

Human Rights Protocol Considerations Research Group
Internet-Draft

Intended status: Informational

Expires: January 17, 2018

N. ten Oever

ARTICLE 19

C. Cath

Oxford Internet Institute

July 16, 2017

Research into Human Rights Protocol Considerations
draft-irtf-hrpc-research-14

Abstract

This document aims to propose guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations [RFC6973]. If you want to apply this work to your own, you can directly go to Section 6. The rest of the document explains the background of the guidelines and how they were developed.

This document is not an Internet Standards Track specification; it is published for informational purposes.

This informational document has consensus for publication from the Internet Research Task Force (IRTF) Human Right Protocol Considerations Research Group. It is the first milestone in a longer term research effort and has been reviewed both by the research group and by individuals from outside the research group. Many of the topics discussed are still under discussion in the research group and will be subjects of continuing research.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 17, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Vocabulary used	5
3. Research Questions	11
4. Literature and Discussion Review	11
5. Methodology	14
5.1. Data Sources	15
5.1.1. Discourse analysis of RFCs	16
5.1.2. Interviews with members of the IETF community	16
5.1.3. Participant observation in Working Groups	16
5.2. Data analysis strategies	16
5.2.1. Identifying qualities of technical concepts that relate to human rights	16
5.2.2. Relating human rights to technical concepts	18
5.2.3. Map cases of protocols, implementations and networking paradigms that adversely impact human rights or are enablers thereof	21
6. Model for developing human rights protocol considerations	39
6.1. Human rights threats	39
6.2. Guidelines for human rights considerations	41
6.2.1. Connectivity	41
6.2.2. Privacy	42
6.2.3. Content agnosticism	43
6.2.4. Security	43
6.2.5. Internationalization	44
6.2.6. Censorship resistance	45
6.2.7. Open Standards	46
6.2.8. Heterogeneity Support	47
6.2.9. Anonymity	48
6.2.10. Pseudonymity	49
6.2.11. Accessibility	50
6.2.12. Localization	50

6.2.13. Decentralization	51
6.2.14. Reliability	52
6.2.15. Confidentiality	53
6.2.16. Integrity	54
6.2.17. Authenticity	54
6.2.18. Adaptability	55
6.2.19. Outcome Transparency	56
7. Document Status	56
8. Acknowledgements	57
9. Security Considerations	57
10. IANA Considerations	58
11. Research Group Information	58
12. References	58
12.1. Informative References	58
12.2. URIs	74
Authors' Addresses	74

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]

"The Internet isn't value-neutral, and neither is the IETF."

[RFC3935]

The evergrowing interconnectedness of Internet and society increases the impact of the Internet on the lives of individuals. Because of this, the design and development of the Internet infrastructure also has a growing impact on society. This has led to a 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 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 exercise human rights such as freedom of expression

and freedom of association [FOC], as defined in the Universal Declaration of Human Rights [UDHR]. The purpose of the Internet to be a global network of networks that provides unfettered connectivity to all users and for any content [RFC1958]. This objective of stimulating global connectivity contributes to the Internet's role as an enabler of human rights. The Internet has given people a platform to exchange opinions, gather information, and it has enabled people of different backgrounds and genders to participate in the public debate, it has also allowed people to congregate and organize. 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 networks that make up the Internet. 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 infrastructure 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 infrastructure. Additionally, access to freely available information gives people access to knowledge that enables them to help satisfy other human rights, as such the Internet increasingly becomes a pre-condition for human rights rather than a supplement.

Human rights can be in conflict with each other, such as the right to freedom of expression and the right to privacy. In such cases the different affected rights need to be balanced. In order to do this it is crucial that the rights impacts are clearly documented in order to mitigate the potential harm. Making that process tangible and practical for protocol developers is what this research aims to ultimately contribute to. Technology can never be fully equated with a human right. Whereas a specific technology might be strong enabler of a specific human right, it might have an adverse impact on another human right. In this case decisions on design and deployment need to take this into account.

The open nature of the initial technical design and its open standards, as well as developments like open source, fostered freedom of communication. What emerged was a network of networks that could enable everyone to connect and to exchange data, information and code. For many, enabling such connections became 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 of networks. New protocols, particularly those that upgrade the core infrastructure of the network, should be designed to continue to enable fundamental human rights.

The IETF has produced guidelines and procedures to ensure and galvanize the privacy of individuals 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 Section 6 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 specific human rights threats, and potentially stimulate authors to think about alternative design choices.

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], [RFC1958]. 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, building as much as possible on existing definitions, and where these were not available definitions have been developed.

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 property of being genuine and able to be verified and be trusted. [RFC4949]

Blocking the practice of preventing access to resources in the aggregate [RFC7754]. Both blocking and filtering can be implemented at the level of "services" (web hosting or video streaming, for example) or at the level of particular "content." [RFC7754]

Censorship technical mechanisms, that include both blocking and filtering, that certain political or private actors around the world use to block or degrade Internet traffic. For further details on the various elements of Internet censorship see [hall]

Censorship resistance Methods and measures to mitigate Internet censorship.

Confidentiality The property that data is not disclosed to system entities unless they have been authorized to know the data.
[RFC4949].

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]. Different types of connectivity are further specified in [RFC4084].

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

Content agnosticism Treating network traffic identically regardless of content.

Decentralized Implementation or deployment of standards, protocols or systems without one single point of control.

End-to-End The principle that application-specific functions should not be embedded into the network and thus stay at the end-points:

in many cases, especially when dealing with failures, the right decisions can only be made with the corresponding application-specific knowledge, which is available at the end-points not in the network.

The end-to-end principle is one of the key architectural guidelines of the Internet. The argument in favor of the end-to-end approach to system design is laid out in the fundamental paper by Saltzer, Reed, and Clark [Saltzer] [Clark]. In it, the authors argue in favor of radical simplification: systems designers should only build the essential and shared functions into the network, as most functions can only be implemented at network end points. Building features into the network for the benefit of certain applications, will come at the expense of others. As such, as a general system designers should attempt to steer clear of building anything into the network that is not a bare necessity for its functioning. Following the end-to-end principle is crucial for innovation, as it makes innovation at the edges possible without having to make changes to the network, and the robustness of the network. Various aspects of end-to-end connectivity are further elaborated on in [RFC2775].

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

Filtering the practice of preventing access to specific resources within an aggregate [RFC7754].

Heterogeneity 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 independent 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]

Human rights Human rights are principles and norms that are indivisible, interrelated, unalienable, universal, and mutually reinforcing that have been codified in national and international bodies of law. The Universal Declaration of Human Rights [UDHR] is the most well-known document in the history of human rights. The aspirations from this documents were later codified into

treaties such as the [ICCPR] and the [ICESCR], after which signatory countries were obliged to reflect them in their national bodies of law. There is also a broad recognition that not only states have an obligations vis a vis human rights, but non-state actors do so as well.

Integrity The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [RFC4949].

Interoperable A property of a documented standard or protocol which allows different independent implementations to work with each other without any restriction on functionality.

Internationalization (i18n) 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 encoding up to local guesswork (which leads, of course, to interoperability problems) [RFC3536]. 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 ad hoc 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 with [RFC2026]: 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 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.

Reliability Reliability ensures that a protocol will execute its function consistently 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 [dict].

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

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.

Scalability The ability to handle increased or decreased system parameters (e.g., number of end-systems, users, data flows, routing entries. etc.) predictably within defined expectations. There should be a clear definition of its scope and applicability. The limits of a system's scalability should be defined. Growth or shrinkage of these parameters is typically considered by orders of magnitude.

Strong encryption / cryptography Used to describe a cryptographic algorithm that would require a large amount of computational power to defeat it. [RFC4949]. In the modern usage of the definition 'strong encryption' this refers to an amount of computing power current not available, not even to major state-level actors.

Transparency In this context transparency is linked to the comprehensibility of a protocol in relation to the choices it makes for both user and protocol developers and implementers and to its outcome.

outcome transparency, is linked to the comprehensibility of the effects of a protocol in relation to the choices it makes for both user and protocol developers and implementers, including the

comprehensibility of possible unintended consequences of protocol choices (e.g. lack of authenticity may lead to lack of integrity and negative externalities)

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 some Internet processes and 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]. According to [Abbate]: "protocols are politics by other means". This statement would probably not garner IETF consensus, but it nonetheless confers that protocols are based on decision making, most often by humans. In this process the values and ideas about the role that a particular technology should perform in society is embedded into the design. Often these design decisions are part pure-technical, and part inspired by certain world view of how technology should function that is inspired by personal, corporate and political views. Within the community of IETF participants there is a strong desire to solve technical problems and minimize engagement with political processes and non-protocol related political issues.

Since the late 1990's a burgeoning group of academics and practitioners researched questions surrounding the societal impact of protocols, and the politics 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 infrastructure 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, infrastructure maintenance 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 three reasons: first, the rights in the UDHR are not absolute. Second, technology is not the only tool in the tussle over human rights. 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 to 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 architectures, 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 architectures or whether the architectures need 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, but rather that the existing infrastructure should be seen as an entity of public value.

Bless and Orwat [Bless] represent a fourth position. They argue that it is too 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].

It is important to contextualize the technical discussion with the academic discussions on this issue. The academic discussions also are important to document as they inform the position of the authors of this document. The Research Groups position is that hard-coding human rights into protocols is complicated and changes with the context. At this point is difficult to say whether hard-coding human rights into protocols is wise or feasible. Additionally, there are many human rights, but that not all are relevant for ICTs. A partial catalog, with references to sources, of human rights related to ICTs

can be found here [Hill2014]. It is however important to make conscious and explicit design decisions that take into account the human rights protocol considerations guidelines developed below. This will contribute to the understanding of the impact protocols can have on human rights, both for developers and for users. In addition, it contributes to the careful consideration of the impact that a specific protocol might have on human rights and that concrete design decisions are documented in the protocol.

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]

This document details the steps taken in the research into human rights protocol considerations by the hrpc research 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 infrastructure as it pertains to the work of the IETF.

The discourse analysis was operationalized using qualitative and quantitative means. The first step taken by the authors and contributors 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 infrastructure 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

Over 30 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 were 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. Several of the participants opted to remain anonymous, if you are interested in this data set please contact the authors.

