement for that RFC.

Note that the guidance provided in this section does not recommend specific practices. The range of protocols developed in the IETF is too broad to make recommendations about particular uses of data or how human rights might be balanced against other design goals. However, by carefully considering the answers to the following questions, document authors should be able to produce a comprehensive analysis that can serve as the basis for discussion on whether the protocol adequately protects against specific human rights threats. This guidance is meant to help the thought process of a human rights analysis; it does not provide specific directions for how to write a human rights protocol considerations section (following the example set in [RFC6973]).

5.3.2.1. Technical concepts as they relate to human rights

5.3.2.1.1. Connectivity

Question(s): Does your protocol add application-specific functions to intermediary nodes? Could this functionality also be added to end nodes instead of intermediary nodes?

Explanation: The end-to-end principle [Saltzer] which aims to extend characteristics of a protocol or system as far as possible within the

system, or in other words 'the intelligence is end to end rather than hidden in the network' [RFC1958]. Middleboxes (which can be Content Delivery Networks, Firewalls, NATs or other intermediary nodes that provide other 'services' than routing), and the protocols guiding them, influence individuals' ability to communicate online freely and privately. The potential for abuse and intentional and unintentional censoring and limiting permissionless innovation, and thus ultimately the impact of middleboxes on the Internet as a place of unfiltered, unmonitored freedom of speech, is real.

Example: End-to-end instant message encryption would conceal communications from one user's instant messaging application through any intermediate devices and servers all the way to the recipient's instant messaging application. If the message was decrypted at any intermediate point-for example at a service provider-then the property of end-to-end encryption would not be present.

Impacts:

- Right to freedom of expression

- Right to freedom of assembly and association

5.3.2.1.2. Privacy

Question(s): Did you have a look at the Guidelines in the Privacy Considerations for Internet Protocols [RFC6973] section 7? Could your protocol in any way impact the confidentiality of protocol metadata? Could your protocol counter traffic analysis, or data minimization?

Explanation: Privacy refers to the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. [RFC4949].

Example: See [RFC6973]

Impacts:

- Right to freedom of expression

- Right to non-discrimination

5.3.2.1.3. Content agnosticism

Question(s): If your protocol impacts packet handling, does it look at the packet content? Is it making decisions based on the content of the packet? Is the protocol transparent about its decisions? Does your protocol prioritize certain content or services over others?

Explanation: Content agnosticism refers to the notion that network traffic is treated identically regardless of content.

Example: Content agnosticism prevents content-based discrimination against packets. This is important because changes to this principle can lead to a two-tiered Internet, where certain packets are prioritized over others on the basis of their content. Effectively this would mean that although all users are entitled to receive their packets at a certain speed, some users become more equal than others.

Impacts:

- Right to freedom of expression

- Right to non-discrimination

- Right to equal protection

5.3.2.1.4. Security

Question(s): Did you have a look at Guidelines for Writing RFC Text on Security Considerations [RFC3552]? Have you found any attacks that are out of scope for your protocol? Would these attacks be pertinent to the human rights enabling features of the Internet (as descibred throughout this document)?

Explanation: Most people speak of security as if it were a single monolithic property of a protocol or system, however, upon reflection; one realizes that it is clearly not true. Rather, security is a series of related but somewhat independent properties. Not all of these properties are required for every application. We can loosely divide security goals into those related to protecting communications (COMMUNICATION SECURITY, also known as COMSEC) and those relating to protecting systems (ADMINISTRATIVE SECURITY or SYSTEM SECURITY). Since communications are carried out by systems and access to systems is through communications channels, these goals obviously interlock, but they can also be independently provided [RFC3552]. Security needs to be also be approached in terms of advesaries, and passive global adversaries whose attack is pervasive

surveillance now need to be taken into consideration when designing new protocols.

Example: See [RFC3552].

Impacts:

- Right to freedom of expression

- Right to freedom of assembly and association

- Right to non discrimination

5.3.2.1.5. Internationalization

Question(s): Does your protocol have text strings that are readable or entered by humans? Does your protocol allow Unicode encoded in UTF-8 only, thereby shifting conversion issues away from individual choices? Did you have a look at [RFC6365]?

Explanation: Internationalization refers to the practice of making protocols, standards, and implementations usable in different languages and scripts. (see Localization). In the IETF, internationalization means to add or improve the handling of non-ASCII text in a protocol. [RFC6365] A different perspective, more appropriate to protocols that are designed for global use from the beginning, is the definition used by W3C:

> "Internationalization is the design and development of a product, application or document content that enables easy localization for target audiences that vary in culture, region, or language." {{W3Ci18nDef}}

Many protocols that handle text only handle one charset (US-ASCII), or leave the question of what CCS and encoding are used up to local guesswork (which leads, of course, to interoperability problems). If multiple charsets are permitted, they must be explicitly identified [RFC2277]. Adding non-ASCII text to a protocol allows the protocol to handle more scripts, hopefully representing users across the world. In today's world, that is normally best accomplished by allowing Unicode encoded in UTF-8 only, thereby shifting conversion issues away from individual choices.

Example: See localization Impacts:

- Right to freedom of expression

- Right to political participation

- Right to participate in cultural life, arts and science

- Right to political participation

5.3.2.1.6. Censorship resistance

Question(s): Does this protocol introduce new identifiers that might be associated with persons or content? Does your protocol make it apparent or transparent when filtering happens? Can your protocol contribute to filtering in a way it could be implemented to censor data or services? Could this be designed to ensure this doesn't happen?

Explanation: Censorship resistance refers to the methods and measures to prevent Internet censorship.

Example: Identifiers of content exposed within a protocol might be used to facilitate censorship, as in the case of IP based censorship, which affects protocols like HTTP. Filtering can be made apparent by the use of status code 451 - which allows server operators to operate with greater transparency in circumstances where issues of law or public policy affect their operation [Bray].

Impacts: - Right to freedom of expression - Right to political participation - Right to participate in cultural life, arts and science - Right to freedom of assembly and association

5.3.2.1.7. Open Standards

Question(s): Is your protocol fully documented in a way that it could be easily implemented, improved, build upon and/or further developed? Do you depend on proprietary code for the implementation, running or further development of your protocol? Does your protocol favor a particular proprietary specification over technically equivalent and competing specification(s), for instance by making any incorporated vendor specification "required" or "recommended" [RFC2026]? Do you normatively reference another standard that is not available without cost? Are you aware of any patents that would prevent your standard from being fully implemented?

Explanation: The Internet was able to developed into the global network of networks because of the existence of open, non-proprietary standards [Zittrain]. They are crucial for enabling interoperability. Yet, open standards are not explicitly defined within the IETF. On the subject, [RFC2606] states: Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined at the IETF. National

and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be "open external standards" for the purposes of the Internet Standards Process. Similarly, [RFC3935] does not define open standards but does emphasize the importance of 'open process': any interested person can participate in the work, know what is being decided, and make his or her voice heard on the issue. Part of this principle is the IETF's commitment to making its documents, WG mailing lists, attendance lists, and meeting minutes publicly available on the Internet.

Open standards are important as they allow for permissionless innovation, which is important to maintain the freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist. It is at the heart of the Internet as we know it, and to maintain its fundamentally open nature, we need to be mindful of the need for developing open standards.

All standards that need to be normatively implemented should be freely available and with reasonable protection for patent infringement claims, so it can also be implemented in open source or free software. Patents have often held back open standardization or been used against those deploying open stadards, particularly in the domain of cryptography [newegg]. Patents in open standards or in normative references to other standards should have a patent disclosure [notewell], royalty-free licensing [patentpolicy], or some other form of reasonable protection. Reasonable patent protection should includes but is not limited to cryptographic primitives.

Example: [RFC6108] describes a system for providing critical end-user notifications to web browsers, which has been deployed by Comcast, an Internet Service Provider (ISP). Such a notification system is being used to provide near-immediate notifications to customers, such as to warn them that their traffic exhibits patterns that are indicative of malware or virus infection. There are other proprietary systems that can perform such notifications, but those systems utilize Deep Packet Inspection (DPI) technology. In contrast to DPI, this document describes a system that does not rely upon DPI, and is instead based in open IETF standards and open source applications.

Impacts:

- Right to freedom of expression

- Right to participate in cultural life, arts and science

5.3.2.1.8. Heterogeneity Support

Question(s): Does your protocol support heterogeneity by design? Does your protocol allow for multiple types of hardware? Does your protocol allow for multiple types of application protocols? Is your protocol liberal in what it receives and handles? Will it remain usable and open if the context changes? Does your protocol allow there to be well-defined extension points? Do these extension points to allow open innovation possibly have security and privacy ramifications, and if so,how can these be dealt with?

Explanation: The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and Internet service providers, each with their own separate policy concerns, there is a large heterogeneity of administrative domains and pricing structures. As a result, the heterogeneity principle proposed in [RFC1958] needs to be supported by design [FIArch].

Example: Heterogeneity is inevitable and needs be supported by design. Multiple types of hardware must be allowed for, e.g. transmission speeds differing by at least 7 orders of magnitude, various computer word lengths, and hosts ranging from memory-starved microprocessors up to massively parallel supercomputers. Multiple types of application protocol must be allowed for, ranging from the simplest such as remote login up to the most complex such as distributed databases [RFC1958].

Impacts: - Right to freedom of expression - Right to security

5.3.2.1.9. Anonymity

Question(s): Did you have a look at the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.1 ?

Explanation: Anonymity refers to the condition of an identity being unknown or concealed [RFC4949]. It is an important feature for many end-users, as it allows them different degrees of privacy online.

Example: Often standards expose private information, it is important to consider ways to mitigate the obvious privacy impacts. For instance, a feature which uses deep packet inspection or geolocation

data could refuse to open this data to third parties, that might be able to connect the data to a physical person.

Impacts: - Right to non-discrimination - Right to political participation - Right to freedom of assembly and association - Right to security

5.3.2.1.10. Pseudonymity

Question(s): Have you considered the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.2 ? Does this specification collect personally derived data? Does the standard utilize data that is personally-derived, i.e. derived from the interaction of a single person, or their device or address? Does this specification generate personally derived data, and if so how will that data be handled?

Explanation: Pseudonymity - the ability to disguise one's identity online - is an important feature for many end-users, as it allows them different degrees of disguised identity and privacy online.

Example: Designing a standard that exposes private information, it is important to consider ways to mitigate the obvious impacts. For instance, a feature which uses deep packet inspection or geolocation data could refuse to open this data to third parties, that might be able to connect the data to a physical person.