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 general themes, technical concepts, and use-cases about human rights and protocols were extracted. This process started at the IETF91 meeting and continues today.

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 Section 2). 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 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

created. 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 selected RFCs

Identifying the protocols and standards that are related to human rights and create a human rights enabling 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 and applied in different circumstances, create an enabling environment for exercising human rights on the Internet.

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

While interviewing experts, investigating 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, as indicated in the vocabulary section.

5.2.1.4. Translating Human Rights Concepts into Technical Definitions

The previous steps allowed for the clarification of relations 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 subsection 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 partially combined can create an enabling environment for human rights.

5.2.1.5. List technical terms that when partially combined can create an enabling environment for human rights

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

Architectural principles and system properties	Enabling features for user rights
/-----\	
+=====+	+=====+
=	=
=	=
=	End to end
=	Reliability
=	Resilience
=	Interoperability
=	Transparency
=	Data minimization
=	Permissionless innovation
=	Graceful degradation
=	Connectivity
=	Heterogeneity support
=	=
=	=
+=====+	+=====+

figure 1 - relation between architectural principles and enabling features for user rights.

5.2.2. Relating human rights to technical concepts

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 in better understanding the roles specific technical concepts have with regards to their contribution to an enabling environment for people to exercise their human rights.

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

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

figure 2 - relation between specific technical concepts with regards to their contribution to an enabling environment for people to exercise their human rights

5.2.3. Map cases of protocols, implementations and networking paradigms that adversely impact human rights or are enablers thereof

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

It is important to note that the assessment here is not a general judgment on these protocols, nor an exhaustive listing of all the potential negative or positive impacts on human rights they might have. When they were conceived, there were many criteria to take into account. For instance, relying on a centralized service can be bad for freedom of speech (it creates one more control point, where censorship could be applied) but it may be a necessity if the endpoints are not connected and reachable permanently. So, when we say "protocol X has feature Y, which may endanger the freedom of speech", it does not mean that protocol X is bad and even less that its authors were evil. The goal here is to show, with actual examples, that the design of protocols have practical consequences for some human rights and these consequences have to be considered in the design phase.

5.2.3.1. 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 of the issues discussed here (with the big exception of NAT, see Address Translation) 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-based traffic 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 to 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.

5.2.3.1.1. 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 people to communicate today, [caida] and can be seen as a restriction of the ability for people 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 do exist, such as the Accountable and Private Internet Protocol [APIP] and Hornet [Hornet] as well as source routing. The latter would allow for the sender to choose a pre-defined (safe) route and spoofing of the source IP address, which are technically supported by the IPv4 protocol, but neither are considered good practice on the Internet [Farrow]. While projects like [torproject] provide an alternative implementation of anonymity in connections, they have been developed in spite of the IPv4 protocol design.

5.2.3.1.2. 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. [RFC3022] 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 an extra possible hurdle for freedom of expression in its design, even though a viable alternative exists. There is a particular problem surrounding NATs and VPN (as well as other connections used for privacy purposes) as NATs sometimes cause VPNs not to work.

5.2.3.2. 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 which function in line with ICANN's policy by answering queries for which organizations have been delegated to manage registration under each Top Level Domain (TLD). The DNS is organized as a rooted tree, 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 [CoE].

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.

5.2.3.2.1. Removal of records

There have been a number of cases where the records for a domain are removed from the name system due to political events. Examples of this removal includes the 'seizure' of wikileaks [bbc-wikileaks] and the names of illegally operating gambling operations by the United States Immigrations and Customs Enforcement unit (ICE). In the first case, a US court ordered the registrar to take down the domain. In the second, ICE 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.

(While mentioning alternative techniques, this is not a comparison of DNS with Namecoin: the latter has its own problems and limitations. The idea here is to show that there are several possible choices, and they have consequences for human rights.)

5.2.3.2.2. 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 can be observed in Chinese network.

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 more excessive blocking of content than was legally required or requested (also known as overblocking). 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].

Users can switch to another resolver, for instance a public one. The distorter can then try to block or hijack the connection to this resolver. This may start an arms race, the user switching to secured connections to this alternative resolver ([RFC7858]), the disruptor then trying to find more sophisticated ways to block or hijack. In some cases, this search for an alternative, non-disrupting resolver, may lead to more centralisation, many people going to a few big commercial public resolvers.

5.2.3.2.3. 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 its 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.

5.2.3.3. 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. Its simple design strongly contributed to the fact that 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) [RFC6101], and later of Transport Layer Security (TLS) [RFC5246], also happened during the 1990s, the fact that HTTP doesn't mandate the use of such encryption layers to developers and service providers, was one of the reasons for a very late adoption of encryption. Only in the middle of the 2000s did we observe 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 certain (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 is taking steady steps to move to the encrypted version of HTTP, HTTPSecure (HTTPS).

While this is commendable, we must not lose track of the fact that different protocols, implementations, configurations and networking paradigms can intersect such that they (can be used to) adversely impact human rights. For instance, certain countries will throttle HTTPS connections forcing users to switch to the (unthrottled) HTTP to facilitate surveillance [Aryanetall].

5.2.3.3.1. 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 were the first ones to enable SSL by default. Google introduced an option for its GMail users to navigate with SSL only in 2008 [Rideout], and turned TLS 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 mail service providers to follow suit. 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 are being 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], certificate pinning [RFC7469] and/or DANE [RFC6698] should be used.

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 [WP-Tempora] and NSA's XKEYSCORE [Greenwald]. 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 some 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 some 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 at a country level [WSJ]. 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.

5.2.3.3.2. 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 actively compromising computers and mobile devices. If an HTTP session travels in the 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, add malware, 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. Certain companies are known to have network injection gear within their products portfolio [Marquis-Boire]. The technology devised and produced by some of them 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 led to human rights abuses and illegitimate surveillance of journalists, human rights defenders, and political activists in many countries around the world [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. In addition to decreasing latency to improve page loading speeds it also facilitates more efficient use of connectivity in low-bandwidth 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, also does not support opportunistic encryption, even though that is now addressed in [RFC8164].

5.2.3.4. 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 on 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 assemble through the protocol.

5.2.3.4.1. 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.

5.2.3.4.2. 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 committed 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.

5.2.3.4.3. 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.

5.2.3.5. Peer to Peer

Peer-to-Peer (P2P) is a distributed network architecture [RFC5694] 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 vary 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 a popular architecture for networks and applications that require (or encourage) decentralization. A prime example is Bitcoin (and similar cryptocurrencies), as well as Bitcoin and proprietary multimedia applications.

In a time of heavily centralized online services, peer-to-peer is regularly described as an alternative, more democratic, and resistant option 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 important 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.

5.2.3.5.1. 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 aimed 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.

5.2.3.5.2. Throttling

Peer-to-Peer traffic (and BitTorrent in particular) represents a significant percentage of global Internet traffic [Sandvine] 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 throttling 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.

5.2.3.5.3. 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 led 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].

5.2.3.5.4. 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 complete, environmentally sustainable, and fully distributed solutions to Sybil attacks, and routing via 'friends' allows users to be de-anonymized via their social graph. It is important to note that Sybil attacks in this context (e.f. astroturfing) are relevant to more than P2P protocols. And are also common on web based systems, and exploited by governments and commercial entities.

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.

5.2.3.6. Virtual Private Network

The Virtual Private Networks (VPN) that are being discussed here are point-to-point connections that enables two computers to communicate over an encrypted tunnel. There are multiple implementations and protocols used in the deployment of VPNs, 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 monitoring 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

[Insinuator] [Alshalanetal] , 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.

5.2.3.6.1. No anonymity against VPN provider

One of the common misconceptions 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, in contrast 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.

5.2.3.6.2. 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 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.

5.2.3.6.3. 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.

5.2.3.6.4. 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.

5.2.3.6.5. 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.

5.2.3.6.6. Traffic Correlation

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 nullify the use of a VPN and ultimately expose the activity and the identity of a user at risk.

5.2.3.7. 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 typically because some content is only for identified users, based on a payment, or on a special status in the organisation. 403 is most of

the time sent by the origin server, not by an intermediary. If a firewall prevents a government employee to access pornography on a work-computer, it does not use 403.

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 [RFC7725].

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 nonetheless important to note that HTTP status code 451 is not a solution to detect all occasions of censorship. A large swath of Internet filtering occurs in the network, at a lower level than HTTP, rather than the server itself. For these forms of censorship 451 plays a limited role, as typical censoring intermediaries won't generate it. Besides technical reasons, 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. 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.

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.

5.2.3.8. DDoS attacks

Many individuals, not excluding IETF engineers, have argued that DDoS attacks are fundamentally against freedom of expression. Technically DDoS attacks are when one or multiple host overload the bandwidth or resources of another host by flooding it with traffic or making resource intensive requests, causing it to temporarily stop being available to users. One can roughly differentiate three types of DDoS attacks: Volume Based Attacks (This attack aims to make the host unreachable by using up all its bandwidth, often used techniques are: UDP floods and ICMP floods), Protocol Attacks (This attack 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).

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 the overwhelming majority of cases, the clients are hacked hosts 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.

All of these issues seem to suggest that the IETF should try to ensure that their protocols cannot be used for DDoS attacks, which is consistent with the long-standing IETF consensus that DDoS is an attack that protocols should mitigate them to the extent they can [BCP72]. Decreasing the number of vulnerabilities in protocols and (outside of IETF) the number of bugs in the network stacks of routers or computers could address this issue. The IETF can clearly play a role in bringing about some of these changes but the IETF cannot be expected to take a positive stance on (specific) DDoS attacks, or create protocols to enable some attacks and inhibit others. What the IETF can do is critically reflect on its role in the development of the Internet, and how this impacts the ability of people to exercise their human rights, such as freedom of expression.

6. Model for developing human rights protocol considerations

This section outlines a set of human rights protocol considerations for protocol developers. It provides questions engineers should ask themselves when developing or improving protocols if they want to understand their human rights impact. It should however be noted that the impact of a protocol cannot solely be deduced from its design, but its usage and implementation should also be studied to form a full protocol human rights impact assessment.

The questions are based on the research performed by the hrpc research group which has been documented before these considerations. The research establishes that human rights relate to standards and protocols and offers 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. With this the contours of a model for developing human rights protocol considerations has taken shape.