Impacts:

- Right to non-discrimination

- Right to freedom of assembly and association

5.3.2.1.11. Accessibility

Question(s): Is your protocol designed to provide an enabling environment for people who are not able-bodied? Have you looked at the W3C Web Accessibility Initiative for examples and guidance? Is your protocol optimized for low bandwidth and high latency connections? Could your protocol also be developed in a stateless manner?

Explanation: The Internet is fundamentally designed to work for all people, whatever their hardware, software, language, culture, location, or physical or mental ability. When the Internet meets this goal, it is accessible to people with a diverse range of hearing, movement, sight, and cognitive ability [W3CAccessibility]. Sometimes in the design of protocols, websites, web technologies, or

web tools, barriers are created that exclude people from using the Web.

Example: The HTML protocol as defined in [RFC1866] specifically requires that every image must have an alt attribute (with a few exceptions for HTML5) to ensure images are accessible for people that cannot themselves decipher non-text content in web pages.

Impacts: - Right to non-discrimination - Right to freedom of assembly and association - Right to education - Right to political participation

5.3.2.1.12. Localization

Question(s): Does your protocol uphold the standards of internationalization? Have made any concrete steps towards localizing your protocol for relevant audiences?

Explanation: Localization refers to the adaptation of a product, application or document content to meet the language, cultural and other requirements of a specific target market (a locale) [W3Ci18nDef]. It is also described as the practice of translating an implementation to make it functional in a specific language or for users in a specific locale (see Internationalization).

Example: The Internet is a global medium, but many of its protocols and products are developed with a certain audience in mind, that often share particular characteristics like knowing how to read and write in ASCII and knowing English. This limits the ability of a large part of the world's online population from using the Internet in a way that is culturally and linguistically accessible. An example of a protocol that has taken into account the view that individuals like to have access to data in their native language can be found in [RFC1766]. This protocol labels the information content with an identifier for the language in which it is written. And this allows information to be presented in more than one language.

Impacts: - Right to non-discrimination - Right to participate in cultural life, arts and science - Right to Freedom of Expression

5.3.2.1.13. Decentralization

Question(s): Can your protocol be implemented without one single point of control? If applicable, can your protocol be deployed in a federated manner? What is the potential for discrimination against users of your protocol? How can use of your protocol be used to implicate users? Does your protocol create additional centralized points of control?

Explanation: Decentralization is one of the central technical concepts of the architecture, and embraced as such by the IETF [RFC3935]. It refers to the absence or minimization of centralized points of control - a feature that is assumed to make it easy for new users to join and new uses to unfold {{Brown}. It also reduces issues surrounding single points of failure, and distributes the network such that it continues to function if one or several nodes are disabled. With the commercialization of the Internet in the early 1990's there has been a slow move to move away from decentralization, to the detriment of the technical benefits of having a decentralized Internet.

Example: The bits traveling the Internet are increasingly susceptible to monitoring and censorship, from both governments and Internet service providers, as well as third (malicious) parties. The ability to monitor and censor is further enabled by the increased centralization of the network that creates central infrastructure points that can be tapped in to. The creation of peer-to-peer networks and the development of voice-over-IP protocols using peer-to-peer technology in combination with distributed hash table (DHT) for scalability are examples of how protocols can preserve decentralization [Pouwelse].

Impacts: - Right to freedom of assembly and association

5.3.2.1.14. Reliability

Question(s): Is your protocol fault tolerant? Does it degrade gracefully? Do you have a documented way to announce degradation? Do you have measures in place for recovery or partial healing from failure? Can your protocol maintain dependability and performance in the face of unanticipated changes or circumstances?

Explanation: Reliability ensures that a protocol will execute its function consistently and error resistant as described, and function without unexpected result. A system that is reliable degenerates gracefully and will have a documented way to announce degradation. It also has mechanisms to recover from failure gracefully, and if applicable, allow for partial healing. As with confidentiality, the growth of the Internet and fostering innovation in services depends on users having confidence and trust [RFC3724] in the network. For reliability it is necessary that services notify the users if a delivery fails. In the case of real-time systems in addition to the reliable delivery the protocol needs to safeguard timeliness.

Example: In the modern IP stack structure, a reliable transport layer requires an indication that transport processing has successfully completed, such as given by TCP's ACK message [RFC0793], and not

simply an indication from the IP layer that the packet arrived. Similarly, an application layer protocol may require an application-specific acknowledgement that contains, among other things, a status code indicating the disposition of the request (See [RFC3724]).

Impacts: - Right to security

5.3.2.1.15. Confidentiality

Question(s): Does this protocol expose information related to identifiers or data? If so, does it do so to each other protocol entity (i.e., recipients, intermediaries, and enablers) [RFC6973]? What options exist for protocol implementers to choose to limit the information shared with each entity? What operational controls are available to limit the information shared with each entity?

What controls or consent mechanisms does the protocol define or require before personal data or identifiers are shared or exposed via the protocol? If no such mechanisms or controls are specified, is it expected that control and consent will be handled outside of the protocol?

Does the protocol provide ways for initiators to share different pieces of information with different recipients? If not, are there mechanisms that exist outside of the protocol to provide initiators with such control?

Does the protocol provide ways for initiators to limit which information is shared with intermediaries? If not, are there mechanisms that exist outside of the protocol to provide users with such control? Is it expected that users will have relationships that govern the use of the information (contractual or otherwise) with those who operate these intermediaries? Does the protocol prefer encryption over clear text operation?

Does the protocol provide ways for initiators to express individuals' preferences to recipients or intermediaries with regard to the collection, use, or disclosure of their personal data?

Explanation: Confidentiality refers to keeping your data secret from unintended listeners [RFC3552]. The growth of the Internet depends on users having confidence that the network protects their private information [RFC1984].

Example: Protocols that do not encrypt their payload make the entire content of the communication available to the idealized attacker along their path. Following the advice in [RFC3365], most such protocols have a secure variant that encrypts the payload for

confidentiality, and these secure variants are seeing ever-wider deployment. A noteworthy exception is DNS [RFC1035], as DNSSEC [RFC4033]does not have confidentiality as a requirement. This implies that, in the absence of changes to the protocol as presently under development in the IETF's DNS Private Exchange (DPRIVE) working group, all DNS queries and answers generated by the activities of any protocol are available to the attacker. When store-and-forward protocols are used (e.g., SMTP [RFC5321]), intermediaries leave this data subject to observation by an attacker that has compromised these intermediaries, unless the data is encrypted end-to-end by the application-layer protocol or the implementation uses an encrypted store for this data [RFC7624].

Impacts:

- Right to security

5.3.2.1.16. Integrity

Question(s): Does your protocol maintain and assure the accuracy of data? Does your protocol maintain and assure the consistency of data? Does your protocol in any way allow for the data to be (intentionally or unintentionally) altered?

Explanation: Integrity refers to the maintenance and assurance of the accuracy and consistency of data to ensure it has not been (intentionally or unintentionally) altered.

Example: See authenticity

Impacts:

- Right to security

5.3.2.1.17. Authenticity

Question(s): Do you have sufficient measures to confirm the truth of an attribute of a single piece of data or entity? Can the attributes get garbled along the way (see security)? If relevant have you implemented IPsec, DNSsec, HTTPS and other Standard Security Best Practices?

Explanation: Authenticity ensures that data does indeed come from the source it claims to come from. This is important to prevent attacks or unauthorized access and use of data.

Example: Authentication of data is important to prevent vulnerabilities and attacks, like man-in-the-middle-attacks. These

attacks happen when a third party (often for malicious reasons) intercepts a communication between two parties, inserting themselves in the middle and posing as both parties. In practice this looks as follows:

Alice wants to communicate with Bob. Alice sends data to Bob. Niels intercepts the data sent to Bob. Niels reads and alters the message to Bob. Bob cannot see the data did not come from Alice but from Niels. Niels intercepts and alters the communication as it is sent between Alice and Bob. Niels knows all.

Wat iImpacts:

- Right to security

5.3.2.1.18. Acceptability

Question(s): Do your protocols follow the principle of non-discrimination? Do your protocols follow the principle of content agnosticism? Does your protocol take into account the needs of special needs (Internet) groups, like the audio-visually impaired? Also see availability.

Explanation: The Internet is a global medium. Yet, there continue to be issues surrounding acceptability - the extent to which standards are non-discriminatory and relevant to the widest range of end-users - that need to be resolved. Many standards are not suitable for end-users who are not-ablebodied, or otherwise restricted in their ability to access the Internet in its current form (text, data and English heavy). Development of new standards should consider the ways in which they exclude or include non-traditional user communities.

Example: Designing a feature that could make access to websites for non-able bodied people more difficult.

- Right to education

- Right to freedom of expression

- Right to freedom of assembly and association

5.3.2.1.19. Adaptability

Question(s): Is your protocol written in such a way that is would be easy for other protocols to be developed on top of it, or to interact with it? Does your protocol impact permissionless innovation? See 'Connectivity' above.

Explanation: Adaptability is closely interrelated permissionless innovation, both maintain the freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist. It is at the heart of the Internet as we know it, and to maintain its fundamentally open nature, we need to be mindful of the impact of protocols on maintaining or reducing permissionless innovation to ensure the Internet can continue to develop.

Example: WebRTC generates audio and/or video data. In order to ensure that WebRTC can be used in different locations by different parties it is important that standard Javascript APIs are developed to support applications from different voice service providers. Multiple parties will have similar capabilities, in order to ensure that all parties can build upon existing standards these need to be adaptable, and allow for permissionless innovation.

Impacts:

- Right to education
- Freedom of expression
- Freedom of assembly and association

6. Acknowledgements

A special thanks to all members of the hrpc RG who contributed to this draft. The following deserve a special mention:

- Joana Varon for helping draft the first iteration of the methodology, previous drafts and the direction of the film Net of Rights and working on the interviews at IETF92 in Dallas.
- Daniel Kahn Gillmor (dkg) for helping with the first iteration of the glossary as well as a lot of technical guidance, support and language suggestions.
- Claudio Guarnieri for writing the first iterations of the case studies on VPN, HTTP, and Peer to Peer.
- Will Scott for writing the first iterations of the case studies on DNS, IP, XMPP.
- Avri Doria for proposing writing a glossary in the first place, help writing the initial proposals and Internet Drafts and contributing to the glossary.

and Stephane Bortzmeyer, John Curran, Barry Shein, Joe Hall, Joss Wright, Harry Halpin, and Tim Sammut who made a lot of excellent suggestions, many of which found their way directly into the text. We want to thank Shane Kerr, Giovane Moura, James Gannon, and Scott Craig for their reviews and testing the HRPC guidelines in the wild. We would also like to thank Molly Sauter, Arturo Filasto, Nathalie Marechal, Eleanor Saitta and all others who provided input on the draft or the conceptualization of the idea.