6.1. 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 individuals perceived as threats to the state are subjected to torture or extrajudicial killing or detention on the basis of information gathered by state agencies through information leakage in protocols.

This section 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 [BCP72], 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]: "The main source of the values of human rights is the International Bill of Human Rights that is composed of the Universal Declaration of Human Rights [UDHR] along with the International Covenant on Civil and Political Rights [ICCPR] and the International Covenant on Economic, Social and Cultural Rights [ICESCR]. In the light of several cases of Internet censorship, the Human Rights Council Resolution 20/8 was adopted in 2012 [UNHRC2016], affirming ". . . that the same rights that people have offline must also be protected online. . . ". In 2015, the Charter of Human Rights and Principles for the Internet [IRP] was developed and released. According to these documents, some examples of human rights relevant for ICT systems are human dignity (Art. 1 UDHR), non-discrimination (Art. 2), rights to life, liberty and security (Art. 3), freedom of opinion and expression (Art. 19), freedom of assembly and association (Art. 20), rights to equal protection, legal remedy, fair trial, due process, presumed innocent (Art. 7-11), appropriate social and international order (Art. 28), participation in public affairs (Art. 21), participation in cultural life, protection of intellectual property (Art. 27), and privacy (Art. 12)." A partial catalog of human rights related to ICTs, including economic rights, can be found in [Hill2014].

This is by no means an attempt to exclude specific rights or prioritize some rights over others. If other rights seem relevant, please contact the authors.

6.2. Guidelines for human rights considerations

This section provides guidance for document authors in the form of a questionnaire about protocols and their (potential) impact. 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]. These guidelines do not seek to replace any existing referenced specifications, but rather contribute to them and look at the design process from a human rights perspective.

Protocols and Internet Standard might benefit from a documented 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 takes specific human rights threats into account. 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]), and the addition of a human rights protocol considerations section has also not yet been proposed. In considering these questions, authors will need to be aware of the potential of technical advances or the passage of time to undermine protections. In general, considerations of rights are likely to be more effective if they are considered given a purpose and specific use cases, rather than as abstract absolute goals.

6.2.1. Connectivity

Question(s): Does your protocol add application-specific functions to intermediary nodes? Could this functionality be added to end nodes instead of intermediary nodes? Is your protocol optimized for low bandwidth and high latency connections? Could your protocol also be developed in a stateless manner?

Explanation: The end-to-end principle [Saltzer] holds that 'the intelligence is end to end rather than hidden in the network' [RFC1958]. The end-to-end principle is important for the robustness of the network and innovation. Such robustness of the network is crucial to enabling human rights like freedom of expression.

Example: Middleboxes (which can be Content Delivery Networks, Firewalls, NATs or other intermediary nodes that provide other 'services' than routing) serve many legitimate purposes. But the protocols guiding them, can 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.

Impacts:

- Right to freedom of expression
- Right to freedom of assembly and association

6.2.2. 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? Could your protocol improve data minimization? Does your document identify potentially sensitive logged data by your protocol and/or for how long that needs to be retained for technical reasons?

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]. If a protocol provides insufficient privacy protection it may have a negative impact on freedom of expression as users self-censor for fear of surveillance, or find themselves unable to express themselves freely.

Example: See [RFC6973]

Impacts:

- Right to freedom of expression
- Right to non-discrimination

6.2.3. Content agnosticism

Question(s): If your protocol impacts packet handling, does it use user data (packet data that is not included in the header)? Is it making decisions based on the payload of the packet? Does your protocol prioritize certain content or services over others in the routing process? Is the protocol transparent about the prioritization that is made (if any)?

Explanation: Content agnosticism refers to the notion that network traffic is treated identically regardless of payload, with some exception where it comes to effective traffic handling, for instance where it comes to delay tolerant or delay sensitive packets, based on the header.

Example: Content agnosticism prevents payload-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

6.2.4. Security

Question(s): Did you have a look at Guidelines for Writing RFC Text on Security Considerations [BCP72]? Have you found any "attacks that are somewhat related to your protocol yet considered out of scope of your document? Would these attacks be pertinent to the human rights enabling features of the Internet (as described 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. 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 [BCP72].

Example: See [BCP72].

Impacts:

- Right to freedom of expression
- Right to freedom of assembly and association
- Right to non-discrimination
- Right to security

6.2.5. Internationalization

Question(s): Does your protocol have text strings that have to be understood or entered by humans? Does your protocol allow Unicode? If so, do you accept texts in one charset (which must be UTF-8), or several (which is dangerous for interoperability)? If character sets or encodings other than UTF-8 are allowed, does your protocol mandate a proper tagging of the charset? 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.

In the current IETF policy [RFC2277], internationalization is aimed at user-facing strings, not protocol elements, such as the verbs used by some text-based protocols. (Do note that some strings are both content and protocol elements, such as the identifiers.) If the Internet wants to be a global network of networks, the protocols

should work with other languages than English and other character sets than latin characters. It is therefore crucial that at least the content carried by the protocol can be in any script, and that all scripts are treated equally.

Example: See localization

Impacts:

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

6.2.6. Censorship resistance

Question(s): Does this protocol introduce new identifiers or reuse existing identifiers (e.g. MAC addresses) that might be associated with persons or content? Does your protocol make it apparent or transparent when access to a resource is restricted? 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: In the development of the IPv6 protocol it was discussed to embed a Media Access Control (MAC) address into unique IP addresses. This would make it possible for 'eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node. [RFC4941] This is why Privacy Extensions for Stateless Address Autoconfiguration in IPv6 have been introduced. [RFC4941]

Identifiers of content exposed within a protocol might be used to facilitate censorship, as in the case of Application Layer based censorship, which affects protocols like HTTP. Denial or restriction of access 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 [RFC7725].

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

6.2.7. Open Standards

Question(s): Is your protocol fully documented in a way that it could be easily implemented, improved, built 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 (and could it possible be done without)? Are you aware of any patents that would prevent your standard from being fully implemented [RFC3979] [RFC6701]?

Explanation: The Internet was able to be 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, [RFC2026] 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 standards, particularly in the domain of cryptography [newegg]. An exemption of this is sometimes made when a protocol is standardized that normatively relies on specifications produced by other SDOs that are not freely available. 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 include 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

6.2.8. 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 allow for open innovation?

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 political participation

6.2.9. 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]. Even though full anonymity is hard to achieve, it is a non-binary concept. Making pervasive monitoring and tracking harder is important for many users as well as for the IETF [RFC7258]. Achieving a higher level of anonymity is an important feature for many end-users, as it allows them different degrees of privacy online.

Example: Often protocols expose personal data, it is important to consider ways to mitigate the obvious privacy impacts. A protocol that uses data that could help identify a sender (items of interest) should be protected from third parties. For instance if one wants to hide the source/destination IP addresses of a packet, the use of IPsec in tunneling mode (e.g., inside a virtual private network) can be helpful to protect from third parties likely to eavesdrop packets exchanged between the tunnel endpoints.

Impacts:

- Right to non-discrimination
- Right to political participation

- Right to freedom of assembly and association
- Right to security

6.2.10. Pseudonymity

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

Explanation: Pseudonymity - the ability to use a persistent identifier not linked to one's offline identity" straight away - 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 personal data, it is important to consider ways to mitigate the obvious impacts. While pseudonyms cannot be simply reverse engineered - some early approaches simply took approaches such as simple hashing of IP addresses, these could then be simply reversed by generating a hash for each potential IP address and comparing it to the pseudonym - limiting the exposure of personal data remains important.

Pseudonymity means using a pseudonym instead of one's "real" name. There are many reasons for users to use pseudonyms, for instance to: hide their gender, protect themselves against harassment, protect their families' privacy, frankly discuss sexuality, or develop a artistic or journalistic persona without retribution from an employer, (potential) customers, or social surrounding. [geekfeminism] The difference between anonymity and pseudonymity is that a pseudonym often is persistent. "Pseudonymity is strengthened when less personal data can be linked to the pseudonym; when the same pseudonym is used less often and across fewer contexts; and when independently chosen pseudonyms are more frequently used for new actions (making them, from an observer's or attacker's perspective, unlinkable)." [RFC6973]

Impacts:

- Right to non-discrimination
- Right to freedom of assembly and association

6.2.11. 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?

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 [HTML5] specifically requires that every image must have an alt attribute (with a few exceptions) 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

6.2.12. 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 [RFC5646]. 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

6.2.13. 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 the 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 of the networks, 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 expression
- Right to freedom of assembly and association

6.2.14. Reliability

Question(s): Is your protocol fault tolerant? Does it degrade gracefully? Can your protocol resist malicious degradation attempts? 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. It is important here to draw a distinction between random degradation and malicious degradation. Many current attacks against TLS, for example, exploit TLS's ability to gracefully degrade to older cipher suites - from a functional perspective, this is good. From a security perspective, this can be very bad. 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 freedom of expression
- Right to security

6.2.15. 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 [BCP72]. The growth of the Internet depends on users having confidence that the network protects their personal data [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 privacy
- Right to security

6.2.16. Integrity

Question(s): Does your protocol maintain, assure and/or verify the accuracy of payload 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: Integrity verification 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 changing the content of the data. In practice this looks as follows:

Alice wants to communicate with Bob.
Corinne forges and sends a message to Bob, impersonating Alice. Bob cannot see the data from Alice was altered by Corinne.
Corinne intercepts and alters the communication as it is sent between Alice and Bob.
Corinne is able to control the communication content.

Impacts:

- Right to freedom of expression
- Right to security

6.2.17. 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 certain 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.
Corinne intercepts the data sent to Bob.
Corinne reads (and potentially alters) the message to Bob.
Bob cannot see the data did not come from Alice but from Corinne.

When there is proper authentication the scenario would be as follows:

Alice wants to communicate with Bob.
Alice sends data to Bob.
Corinne intercepts the data sent to Bob.
Corinne reads and alters the message to Bob.
Bob can see the data did not come from Alice but from Corinne.

Impacts:

- Right to privacy
- Right to freedom of expression
- Right to security

6.2.18. Adaptability

Question(s): Is your protocol written in such a way that it 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 with 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

6.2.19. Outcome Transparency

Question(s): Are the effects of your protocol fully and easily comprehensible, including with respect to unintended consequences of protocol choices?

Explanation: certain technical choice may have unintended consequences.