7. Security Considerations

As this document 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 [3]. 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

10. References

10.1. Informative References

[Abbate] Abbate, J., "Inventing the Internet", MIT Press , 2000, <https://mitpress.mit.edu/books/inventing-internet>.

[Abibil] Danchev, D., "Dissecting 'Operation Ababil' - an OSINT Analysis", 2012, <http://ddanchev.blogspot.be/2012/09/dissecting-operation-ababil-osint.html>.

[Adrian] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J., Heninger, N., Springall, D., Thome, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella Beguelin, S., and P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", ACM Conference on Computer and Communications Security 2015: 5-17 , 2015.

[Appelbaum]
Appelbaum, J., Gibson, A., Kabish, V., Kampf, L., and L. Ryge, "NSA targets the privacy-conscious", 2015, <http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html>.

[Babbie] Babbie, E., "The Basics of Social Research", Belmont CA Cengage , 2010.

[Benkler] Benkler, Y., "The wealth of Networks - How social production transforms markets and freedom", New Haven and London - Yale University Press , 2006, <http://is.gd/rxUpTQ>.

[Berners-Lee]
Berners-Lee, T. and M. Fischetti, "Weaving the Web,", HarperCollins p 208, 1999.

[BernersLeeHalpin]
Berners-Lee, T. and H. Halpin, "Defend the Web", 2012, <http://www.ibiblio.org/hhalpin/homepage/publications/def-timbl-halpin.pdf>.

[Bhargavan]
Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Pironti, A., and P. Strub, "Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS", IEEE Symposium on Security and Privacy 2014: 98-113 , 2014.

[Bless] Bless, R. and C. Orwat, "Values and Networks", 2015.

[Blumenthal]
Blumenthal, M. and D. Clark, "Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world", ACM Transactions on Internet Technology, Vol. 1, No. 1, August 2001, pp 70-109. , 2001.

[Bray] Bray, T., "A New HTTP Status Code for Legally-restricted Resources", 2016, <https://tools.ietf.org/html/draft-ietf-httpbis-legally-restricted-status-04>.

[Broeders]
Broeders, D., "The public core of the Internet", WRR , 2015, <http://www.wrr.nl/en/publications/publication/article/de-publieke-kern-van-het-internet-1/>.

[Brown] Brown, I. and M. Ziewitz, "A Prehistory of Internet Governance", Research Handbook on Governance of the Internet. Cheltenham, Edward Elgar. , 2013.

[BrownMarsden] Brown, I. and C. Marsden, "Regulating code", MIT Press , 2013, <https://mitpress.mit.edu/books/regulating-code>.

[Brownetal] Brown, I., Clark, D., and D. Trossen, "Should specific values be embedded in the Internet Architecture?", Sigcomm , 2010, <http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf>.

[Cath] Cath, C., "A Case Study of Coding Rights: Should Freedom of Speech Be Instantiated in the Protocols and Standards Designed by the Internet Engineering Task Force?", 2015, <https://www.ietf.org/mail-archive/web/hrpc/current/pdf36GrmRM84S.pdf>.

[CathFloridi] Cath, C. and L. Floridi, "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights", August 2016.

[Clark] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", Proc SIGCOMM 88, ACM CCR Vol 18, Number 4, August 1988, pp. 106-114. , 1988.

[Clarketal] Clark, D., Wroclawski, J., Sollins, K., and R. Braden, "Tussle in cyberspace - defining tomorrow's Internet", ACM Digital Library , 2005, <https://dl.acm.org/citation.cfm?id=1074049>.

[Collins] Collins, K., "Hacking Team's oppressive regimes customer list revealed in hack", 2015, <http://www.wired.co.uk/news/archive/2015-07/06/hacking-team-spyware-company-hacked>.

[Daedalus] Clark, D., "The Contingent Internet", Daedalus Winter 2016, Vol. 145, No. 1. p. 9-17 , 2016, <http://www.mitpressjournals.org/toc/daed/current>.

[Davidsonetal]
Davidson, A., Morris, J., and R. Courtney, "Strangers in a strange land", Telecommunications Policy Research Conference , 2002, <https://www.cdt.org/files/publications/piais.pdf>.

[Denardis14]
Denardis, L., "The Global War for Internet Governance", Yale University Press , 2014, <https://www.jstor.org/stable/j.ctt5vkz4n>.

[Denardis15]
Denardis, L., "The Internet Design Tension between Surveillance and Security", IEEE Annals of the History of Computing (volume 37-2) , 2015, <http://is.gd/7GAnFy>.

[Denzin] Denzin, N. and Y. Lincoln, "Handbook of Qualitative Research", Thousand Oaks CA Sage , 2000, <http://www.amazon.com/SAGE-Handbook-Qualitative-Research-Handbooks/dp/1412974178>.