Example: lack of authenticity may lead to lack of integrity and negative externalities, of which spam is an example. Lack of data that could be used for billing and accounting can lead to so-called "free" arrangements which obscure the actual costs and distribution of the costs, for example the barter arrangements that are commonly used for Internet interconnection; and the commercial exploitation of personal data for targeted advertising which is the most common funding model for the so-called "free" services such as search engines and social networks.

Impacts: - Freedom of expression - Privacy - Freedom of assembly and association - Access to information

7. Document Status

This document has been developed within the framework of the Human Rights Protocols Considerations Research Group, based on discussions on the hrpc mailinglist and during hrpc sessions, where this document also has been extensively discussed. The document has received eleven in-depth reviews on list, and received many comments from

inside and outside the IRTF and IETF community. The research group has reached consensus on publishing this document as informational research group consensus document.

8. 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 with writing the initial proposals and Internet Drafts, her reviews and contributions 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 Amelia Andersdotter, Stephen Farrell, Stephane Bortzemeyer, Shane Kerr, Giovane Moura, James Gannon, Alissa Cooper, Andrew Sullivan, S. Moonesamy, Roland Bless 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, Richard Hill and all others who provided input on the draft or the conceptualization of the idea. Thanks to Edward Snowden for his comments regarding the impact of protocols on the rights of users at IETF93.

9. Security Considerations

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

10. IANA Considerations

This document has no actions for IANA.

11. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research 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>

12. References

12.1. 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.
- [Alshalanetal] Alshalan, A., Pisharody, S., and D. Huang, "A Survey of Mobile VPN Technologies", 2016, <<http://ieeexplore.ieee.org.proxy.uba.uva.nl:2048/stamp/stamp.jsp?arnumber=7314859>>.
- [APIP] Naylor, D., Mukerjee, M., and P. Steenkiste, "Balancing accountability and privacy in the network", SIGCOMM '14 Proceedings of the 2014 ACM conference on SIGCOMM Pages 75-86 , 2014, <<https://dl.acm.org/citation.cfm?id=2626306>>.

- [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>.
- [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/>>.
- [Aryanetall] Aryan, S., Aryan, H., and J. Alex Halderman, "Internet Censorship in Iran: A First Look", 2013, <<https://jhalderm.com/pub/papers/iran-foci13.pdf>>.
- [Babbie] Babbie, E., "The Basics of Social Research", Belmont CA Cengage , 2010.
- [bbc-wikileaks] BBC, "Whistle-blower site taken offline", 2008, <<http://news.bbc.co.uk/2/hi/technology/7250916.stm>>.
- [BCP72] IETF, "Guidelines for Writing RFC Text on Security Considerations", 2003, <<https://datatracker.ietf.org/doc/bcp72/>>.
- [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.

- [bitmessage] Bitmessage, "Bitmessage Wiki?", 2014, <https://bitmessage.org/wiki/Main_Page>.
- [Bless] Bless, R. and C. Orwat, "Values and Networks", 2015.
- [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.
- [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>.
- [BrownMarsden] Brown, I. and C. Marsden, "Regulating code", MIT Press , 2013, <<https://mitpress.mit.edu/books/regulating-code>>.
- [caida] Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., and A. Pescapé, "Analysis of Country-wide Internet Outages Caused by", 2013, <http://www.caida.org/publications/papers/2014/outages_censorship/outages_censorship.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", July 2017.
- [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>>.
- [CoE] Council of Europe, "Applications to ICANN for community-based new generic top level domains: Opportunities and challenges from a human rights perspective", 2016, <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b5a14>>.
- [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>>.
- [Davidsonetal] Davidson, A., Morris, J., and R. Courtney, "Strangers in a strange land", Telecommunications Policy Research Conference , 2002, <<https://www.cdt.org/files/publications/piaais.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>>.
- [dict] BusinessDictionary.com. WebFinance, Inc., "Reliability (dictionary entry)", 2016, <<http://www.businessdictionary.com/definition/reliability.html>>.
- [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>.
- [Farrow] Farrow, R., "Source Address Spoofing", 2016,
<<https://technet.microsoft.com/library/cc723706.aspx>>.
- [FIArch] "Future Internet Design Principles", January 2012,
<http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf>.
- [FOC] Ministers of the Freedom Online Coalition, "The Tallinn Agenda - Recommendations for Freedom Online", 2014,
<<https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.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>>.
- [freenet1] Freenet, "What is Freenet?", n.d.,
<<https://freenetproject.org/whatis.html>>.
- [freenet2] Ian Clarke, ., "The Philosophy behind Freenet?", n.d.,
<<https://freenetproject.org/philosophy.html>>.
- [geekfeminism] Geek Feminism Wiki, "Pseudonymity", 2015,
<<http://geekfeminism.wikia.com/wiki/Pseudonymity>>.
- [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>>.
- [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>>.
- [GreenMovement] Villeneuve, N., "Iran DDoS", 2009, <<https://www.nartv.org/2009/06/16/iran-ddos/>>.
- [Greenwald] Greenwald, G., "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", 2013, <<https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>>.
- [Haagsma] Haagsma, L., "Deep dive into QUANTUM INSERT", 2015, <<http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/>>.
- [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>>.
- [Hill2014] Hill, R., "Partial Catalog of Human Rights Related to ICT Activities", 2014, <<http://www.apig.ch/UNIGE%20Catalog.pdf>>.
- [Hornet] Chen, C., Asoni, D., Barrera, D., Danezis, G., and A. Perrig, "HORNET: High-speed Onion Routing at the Network Layer", CCS '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security Pages 1441-1454 , 2015, <<https://dl.acm.org/citation.cfm?id=2813628>>.
- [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>>.
- [HTML5] W3C, "HTML5", 2014, <<https://www.w3.org/TR/html5/>>.

- [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>>.
- [Insinuator] Schiess, N., "Vulnerabilities & attack vectors of VPNs (Pt 1)", 2013, <<https://www.insinuator.net/2013/08/vulnerabilities-attack-vectors-of-vpns-pt-1/>>.
- [IRP] Internet Rights and Principles Dynamic Coalition, "10 Internet Rights & Principles", 2014, <http://internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_10RightsandPrinciples_28May2014-11.pdf>.
- [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/>>.

- [Meyer] Meyer, J., "Defining and Evaluating Resilience: A Performability Perspective, presentation at International Workshop on Performability Modeling of Computer and Communication Systems.", 2009.
- [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", Westminster Papers in Communication and Culture , 2015, <<http://doi.org/10.16997/wpcc.214>>.
- [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>>.
- [NETmundial] NETmundial, "NETmundial Multistakeholder Statement", 2014, <<http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.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/>>.
- [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>>.
- [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>>.
- [pidgin] js, . and Pidgin Developers, "-XMPP- Invisible mode violating standard", July 2015, <<https://developer.pidgin.im/ticket/4322>>.
- [Pouwelse] Pouwelse, Ed, J., "Media without censorship", 2012, <<https://tools.ietf.org/html/draft-pouwelse-censorfree-scenarios>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <<http://www.rfc-editor.org/info/rfc2775>>.
- [RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, DOI 10.17487/RFC3022, January 2001, <<http://www.rfc-editor.org/info/rfc3022>>.
- [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>>.

- [RFC3536] Hoffman, P., "Terminology Used in Internationalization in the IETF", RFC 3536, DOI 10.17487/RFC3536, May 2003, <<http://www.rfc-editor.org/info/rfc3536>>.
- [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>>.
- [RFC3979] Bradner, S., Ed., "Intellectual Property Rights in IETF Technology", RFC 3979, DOI 10.17487/RFC3979, March 2005, <<http://www.rfc-editor.org/info/rfc3979>>.
- [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>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <<http://www.rfc-editor.org/info/rfc4941>>.
- [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>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <<http://www.rfc-editor.org/info/rfc5246>>.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <<http://www.rfc-editor.org/info/rfc5321>>.

- [RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <<http://www.rfc-editor.org/info/rfc5646>>.
- [RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, DOI 10.17487/RFC5694, November 2009, <<http://www.rfc-editor.org/info/rfc5694>>.
- [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>>.
- [RFC6101] Freier, A., Karlton, P., and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0", RFC 6101, DOI 10.17487/RFC6101, August 2011, <<http://www.rfc-editor.org/info/rfc6101>>.
- [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>>.
- [RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <<http://www.rfc-editor.org/info/rfc6698>>.
- [RFC6701] Farrel, A. and P. Resnick, "Sanctions Available for Application to Violators of IETF IPR Policy", RFC 6701, DOI 10.17487/RFC6701, August 2012, <<http://www.rfc-editor.org/info/rfc6701>>.
- [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>>.
- [RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <<http://www.rfc-editor.org/info/rfc7754>>.
- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<http://www.rfc-editor.org/info/rfc7858>>.

- [RFC8164] Nottingham, M. and M. Thomson, "Opportunistic Security for HTTP/2", RFC 8164, DOI 10.17487/RFC8164, May 2017, <<http://www.rfc-editor.org/info/rfc8164>>.
- [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>>.
- [RSF] RSF, "Syria using 34 Blue Coat Servers to spy on Internet users", 2013, <<https://rsf.org/en/news/syria-using-34-blue-coat-servers-spy-internet-users>>.
- [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.
- [Sandvine] Sandvine, "Sandvine: Over 70% Of North American Traffic Is Now Streaming Video And Audio", 2015, <<https://www.sandvine.com/pr/2015/12/7/sandvine-over-70-of-north-american-traffic-is-now-streaming-video-and-audio.html>>.
- [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>>.

- [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>>.
- [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>>.

[UNHRC2016]

United Nations Human Rights Council, "UN Human Rights Council Resolution "The promotion, protection and enjoyment of human rights on the Internet" (A/HRC/32/L.20)", 2016, <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>>.

[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>>.

[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>>.

[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>>.

[WP-Tempora]

Wikipedia, "Tempora", 2016, <<https://en.wikipedia.org/wiki/Tempora>>.

[WSJ]

Sonne, P. and M. Coker, "Firms Aided Libyan Spies", 2011, <<http://www.wsj.com/articles/SB10001424053111904199404576538721260166388>>.

[WynsbergheMoura]

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

[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>>.

[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>.

12.2. URIs

[1] <mailto:node@domain/home>

[2] <mailto:node@domain/work>

[3] <mailto:hrpc@ietf.org>

Authors' Addresses

Niels ten Oever
ARTICLE 19

EMail: niels@article19.org

Corinne Cath
Oxford Internet Institute

EMail: corinnecath@gmail.com

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: August 10, 2017

N. ten Oever
Article19
February 06, 2017

Anonymity, Human Rights and Internet Protocols
draft-tenoever-hrpc-anonymity-00

Abstract

Anonymity is less discussed topic in the IETF than for instance security [RFC3552] or privacy [RFC6973]. This can be attributed to the fact anonymity is a hard technical problem or that anonymizing user data is not of specific market interest. It remains a fact that 'most internet users would like to be anonymous online at least occasionally' [Pew].

This document aims to break down the different meanings and implications of anonymity on a mediated computer network.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 10, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Vocabulary Used	2
3. Research Questions	3
4. Use Cases	4
5. Security Considerations	4
6. IANA Considerations	4
7. Research Group Information	4
8. References	4
8.1. Informative References	4
8.2. URIs	6
Author's Address	6

1. Introduction

There seems to be a clear need for anonymity when harassment on the Internet on the increase [Pew2] and the UN Special Rapporteur for Freedom of Expression call anonymity 'necessary for the exercise of the right to freedom of opinion and expression in the digital age' [UNHRC2015].

Nonetheless anonymity is not getting much discussion at the IETF, providing anonymity does not seem a (semi-)objective for many protocols, even though several documents contribute to improving anonymity such as [RFC7258], [RFC7626], [RFC7858].

There are initiatives on the Internet to improve end users anonymity, most notably [torproject], but this all relies on adding encryption in the application layer.

This document aims to break down the different meanings and implications of anonymity on a mediated computer network and to see whether (some parts of) anonymity should be taken into consideration in protocol development.

2. Vocabulary Used

Concepts in this draft currently strongly hinges on [AnonTerm]

Anonymity 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]

Linkability Linkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not. [AnonTerm]

Pseudonymity Derived from pseudonym, a persistent identity which is not the same as the entity's given name.

Unlinkability Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not. [AnonTerm]

Undetectability The impossibility of being noticed or discovered

Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not [AnonTerm]

Unobservability

Unobservability of an item of interest (IOI) means:
undetectability of the IOI against all subjects uninvolved in it
and

anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI. [AnonTerm]

3. Research Questions

Premise: activity on the network has the ability for is to be anonymous or authenticated

While analyzing protocols for their impact on users anonymity, would it make sense to ask the following questions:

1. How anonymous is the end user to:
 - o local network operator
 - o other networks you connect to
 - o your communications peer on the other end of the pipe
2. How well can they distinguish my identity from somebody else (with a similar communication) (ie linkability)

3. How does the protocol impact pseudonymity?

- o in case of long term pseudonymity
- o in case of short term pseudonymity

4. How does the protocol, in conjunction with other protocols, impact pseudonymity?

5. Could there be advice for protocol developers and implementers to improve anonymity and pseudonymity?

4. Use Cases

- multiple identities concurrently used, mixing them in operations / keeping them distinct (talking to XMPP, alias, etc)
- when you change identity, do cross stack analysis, so you have no bleedover, anonymity on a cross protocol, cross stack level

5. Security Considerations

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

6. IANA Considerations

This document has no actions for IANA.

7. Research Group Information

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

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

8. References

8.1. Informative References

- [AnonTerm] Pfitzmann, A. and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", 2010, <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf>.
- [Pew] Rainie, L., Kiesler, S., Kang, R., and M. Madden, "Anonymity, Privacy, and Security Online", 2013, <<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>>.
- [Pew2] Duggan, M., "Online Harassment", 2014, <<http://www.pewinternet.org/2014/10/22/online-harassment/>>.
- [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>>.
- [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>>.
- [RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <<http://www.rfc-editor.org/info/rfc7626>>.
- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<http://www.rfc-editor.org/info/rfc7858>>.
- [torproject] The Tor Project, ., "Tor Project - Anonymity Online", 2007, <<https://www.torproject.org/>>.

[UNHRC2015]

Kaye, D., "Anonymity, Privacy, and Security Online (A/HRC/29/32)", 2015,
<[www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)
Documents/A.HRC.29.32_AEV.doc>.

8.2. URIs

[1] <mailto:hrpc@ietf.org>

Author's Address

Niels ten Oever
Article19

EMail: niels@article19.org

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: August 13, 2018

S. Bortzmeyer
AFNIC
N. ten Oever
ARTICLE 19
February 09, 2018

Anonymity, Human Rights and Internet Protocols
draft-tenoever-hrpc-anonymity-02

Abstract

Anonymity is less discussed in the IETF than for instance security [RFC3552] or privacy [RFC6973]. This can be attributed to the fact anonymity is a hard technical problem or that anonymizing user data is not of specific market interest. It remains a fact that 'most internet users would like to be anonymous online at least occasionally' [Pew].

This document aims to break down the different meanings and implications of anonymity on a mediated computer network.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 13, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Vocabulary Used	3
3. Should protocols promote anonymity?	4
4. Example of use cases	5
4.1. Simultaneous use	5
4.2. Successive use	5
4.3. TODO	5
5. Practical advices	5
5.1. Protocol developers	5
5.2. Protocol implementors	6
6. Open Questions	6
7. Security Considerations	7
8. IANA Considerations	7
9. Research Group Information	7
10. Objections against anonymity	7
11. References	8
11.1. Informative References	8
11.2. URIs	10
Authors' Addresses	10

1. Introduction

There seems to be a clear need for anonymity online in an environment where harassment on the Internet is on the increase [Pew2] and the UN Special Rapporteur for Freedom of Expression calls anonymity 'necessary for the exercise of the right to freedom of opinion and expression in the digital age' [UNHRC2015].

Nonetheless anonymity is not getting much discussion at the IETF, providing anonymity does not seem a (semi-)objective for many protocols, even though several documents contribute to improving anonymity such as [RFC7258], [RFC7626], [RFC7858].

There are initiatives on the Internet to improve end users anonymity, most notably [torproject], but these initiatives rely on adding encryption in the application layer.

This document aims to break down the different meanings and implications of anonymity on a mediated computer network and to see

whether (some parts of) anonymity should be taken into consideration in protocol development.

2. Vocabulary Used

Concepts in this draft currently strongly hinges on [AnonTerm]

Anonymity 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]

Linkability Linkability of two or more items of interest (IOIs - Items Of Interest, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not. [AnonTerm]

Pseudonymity Derived from pseudonym, a persistent identity which is not the same as the entity's given (or official) name. For all IETF protocols, pseudonymity is a given: protocols don't care whether the identity is an official one or not. Even if the protocol allows to use official identities (for instance in the From: header of an Internet email), it does not require it. But it should be noted that, if the user cannot create new pseudonyms easily, pseudonyms suffer from linkability. Unlinkability depends on this ability to create new pseudonyms gratis and at will (good examples are SSH keys or Bitcoin addresses).

Unlinkability Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not. [AnonTerm]

Undetectability The impossibility of being noticed or discovered

Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not [AnonTerm]

Unobservability

Unobservability of an item of interest (IOI) means:
undetectability of the IOI against all subjects uninvolved in it
and

anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI. [AnonTerm]

It should be noted that the word "anonymity" is both very loaded politically (witness all the headlines about the "darknet") and poorly understood. Most texts talking about anonymity actually refer to pseudonymity (for instance, when people say that "Bitcoin is anonymous"). This confusion is even in the example given in [RFC4949] definition of anonymity.

Anonymity is strongly linked to unlinkability: if your actions are linkable, it suffices that one of them is tied to your identity, and anonymity is over.

It should be noted that anonymity is not binary: there have been these recent years a lot of progress of desanonymisation techniques (see also [GDPR], article 26). Data is never fully "anonymous", it is only more or less anonymous. [RFC6235] [MITdeano] [Utexas] [Article29]

3. Should protocols promote anonymity?

The amount of data that is generated by and about individuals is growing exponentially. This can be attributed to the fact that an ever increasing number of actions is digitally mediated, and the increase of connected sensors in the every day environment. Even though these two causes do not fully fall within the scope of the IETF, there is a significant part of these two examples that do.

TODO add here more examples of the need to anonymity

With the increase of data there is also an increasing ability for third parties to analyze human behaviour. It should be noted that any data that could identify an individual is personally identifiable information (PII). This means that information which can be used to distinguish an individual from other individuals can be considered as personally identifiable information. The access and control of personally identifiable information by a third party is a (potential) liability for both the third party and the individual. This liability could for example translate into a physical risk for the individual or into a legal risk for the third party under information security and privacy laws.

Some network operators argue that without the opportunity to persistently identify individual users it becomes harder to thwart attacks and troubleshoot network issues. Whereas identification might be helpful to address issues in some cases, it poses an inherent threat to the anonymity of users. Not protecting the anonymity of users leads to a deterioration of the right to privacy, and the right to freedom of opinion and expression. There can be limitations the right to privacy and freedom of expression, but these

should always be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives. It is clear that anonymity may make system and network administration different. To quote [RFC7824], "Those properties (stable and trackable IP addresses, derived from static identifiers) are convenient for system administrators". Here, there is a clear and fundamental tussle between the protection of the users and the ability of the system and network administrator to continue their work in the same way.

Anonymity will always be a balancing act between user protection (which requires a high level of anonymity) and other requirements for operations and research, such as routing information. Anonymity is by no means achieved by default in an online environment, nor has it been a strong consideration in protocol development in the development of the Internet. Increasing anonymity in the digital environment is not an easy task, exactly because the ubiquity of data that is generated and stored. But exactly the fact that we generate so much data urges us to address this issue.

4. Example of use cases

4.1. Simultaneous use

One user may use concurrently several identities, mixing them in operations, while wanting to keep them distinct. The protocol and its implementations should not preclude this use.

4.2. Successive use

One user may switch from one identity to another. In that case, it must be doable without a "bleedover" from the old identity to the new one.

4.3. TODO

TODO more use cases

5. Practical advices

5.1. Protocol developers

First, the protocol should avoid to have mandatory persistent identifiers.

Even without persistent identifiers, anonymity could be broken by examining the patterns of access. If an user visits each morning the three same Web sites, always in the same order, it will be easy to identify them even without persistent identifier. Protocol designers

should therefore ask themselves if patterns are easily visible, or obfuscated in some way.