[Doty] Doty, N., "Automated text analysis of Requests for Comment (RFCs)", 2014, <https://github.com/npdoty/rfc-analysis>.

[Douceur] Douceur, J., "The Sybil Attack", 2002, <http://research.microsoft.com:8082/pubs/74220/IPTPS2002.pdf>.

[Dutton] Dutton, W., "Freedom of Connection, Freedom of Expression: the Changing legal and regulatory Ecology Shaping the Internet.", 2011, <http://portal.unesco.org/ci/en/ev.php-URL_ID=31397%26URL_DO=DO_TOPIC%26URL_SECTION=201.html>.

[Elahi] Elahi, T. and I. Goldberg, "CORDON - A taxonomy of Internet Censorship Resistance Strategies", 2012, <http://cacr.uwaterloo.ca/techreports/2012/cacr2012-33.pdf>.

[FIArch] "Future Internet Design Principles", January 2012, <http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf>.

[FRAMEWORK]
ISO/IEC, ., "Information technology - Framework for internationalization, prepared by ISO/IEC JTC 1/SC 22/WG 20 ISO/IEC TR 11017", 1997.

[Franklin]
Franklin, U., "The Real World of Technology", 1999, <http://houseofanansi.com/products/the-real-world-of-technology-digital>.

[Geertz] Clifford, G., "Kinship in Bali", Chicago University of Chicago Press. , 1975, <http://press.uchicago.edu/ucp/books/book/chicago/K/bo3625088.html>.

[Googlepatent]
Google, ., "Method and device for network traffic manipulation", 2012, <https://www.google.com/patents/EP2601774A1?cl=en>.

[GreenMovement]
Villeneuve, N., "Iran DDoS", 2009, <https://www.nartv.org/2009/06/16/iran-ddos/>.

[HRC2012] United Nations Human Rights Council, "UN General Assembly Resolution "The right to privacy in the digital age" (A/C.3/68/L.45)", 2011, <http://daccess-ods.un.org/TMP/554342.120885849.html>.

[Haagsma] Haagsma, L., "Deep dive into QUANTUM INSERT", 2015, <http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[ICESCR] United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights", 1966, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>.

[Jabri] Jabri, V., "Discourses on Violence - conflict analysis reconsidered", Manchester University Press , 1996.

[Kaye] Kaye, D., "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 2016, <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx>.

[King] King, C., "Power, Social Violence and Civil Wars", Washington D.C. United States Institute of Peace Press , 2007.

[Lessig] Lessig, L., "Code - And Other Laws of Cyberspace, Version 2.0.", New York Basic Books , 2006, <http://codev2.cc/>.

[Marcak] Marcak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., and V. Paxson, "China's Great Fire Cannon", 2015, <https://citizenlab.org/2015/04/chinas-great-cannon/>.

[Marquis-Boire] Marquis-Boire, M., "Schrodinger's Cat Video and the Death of Clear-Text", 2014, <https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/>.

[Mueller] Mueller, M., "Networks and States", MIT Press , 2010, <https://mitpress.mit.edu/books/networks-and-states>.

[Musiani] Musiani, F., "Giants, Dwarfs and Decentralized Alternatives to Internet-based Services - An Issue of Internet Governance", Westminister Papers in Communication and Culture , 2015, <http://doi.org/10.16997/wpcc.214>.

[NETmundial] NETmundial, "NETmundial Multistakeholder Statement", 2014, <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

[PETS2015VPN] Pera, V., Barbera, M., Tyson, G., Haddadi, H., and A. Mei, "A Glance through the VPN Looking Glass", 2015, <http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf>.

[Penney] Penney, J., "Chilling Effects: Online Surveillance and Wikipedia Use", 2016, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645>.

[Peterson] Peterson, A., Gellman, B., and A. Soltani, "Yahoo to make SSL encryption the default for Webmail users. Finally.", 2013, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[Pouwelse]
Pouwelse, Ed, J., "Media without censorship", 2012, <https://tools.ietf.org/html/draft-pouwelse-censorfree-scenarios>.

[RFC0226] Karp, P., "Standardization of host mnemonics", RFC 226, DOI 10.17487/RFC0226, September 1971, <http://www.rfc-editor.org/info/rfc226>.

[RFC0760] Postel, J., "DoD standard Internet Protocol", RFC 760, DOI 10.17487/RFC0760, January 1980, <http://www.rfc-editor.org/info/rfc760>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[RFC0894] Hornig, C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks", STD 41, RFC 894, DOI 10.17487/RFC0894, April 1984, <http://www.rfc-editor.org/info/rfc894>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

[RFC1631] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, <http://www.rfc-editor.org/info/rfc1631>.

[RFC1766] Alvestrand, H., "Tags for the Identification of Languages", RFC 1766, DOI 10.17487/RFC1766, March 1995, <http://www.rfc-editor.org/info/rfc1766>.

[RFC1866] Berners-Lee, T. and D. Connolly, "Hypertext Markup Language - 2.0", RFC 1866, DOI 10.17487/RFC1866, November 1995, <http://www.rfc-editor.org/info/rfc1866>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <http://www.rfc-editor.org/info/rfc1958>.