If the protocol collects data and distributes it (see [RFC6235]), "anonymizing" the data is often suggested but it is notoriously hard. Do not think that just dropping the last byte of an IP address "anonymizes" data.

Pay attention to the fact that Internet actors do not all see the same thing. Consider the anonymity of the user with respect to:

- local network operator
- other networks you connect to
- your communications peer on the other end of the pipe
- intermediaries ([RFC6973])
- enablers ([RFC6973])
- someone who is in several roles, for instance a big state surveillance agency

5.2. Protocol implementors

Avoid adding options or configurations that create or might lead to patterns or regularities that are not explicitly required by the protocol.

An example is DHCP where sending a persistent identifier as the client name was not mandatory but, in practice, done by many implementations, before [RFC7844].

If an implementation allows for identity management, there should be a clear barrier between the identities to ensure that they cannot (easily) be associated with each other.

If there are anonymization option for the protocol, these should be enabled by default.

6. Open Questions

While analyzing protocols for their impact on users anonymity, would it make sense to ask the following questions:

1. How does the protocol impact pseudonymity? If the protocol limits the creation of new pseudonyms, it can limit their

usefulness to "hide" an user's identity. For instance, IP addresses are pseudonyms but, since they are not under end users's control, they have strong linkability. That's why they are rightly regarded as personal identifiers [EUcourt]. On the other hand, Bitcoin addresses are pseudonyms with limited linkability, since the user can always create a lot of them.

2. Could there be more advice for protocol developers and implementers to improve anonymity? (Besides the ones in Section 5.)

7. Security Considerations

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

8. IANA Considerations

This document has no actions for IANA.

9. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at <https://www.irtf.org/mailman/listinfo/hrpc> [2]

Archives of the list can be found at: <https://www.irtf.org/mail-archive/web/hrpc/current/index.html> [3]

10. Objections against anonymity

TODO: should be turned into an appendix. This draft is about how to allow anonymity, not about how to fight it.

For a long time, there have been objections against anonymity. This document won't attempt to rebuke them all, since it is concerned about how to ensure that protocols allow anonymity. But it is interesting to keep in mind that protocols never forbid anonymity. If smeones want his or her actions to be trackable, and under her or his official name, they can do so, by adding this information to their messages. In the same way, people are free not to engage with anonymous entities, in the same way that a SIP use, for instance, is free not to pick up a call if it comes from `sip:anonymous@anonymous.invalid`. This document is concerned about enabling anonymity, not about mandating it.

11. References

11.1. Informative References

- [AnonTerm] Pfitzmann, A. and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", 2010, <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf>.
- [Article29] Article29, ., "Opinion 05/2014 on Anonymisation Techniques", 2014, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
- [EUCourt] "EUCJ Case C-70/10: Scarlet Extended SA vs. Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM)", 2011, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:HTML&lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3BSFHas%2FXMRHeHVu46775ezw%3D%3D>.
- [GDPR] European Parliament and Council, ., "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", 2016, <<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>>.
- [MITdeano] de Montjoye, Y., Hidalgo, C., Verleysen, M., and V. Blondel, "Unique in the Crowd: The privacy bounds of human mobility", 2013, <<https://www.nature.com/articles/srep01376>>.
- [Pew] Rainie, L., Kiesler, S., Kang, R., and M. Madden, "Anonymity, Privacy, and Security Online", 2013, <<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>>.
- [Pew2] Duggan, M., "Online Harassment", 2014, <<http://www.pewinternet.org/2014/10/22/online-harassment/>>.

- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC6235] Boschi, E. and B. Trammell, "IP Flow Anonymization Support", RFC 6235, DOI 10.17487/RFC6235, May 2011, <<https://www.rfc-editor.org/info/rfc6235>>.
- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc7258>>.
- [RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <<https://www.rfc-editor.org/info/rfc7626>>.
- [RFC7824] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy Considerations for DHCPv6", RFC 7824, DOI 10.17487/RFC7824, May 2016, <<https://www.rfc-editor.org/info/rfc7824>>.
- [RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <<https://www.rfc-editor.org/info/rfc7844>>.
- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<https://www.rfc-editor.org/info/rfc7858>>.
- [torproject] The Tor Project, ., "Tor Project - Anonymity Online", 2007, <<https://www.torproject.org/>>.

[UNHRC2015]

Kaye, D., "Anonymity, Privacy, and Security Online (A/HRC/29/32)", 2015, <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>.

[Utexas]

Narayanan, A. and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets", 2008, <http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pd>.

11.2. URIs

[1] <mailto:hrpc@ietf.org>

[2] <https://www.irtf.org/mailman/listinfo/hrpc>

[3] <https://www.irtf.org/mail-archive/web/hrpc/current/index.html>

Authors' Addresses

Stephane Bortzmeyer
AFNIC

EMail: bortzmeyer+ietf@nic.fr

Niels ten Oever
ARTICLE 19

EMail: niels@article19.org

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: September 13, 2017

N. ten Oever
ARTICLE 19
G. Perez de Acha
Derechos Digitales
March 12, 2017

Freedom of Association on the Internet
draft-tenoever-hrpc-association-00

Abstract

This documents aims to document the relation between Internet protocols and the right to freedom of assembly and association. The Internet increasingly mediates our lives and thus the ability to exercise human rights. Since Internet protocols play a central role in the management, development and use of the Internet the relation between the two should be documented and adverse impacts on this human right should be mitigated. On the other hand there have also been methods of protest, a form of freedom of assembly, on the Internet that have been harmful to Internet connectivity and the Internet infrastructure, such as DDoS attacks. This document aims to document forms of protest, association and assembly that do not have a negative impact on the Internet infrastructure.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 13, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Vocabulary used	4
3. Research questions	5
4. Cases and examples	5
4.1. Communicating	5
4.1.1. Mailinglists	5
4.1.2. Multi party video conferencing and risks	5
4.1.3. Reaching out	6
4.2. Working together (peer production)	7
4.2.1. Version control	8
4.3. Grouping together (identities)	8
4.3.1. DNS	8
4.3.2. ISPs	8
5. Acknowledgements	8
6. Security Considerations	8
7. IANA Considerations	8
8. Research Group Information	8
9. References	9
9.1. Informative References	9
9.2. URIs	12
Authors' Addresses	12

1. Introduction

Freedom of assembly and freedom of association are two human rights that protect and enable collective action and expression [UDHR] [ICCPR]. This is important because causes and opinions take more force within a group of people that come together for the same means [Tocqueville].

The difference between the freedom of assembly and the freedom of associatiation is merely gradual one. An assembly is an intentional and temporary gathering of a collective in a private or public space for a specific purpose: demonstrations, inside meetings, strikes, processions, rallies or even sits-in [UNHRC]. The right to protest is one of the rights encompassed by freedom of assembly, but also

exercised along with freedom of expression and the right to hold an opinion. Nonetheless, protest unlike assembly, implies an element of dissent that can be exercised individually, where as assembly always has a collective component [ARTICLE19].

Association on the other hand has a more formal nature. It refers to a group of individuals or any legal entities brought together in order to collectively act, express, promote, pursue or defend a field of common interests [UNGA]. This means civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations or even online associations as the Internet has been instrumental, for instance, in 'facilitating active citizen participation in building democratic societies' [UNHRC].

In less democratic or authoritarian countries, online association and assembly has been crucial to mobilise groups and people, where physical gatherings have been impossible or dangerous [APC]. Both rights protect the right to join or leave a group of choice. Thus any collective, gathered for peaceful purposes, is protected by these rights.

In draft-irtf-hrhc-research the relationship between human rights and Internet protocols has been shown, and guidelines for considerations of human rights impact in protocol design have been provided.

Further research is needed to understand the exact shape, extend and form of Internet protocols on human rights. This document aims to break down the relationship between Internet protocols and the right to freedom of assembly and association.

The right to privacy and the right to freedom of expression are the most discussed human rights when it comes to the Internet. Still we must recognize that communities, collaboration and joint action lie at the heart of the Internet.

Even at a linguistical level, the words "networks" and "associations" are close synonyms. Both interconnected groups and association of persons depend on "links" and "relationships" [Swire]. One could even argue that as a whole, the networked internet constitutes a big collective, and thus an assembly and an association.

On the other hand, IETF itself, defined as a 'open global community' of network designers, operators, vendors, and researchers, is also protected by freedom of assembly and association [RFC3233]. Discussion, comments and consensus around RFCs are possible because of the collective expression that freedom of association and assembly allow. The very word "protocol" found its way into the language of

computer networking based on the need for collective agreement among network users [HafnerandLyon].

Throughout the world -from the Arab Spring to Latin American student movements- the Internet has also played a crucial role by providing a means for the fast dissemination of information that was otherwise mediated by broadcast media, or even forbidden by the government [Pensado]. According to Hussain and Howard the Internet helped to 'build solidarity networks and identification of collective identities and goals', facilitate protest, 'extend the range of local coverage to international broadcast networks' and as platform for contestation for the future of 'the future of civil society and information infrastructure' [HussainHoward].

However, some of these examples go beyond the use of Internet protocols and flow over into the applications layer or association in the offline world, whereas we'll focus on the Internet protocols and architecture.

This can be contrasted with the example of association on the infrastructure level (albeit one can contest whether this is 'peaceful') of Distributed Denial of Service Attacks (DDoS) in which the infrastructure of the Internet is used to express discontent with a specific cause [Abibil] [GreenMovement]. Unfortunately more of than not DDoS are used to 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. This is one of the reasons protocols should seek to mitigate DDoS attacks [BCP72].

This document will further seek to map how the internet architecture impacts freedom of association and assembly.

2. Vocabulary used

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

Censorship resistance Methods and measures to mitigate Internet censorship.

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]. Different types of connectivity are further specified in [RFC4084]. The combination of the end-to-end principle, interoperability, distributed architecture, resilience, reliability and robustness

are the enabling factors that result in connectivity to and on the Internet.

Decentralization Implementation or deployment of standards, protocols or systems without one single point of control.

Pseudonymity The ability to disguise one's identity online with a different name than the "real" one, allowing for diverse degrees of disguised identity and privacy. It is strengthened when less personal data can be linked to the pseudonym; when the same pseudonym is used less often and across fewer contexts; and when independently chosen pseudonyms are more frequently used for new actions (making them, from an observer's or attacker's perspective, unlinkable)." [RFC6973]

3. Research questions

How does the internet architecture enables and/or inhibits freedom of association and assembly.

4. Cases and examples

4.1. Communicating

4.1.1. Mailinglists

Since the beginning of the Internet mailing lists have been a key site of assembly and association [RFC0155] [RFC1211]. In fact, mailing lists were one of the Internet's first functionalities [HafnerandLyon].

In 1971, four years after the invention of email, the first mailing list was created to discuss the idea of using Arpanet for discussion. By this time, what had initially propelled the Arpanet project forward as a resource sharing platform was gradually replaced by the idea of a network as a means of bringing people together [Abbate]. More than 45 years after, mailing lists are pervasive and help communities to engage, have discussion, share information, ask questions, and build ties. Even as social media and discussion forums grew, mailing lists continue to be widely used [AckermannKargerZhang]. They are a crucial tool to organise groups and individuals around themes and causes [APC].

4.1.2. Multi party video conferencing and risks

'Beginning in early 2008, Iranian security entities have engaged in operations to identify and arrest administrators of "illicit" websites and social media groups. In recent years, the detention and

interrogation of members of online communities has been publicized by state media for propaganda purposes. However, the heavy-handedness of the government has also inadvertently created a situation where Iranian users are better positioned than others to avoid some surveillance activities - increasing the burden of finding pseudonymous users.' [AndersonGuarnieri].

'The WebRTC protocol was designed to enable responsive real-time communications over the Internet, and is instrumental in allowing streaming video and conferencing applications to run in the browser. In order to easily facilitate direct connections between computers (bypassing the need for a central server to act as a gatekeeper), WebRTC provides functionality to automatically collect the local and public IP addresses of Internet users (ICE or STUN). These functions do not require consent from the user, and can be instantiated by sites that a user visits without their awareness. The potential privacy implications of this aspect of WebRTC are well documented, and certain browsers have provided options to limit its behavior.' [AndersonGuarnieri].

'The disclosure of network addresses presents a specific risk to individuals that use privacy tools to conceal their real IP address to sites that they visit. Typically, when a user browses the Internet over a VPN, the only address that should be recorded by sites they visit would be that of the VPN provider itself. Using the WebRTC STUN function allows a site to additionally enumerate the addresses that are associated with the computer that the visitor is using - rather than those of intermediaries. This means that if a user is browsing the Internet on an ADSL connection over a VPN, a malicious site they visit could potentially surreptitiously record the home address of the user.' [AndersonGuarnieri].

4.1.3. Reaching out

In the 1990s as the internet became more and more commercial, spam came to be defined as irrelevant or unsolicited messages that were posted many times to multiple news groups or mailing lists [Marcus]. Here the question of consent is crucial. In the 2000s a large part of the discussion revolved around the fact that certain corporations -protected by the right to freedom of association- considered spam to be a form of "commercial speech", thus encompassed by free expression rights [Marcus]. Nonetheless, if we consider that the rights to assembly and association also mean that "no one may be compelled to belong to an association" [UDHR], spam infringes both rights if an opt-out mechanism is not provided and people are obliged to receive unwanted information, or be reached by people they do not know.

This leaves us with an interesting case: spam is currently handled mostly by mailproviders on behalf of the user, next to that countries are increasingly adopting opt-in regimes for mailinglists and commercial e-mail, with a possibility of serious fines in case of violation.

This protects the user from being confronted with unwanted messages, but it also makes it legally and technically very difficult to communicate a message to someone who did not explicitly ask for this. In the public offline spaces we regularly get exposed to flyers, invitations or demonstrations where our opinions get challenged, or we are invited to consider different viewpoints. There is no equivalent on the Internet with the technical and legal regime that currently operates in it. In other words, it is nearly impossible impossibility to provide information, in a proportionate manner, that someone is not explicitly expecting or asking for. This reinforces a concept that is regularly discussed on the application level, called 'filter bubble': "The proponents of personalization offer a vision of a custom-tailored world, every facet of which fits us perfectly. It's a cozy place, populated by our favorite people and things and ideas." [Pariser]. "The filter bubble's costs are both personal and cultural. There are direct consequences for those of us who use personalized filters. And then there are societal consequences, which emerge when masses of people begin to live a filter bubbled-life (...). Left to their own devices, personalization filters serve up a kind of invisible autopropaganda, indoctrinating us with our own ideas, amplifying our desire for things that are familiar and leaving us oblivious to the dangers lurking in the dark territory of the unknown." [Pariser]. It seems that the 'filter bubble'-effect can also be observed at the infrastructure level, which actually strengthens the impact and thus hampers the effect of collective expression.

There have been creative alternatives for this problem, such as when a message was distributed to the server logs of millions of servers through the 'masscan'-tool [Cox].

4.2. Working together (peer production)

At the organizational level, peer production is one of the most relevant innovations from Internet mediated social practices. According to Benkler, it implies 'open collaborative innovation and creation, performed by diverse, decentralized groups organized principally by neither price signals nor organizational hierarchy, harnessing heterogeneous motivations, and governed and managed based on principles other than the residual authority of ownership implemented through contract.' [Benkler].

4.2.1. Version control

Ever since developers needed to collaboratively write, maintain and discuss large code basis for the Internet there have been different approaches of doing so. One approach is discussing code through mailing lists, but this has proven to be hard in case of maintaining the most recent versions. There are many different versions and characteristics of version control systems.

Centralization - differences (and gradients) between free (as in beer) and free (as in freedom). Git vs Github.

4.3. Grouping together (identities)

Collective identities are also protected by freedom of association and assembly rights. According to Melucci these are 'shared definitions produced by several interacting individuals who are concerned with the orientation of their action as well as the field of opportunities and constraints in which their action takes place.' [Melucci]

4.3.1. DNS

Advantages and disadvantages

4.3.2. ISPs

Access, diversity and forced association

5. Acknowledgements

6. Security Considerations

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

7. IANA Considerations

This document has no actions for IANA.

8. Research Group Information

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

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

9. References

9.1. Informative References

- [Abbate] Janet Abbate, ., "Inventing the Internet", Cambridge: MIT Press (2013): 11. , 2013, <<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>>.
- [AckermannKargerZhang]
Ackerman, M., Karger, D., and A. Zhang, "Mailing Lists: Why Are They Still Here, What's Wrong With Them, and How Can We Fix Them?", Mit. edu (2017): 1. , 2017, <<https://people.csail.mit.edu/axz/papers/maillinglists.pdf>>.
- [AndersonGuarnieri]
Anderson, C. and C. Guarnieri, "Fictitious Profiles and webRTC's Privacy Leaks Used to Identify Iranian Activists", 2016, <<https://iranthreats.github.io/resources/webrtc-deanonymization/>>.
- [APC] Association for Progressive Communications and . Gayathry Venkiteswaran, "Freedom of assembly and association online in India, Malaysia and Pakistan. Trends, challenges and recommendations.", 2016, <https://www.apc.org/es/system/files/FOAA_online_IndiaMalaysiaPakistan.pdf>.
- [ARTICLE19]
ARTICLE 19, "The Right to Protest Principles: Background Paper", 2016, <<https://www.article19.org/data/files/medialibrary/38581/Protest-Background-paper-Final-April-2016.pdf> page 7>.
- [BCP72] IETF, "Guidelines for Writing RFC Text on Security Considerations", 2003, <<https://datatracker.ietf.org/doc/bcp72/>>.

- [Benkler] Benkler, Y., "Peer Production and Cooperation", 2009, <<http://www.benkler.org/Peer%20production%20and%20cooperation%2009.pdf>>.
- [Cox] Cox, J., "Chaos Communication Congress Hackers Invaded Millions of Servers With a Poem", 2016, <https://motherboard.vice.com/en_us/article/chaos-communication-congress-hackers-invaded-millions-of-servers-with-a-poem>.
- [GreenMovement] Villeneuve, N., "Iran DDoS", 2009, <<https://www.nartv.org/2009/06/16/iran-ddos/>>.
- [HafnerandLyon] Hafnerand, K. and M. Lyon, "Where Wizards Stay Up Late. The Origins of the Internet", First Touchstone Edition (1998): 93. , 1998, <<https://doi.org/10.1111/misr.12020>>.
- [HussainHoward] Hussain, M. and P. Howard, "What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring", Int Stud Rev (2013) 15 (1): 48-66. , 2013, <<https://doi.org/10.1111/misr.12020>>.
- [ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976, <<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>>.
- [Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and the first amendment", 1998, <<http://www.cardozoaelj.com/wp-content/uploads/2013/02/Marcus.pdf>>.
- [Melucci] Melucci, A., "The Process of Collective Identity", Temple University Press, Philadelphia , 1995.
- [Pariser] Pariser, E., "The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think", Penguin Books, London. , 2012.
- [Pensado] Jaime Pensado, ., "Student Activism. Utopian Dreams.", ReVista. Harvard Review of Latin America (2012). , 2012, <<http://revista.drclas.harvard.edu/book/student-activism>>.
- [RFC0155] North, J., "ARPA Network mailing lists", RFC 155, DOI 10.17487/RFC0155, May 1971, <<http://www.rfc-editor.org/info/rfc155>>.

- [RFC1211] Westine, A. and J. Postel, "Problems with the maintenance of large mailing lists", RFC 1211, DOI 10.17487/RFC1211, March 1991, <<http://www.rfc-editor.org/info/rfc1211>>.
- [RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <<http://www.rfc-editor.org/info/rfc1958>>.
- [RFC3233] Hoffman, P. and S. Bradner, "Defining the IETF", BCP 58, RFC 3233, DOI 10.17487/RFC3233, February 2002, <<http://www.rfc-editor.org/info/rfc3233>>.
- [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>>.
- [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>>.
- [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>>.
- [Swire] Peter Swire, ., "Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection", North Carolina Law Review (2012) 90 (1): 104. , 2012, <<https://ssrn.com/abstract=1989516> or <http://dx.doi.org/10.2139/ssrn.1989516>>.
- [Tocqueville] de Tocqueville, A., "Democracy in America", n.d., <http://classiques.uqac.ca/classiques/De_tocqueville_alexis/democracy_in_america_historical_critical_ed/democracy_in_america_vol_2.pdf p. 304>.
- [UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <<http://www.un.org/en/documents/udhr/>>.
- [UNGA] Hina Jilani, ., "Human rights defenders", A/59/401 , 2004, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/401 para. 46>.