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <http://www.rfc-editor.org/info/rfc1984>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <http://www.rfc-editor.org/info/rfc2026>.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <http://www.rfc-editor.org/info/rfc2277>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <http://www.rfc-editor.org/info/rfc2606>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <http://www.rfc-editor.org/info/rfc2775>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <http://www.rfc-editor.org/info/rfc3365>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <http://www.rfc-editor.org/info/rfc3552>.

[RFC3724] Kempf, J., Ed., Austein, R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <http://www.rfc-editor.org/info/rfc3724>.

[RFC3935] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <http://www.rfc-editor.org/info/rfc3935>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <http://www.rfc-editor.org/info/rfc4084>.

[RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <http://www.rfc-editor.org/info/rfc4101>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[RFC4906] Martini, L., Ed., Rosen, E., Ed., and N. El-Aawar, Ed., "Transport of Layer 2 Frames Over MPLS", RFC 4906, DOI 10.17487/RFC4906, June 2007, <http://www.rfc-editor.org/info/rfc4906>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", RFC 5944, DOI 10.17487/RFC5944, November 2010, <http://www.rfc-editor.org/info/rfc5944>.

[RFC6108] Chung, C., Kasyanov, A., Livingood, J., Mody, N., and B. Van Lieu, "Comcast's Web Notification System Design", RFC 6108, DOI 10.17487/RFC6108, February 2011, <http://www.rfc-editor.org/info/rfc6108>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[RFC6365] Hoffman, P. and J. Klensin, "Terminology Used in Internationalization in the IETF", BCP 166, RFC 6365, DOI 10.17487/RFC6365, September 2011, <http://www.rfc-editor.org/info/rfc6365>.

[RFC6797] Hodges, J., Jackson, C., and A. Barth, "HTTP Strict Transport Security (HSTS)", RFC 6797, DOI 10.17487/RFC6797, November 2012, <http://www.rfc-editor.org/info/rfc6797>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7469] Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April 2015, <http://www.rfc-editor.org/info/rfc7469>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <http://www.rfc-editor.org/info/rfc7540>.

[RFC7574] Bakker, A., Petrocco, R., and V. Grishchenko, "Peer-to-Peer Streaming Peer Protocol (PPSPP)", RFC 7574, DOI 10.17487/RFC7574, July 2015, <http://www.rfc-editor.org/info/rfc7574>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <http://www.rfc-editor.org/info/rfc7624>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <http://www.rfc-editor.org/info/rfc7626>.

[RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles", RFC 7725, DOI 10.17487/RFC7725, February 2016, <http://www.rfc-editor.org/info/rfc7725>.

[RSF] RSF, "Syria using 34 Blue Coat Servers to spy on Internet users", 2013, <https://en.rsf.org/syria-syria-using-34-blue-coat-servers-23-05-2013,44664.html>.

[Rachovitsa]
Rachovitsa, A., "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", International Journal of Law and Information Technology , 2015, <https://www.ietf.org/mail-archive/web/hrpc/current/pdfRBnRYFeVsm.pdf>.

[Richie] Richie, J. and J. Lewis, "Qualitative Research Practice - A Guide for Social Science Students and Researchers", London Sage , 2003, <http://www.amazon.co.uk/Qualitative-Research-Practice-Students-Researchers/dp/0761971106>.

[Rideout] Rideout, A., "Making security easier", 2008, <http://gmailblog.blogspot.de/2008/07/making-security-easier.html>.

[Saltzer] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design", ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288. , 1984.

[Sauter] Sauter, M., "The Coming Swarm", Bloomsbury, London , 2014.

[Schillace]
Schillace, S., "Default https access for Gmail", 2010, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[Schneier]
Schneier, B., "Attacking Tor - how the NSA targets users' online anonymity", 2013, <http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>.

[Schroeder]
Schroeder, I. and B. Schmidt, "Introduction - Violent Imaginaries and Violent Practice", London and New York Routledge , 2001, <http://resourcelists.st-andrews.ac.uk/items/BFC20363-67B0-B3EF-EA48-13E5230E7899.html>.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <http://www.un.org/en/documents/udhr/>.

[UNGA2013]
United Nations General Assembly, "UN General Assembly Resolution "The right to privacy in the digital age" (A/C.3/68/L.45)", 2013, <http://daccess-ods.un.org/TMP/1133732.05065727.html>.

[W3CAccessibility]
W3C, "Accessibility", 2015, <https://www.w3.org/standards/webdesign/accessibility>.

[W3Ci18nDef]
W3C, "Localization vs. Internationalization", 2010, <http://www.w3.org/International/questions/qa-i18n.en>.

[WP-Debugging]
"Debugging", n.d., <https://en.wikipedia.org/wiki/Debugging>.

[WP-Stateless]
"Stateless protocol", n.d., <https://en.wikipedia.org/wiki/Stateless_protocol>.

[Walfish] Walfish, M., Stribling, J., Krohn, M., Balakrishnan, H., Morris, R., and S. Shenker, "Middleboxes No Longer Considered Harmful", 2004, <http://nms.csail.mit.edu/doa>.

[WynsbergheMoura]
Wynsberghe, A. and G. Moura, "The concept of embedded values and the example of internet security", 2013, <http://doc.utwente.nl/87095/>.

[Zittrain]
Zittrain, J., "The Future of the Internet - And How to Stop It", Yale University Press , 2008, <https://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf?sequence=1>.

[Zuckerman]
Zuckerman, E., Roberts, H., McGrady, R., York, J., and J. Palfrey, "Report on Distributed Denial of Service (DDoS) Attacks", The Berkman Center for Internet and Society at Harvard University , 2010, <https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf>.

[ars] Anderson, N., "P2P researchers - use a blocklist or you will be tracked... 100% of the time", 2007, <http://arstechnica.com/uncategorized/2007/10/p2p-researchers-use-a-blocklist-or-you-will-be-tracked-100-of-the-time/>.

[bbc-wikileaks] BBC, "Whistle-blower site taken offline", 2008, <http://news.bbc.co.uk/2/hi/technology/7250916.stm>.

[bitmessage] Bitmessage, "Bitmessage Wiki?", 2014, <https://bitmessage.org/wiki/Main_Page>.

[caida] Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., and A. Pescape, "Analysis of Country-wide Internet Outages Caused by Censorship", 2013, <http://www.caida.org/publications/papers/2014/outages_censorship/outages_censorship.pdf>.

[freenet1] Freenet, "What is Freenet?", n.d., <https://freenetproject.org/whatis.html>.

[freenet2] Ian Clarke, ., "The Philosphy behind Freenet?", n.d., <https://freenetproject.org/philosophy.html>.

[greatfirewall] Anonymous, ., "Towards a Comprehensive Picture of the Great Firewall's DNS Censorship", 2014, <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>.

[hall] Hall, J., Aaron, M., and B. Jones, "A Survey of Worldwide Censorship Techniques", 2015, <https://tools.ietf.org/html/draft-hall-censorship-tech-01>.

[namecoin] Namecoin, "Namecoin - Decentralized secure names", 2015, <https://namecoin.info/>.

[natusage] Maier, G., Schneider, F., and A. Feldmann, "NAT usage in Residential Broadband networks", 2011, <http://www.icsi.berkeley.edu/pubs/networking/NATusage11.pdf>.

[newegg] Mullin, J., "Newegg on trial: Mystery company TQP rewrites the history of encryption", 2013, <http://arstechnica.com/tech-policy/2013/11/newegg-on-trial-mystery-company-tqp-re-writes-the-history-of-encryption/>.

[notewell] IETF, "Note Well", 2015, <https://www.ietf.org/about/note-well.html>.

[patentpolicy] W3C, "W3C Patent Policy", 2004, <https://www.w3.org/Consortium/Patent-Policy-20040205/>.

[pidgin] js, . and Pidgin Developers, "-XMPP- Invisible mode violating standard", July 2015, <https://developer.pidgin.im/ticket/4322>.

[quic] The Chromium Project, "QUIC, a multiplexed stream transport over UDP", 2014, <https://www.chromium.org/quic>.

[spdy] The Chromium Project, "SPDY - An experimental protocol for a faster web", 2009, <https://www.chromium.org/spdy/spdy-whitepaper>.

[spiegel] SPIEGEL, "Prying Eyes - Inside the NSA's War on Internet Security", 2014, <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>.

[sslstrip] Marlinspike, M., "Software >> sslstrip", 2011, <https://moxie.org/software/sslstrip/>.

[techyum] Violet, ., "Official - vb.ly Link Shortener Seized by Libyan Government", 2010, <http://techyum.com/2010/10/official-vb-ly-link-shortener-seized-by-libyan-government/>.

[torproject] The Tor Project, ., "Tor Project - Anonymity Online", 2007, <https://www.torproject.org/>.

[torrentfreak1] Van der Sar, E., "Proposal for research on human rights protocol considerations", 2015, <https://torrentfreak.com/is-your-isp-messing-with-bittorrent-traffic-find-out-140123/>.

[torrentfreak2]
Andy, ., "LAWYERS SENT 109,000 PIRACY THREATS IN GERMANY DURING 2013", 2014, <https://torrentfreak.com/lawyers-sent-109000-piracy-threats-in-germany-during-2013-140304/>.

[tribler] Delft University of Technology, Department EWI/PDS/Tribler, "About Tribler", 2013, <https://www.tribler.org/about.html>.

[turkey] Akguel, M. and M. Kirlidoğ, "Internet censorship in Turkey", 2015, <http://policyreview.info/articles/analysis/internet-censorship-turkey>.

[ververis]
Vasilis, V., Kargiotakis, G., Filasto, A., Fabian, B., and A. Alexandros, "Understanding Internet Censorship Policy - The Case of Greece", 2015, <https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-update.pdf>.

[wikileaks]
Sladek, T. and E. Broese, "Market Survey : Detection & Filtering Solutions to Identify File Transfer of Copyright Protected Content for Warner Bros. and movielabs", 2011, <https://wikileaks.org/sony/docs/05/docs/Anti-Piracy/CDSA/EANTC-Survey-1.5-unsecured.pdf>.

[xmppmanifesto]
Saint-Andre, P. and . XMPP Operators, "A Public Statement Regarding Ubiquitous Encryption on the XMPP Network", 2014, <https://raw.githubusercontent.com/stpeter/manifesto/master/manifesto.txt>.

10.2. URIs

[1] mailto:node@domain/home

[2] mailto:node@domain/work

[3] mailto:hrpc@ietf.org

Authors' Addresses

Niels ten Oever
Article19

EMail: niels@article19.org

Corinne Cath
Oxford Internet Institute

EMail: corinnecath@gmail.com