[UNHRC] Maina Kiai, ., "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", A/HRC/20/27 , 2012, <http://freeassembly.net/wp-content/uploads/2013/10/A-HRC-20-27_en-annual-report-May-2012.pdf>.

9.2. URIs

[1] <mailto:hrpc@ietf.org>

Authors' Addresses

Niels ten Oever
ARTICLE 19

Email: niels@article19.org

Gisela Perez de Acha
Derechos Digitales

Email: gisela@derechosdigitales.org

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: November 30, 2018

N. ten Oever
University of Amsterdam
G. Perez de Acha
Derechos Digitales
May 29, 2018

Freedom of Association on the Internet
draft-tenoever-hrpc-association-05

Abstract

This document scopes the relation between Internet protocols and the right to freedom of assembly and association. Increasingly, the Internet mediates our lives, our relationships and our ability to exercise our human rights. The Internet provides a global public space, but one that is built predominantly on private infrastructure. Since Internet protocols play a central role in the management, development and use of the Internet, the relation between protocols and the aforementioned rights should be documented and any adverse impacts of this relation should be mitigated.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 30, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Vocabulary used	3
3. Research questions	5
4. Methodology	5
5. Literature Review	5
6. Cases and examples	7
6.1. Conversing	7
6.1.1. Mailing Lists	7
6.1.2. Multi-party video conferencing	8
6.1.3. Internet Relay Chat	8
6.2. Peer-to-peer networks and systems	9
6.2.1. Peer-to-peer system architectures	9
6.2.2. Version control	11
6.3. Grouping together (identities)	11
6.3.1. DNS	12
6.3.2. Autonomous Systems	12
7. Discussion: Protocols vs Platforms	13
8. Conclusions	14
9. Acknowledgements	15
10. Security Considerations	15
11. IANA Considerations	15
12. Research Group Information	15
13. References	15
13.1. Informative References	15
13.2. URIs	22
Authors' Addresses	22

1. Introduction

"We shape our tools and, thereafter, our tools shape us." 
 - John Culkin (1967)

The Internet is a technology which shapes modern information societies. The ordering that the Internet provides is socio-technical, in other words, the Internet infrastructure and architecture consists of social and technological arrangements [StarRuhleder]. This ordering is not always apparent because infrastructure also tends to hide itself in the societal woodwork [Mosco], or with [Weiser]: 'The most profound technologies are those that disappear'. Next to that infrastructure is often taken for

granted by those using it. Infrastructure therefore is mostly known by an epistemic community of experts [Haas] and only get recognized by the larger public when it fails. With the increasing societal use of the Internet the importance of the Internet is growing, and the decisions made about its infrastructure and architecture therefore also become more important. [RFC8280] established the relationship between human rights and Internet protocols, and in this document we seek to uncover the relation between two specific human rights and the Internet infrastructure and architecture.

The rights to freedom of assembly and association protect collective expression, in turn, systems and protocols that enable communal communication between people and servers allow these rights to prosper. The Internet itself was originally designed as "a medium of communication for machines that share resources with each other as equals" [NelsonHedlun], the Internet thus forms a basic infrastructure for the right freedom of assembly and association.

The manner in which communication is designed and implemented impacts the ways in which rights can be exercised. For instance a decentralized and resilient architecture that protects anonymity and privacy, offers a strong protection for the exercise of such freedoms in the online environment. At the same time, centralized solutions have enabled people to group together in recognizable places and helped the visibility of groups. In other words, different architectural designs come with different affordances, or characteristics. These characteristics should be taken into account at the time of design, and when designing, updating and maintaining other parts of the architecture and infrastructure.

This draft continues the work started in [RFC8280] by investigating the exact impact of Internet protocols on specific human rights, namely the right to freedom of assembly and association given their importance for the Internet, in order to mitigate (potential) negative impacts.

2. Vocabulary used

Architecture The design of a structure

Autonomous System (AS) Autonomous Systems are the unit of routing policy in the modern world of exterior routing [RFC1930].

Within the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet [RFC1930].

The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs [RFC1771].

Border Gateway Protocol (BGP) An inter-Autonomous System routing protocol [RFC4271].

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]. Different types of connectivity are further specified in [RFC4084]. The combination of the end-to-end principle, interoperability, distributed architecture, resilience, reliability and robustness are the enabling factors that result in connectivity to and on the Internet.

Decentralization Implementation or deployment of standards, protocols or systems without one single point of control.

Distributed system A system with multiple components that have their behavior co-ordinated via message passing. These components are usually spatially separated and communicate using a network, and may be managed by a single root of trust or authority. [Troncosoetal]

Infrastructure Underlying basis or structure for a functioning society, organization or community. Because infrastructure is a precondition for other activities it has a procedural, rather than static, nature due to its social and cultural embeddedness [PipekWulf] [Bloketal]. This means that infrastructure is always relational: infrastructure always develops in relation to something or someone [Bowker].

Internet The Network of networks, that consists of Autonomous Systems that are connected through the Internet Protocol (IP).

A persistent socio-technical system over which services are delivered [Mainwaringetal],

A techno-social assemblage of devices, users, sensors, networks, routers, governance, administrators, operators and protocols

An emergent-process-driven thing that is born from the collections of the ASes that happen to be gathered together at any given time. The fact that they tend to interact at any given time means it is

an emergent property that happens because they use the protocols defined at IETF.

3. Research questions

1. How does the internet architecture enable and/or inhibit freedom of association and assembly?
2. If the Internet is used to exercise the right to freedom of association, what are the implications for its architecture and infrastructure?

4. Methodology

In order to answer the research questions, first a number of cases have been collected to analyze where Internet infrastructure and protocols have either enabled or inhibited groups of people to collaborate, cooperate or communicate. This overview does not aim to cover all possible ways in which people can collectively organize or reach out to each other using Internet infrastructure and Internet protocols, but rather cover typical uses in an attempt at an ethnography of infrastructure [Star]. Subsequently we analyze the cases with the theoretical framework provided in the literature review and provide recommendations based on the findings.

5. Literature Review

The rights to freedom of assembly and association protects and enables collective action and expression [UDHR] [ICCPR]. These rights ensure everyone in a society has the opportunity to express the opinions they hold in common with others, which in turn facilitates dialogue among citizens, as well as with political leaders or governments [OSCE]. This is relevant because in the process of democratic deliberation, causes and opinions are more widely heard when a group of people come together behind the same cause or issue [Tocqueville].

In international law, the rights to freedom of assembly and association protect any collective, gathered either permanently or temporarily for "peaceful" purposes. It is important to underline the property of "freedom" because the right to freedom of association and assembly are voluntary and uncoerced: anyone can join or leave a group of choice, which in turn means one should not be forced to either join, stay or leave.

The difference between freedom of assembly and freedom of association is merely gradual one: the former tends to have an informal and ephemeral nature, whereas the latter refers to established and

permanent bodies with specific objectives. Nonetheless, one and the other are protected to the same degree.

An assembly is an intentional and temporary gathering of a collective in a private or public space for a specific purpose: demonstrations, indoor meetings, strikes, processions, rallies or even sits-in [UNHRC]. Association on the other hand has a more formal and established nature. It refers to a group of individuals or legal entities brought together in order to collectively act, express, pursue or defend a field of common interests [UNGA]. Within this category we can think about civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions or foundations.

The right to freedom of assembly and association is quintessential for the Internet, even if privacy and freedom of expression are the most discussed human rights when it comes to the online world. Online association and assembly are crucial to mobilise groups and people where physical gatherings have been impossible or dangerous [APC]. Throughout the world -from the Arab Spring to Latin American student movements and the #WomensMarch- the Internet has also played a crucial role by providing a means for the fast dissemination of information that was otherwise mediated by broadcast media, or even forbidden by the government [Pensado]. According to Hussain and Howard the Internet helped to "build solidarity networks and identification of collective identities and goals, extend the range of local coverage to international broadcast networks" and as platform for contestation for "the future of civil society and information infrastructure" [HussainHoward].

The IETF itself, defined as a 'open global community' of network designers, operators, vendors, and researchers, is also protected by freedom of assembly and association [RFC3233]. Discussions, comments and consensus around RFCs are possible because of the collective expression that freedom of association and assembly allow. The very word "protocol" found its way into the language of computer networking based on the need for collective agreement among network users [HafnerandLyon].

We are aware that some of these examples go beyond the use of Internet protocols and flow over into the applications layer or examples in the offline world whereas the purpose of the following document is to break down the relationship between Internet protocols and the right to freedom of assembly and association. Nonetheless, given that protocols are a part of the socio-technical ordering of reality, we do recognize that in some cases the line between them and applications, implementations, policies and offline realities are often blurred and hard (if not impossible) to differentiate.

6. Cases and examples

The Internet has become a central mediator for collective action and collaboration. This means the Internet has become a strong enabler of the rights to freedom of association and assembly.

Here we will discuss different cases to give an overview of how the Internet protocol and architecture facilitates the freedom of assembly and association.

6.1. Conversing

An interactive conversation between two or more people forms the basis for people to organize and associate. According to Anderson "the relationship between political conversation and engagement in the democratic process is strong." [Anderson]. By this definition, what defines the "political" is essentially assembly or association: a basis for the development of social cohesion in society.

6.1.1. Mailing Lists

Since the beginning of the Internet mailing lists have been a key site of assembly and association [RFC0155] [RFC1211]. In fact, mailing lists were one of the Internet's first functionalities [HafnerandLyon].

In 1971, four years after the invention of email, the first mailing list was created to talk about the idea of using Arpanet for discussion. What had initially propelled the Arpanet project forward as a resource sharing platform was gradually replaced by the idea of a network as a means of bringing people together [Abbate]. More than 45 years after, mailing lists are pervasive and help communities to engage, have discussion, share information, ask questions, and build ties. Even as social media and discussion forums grow, mailing lists continue to be widely used [AckermannKargerZhang]. They are a crucial tool to organise groups and individuals around themes and causes [APC].

Mailinglist are still in wide use, also in the IETF because they allow for easy association and allow people to subscribe (join) and unsubscribe (leave) as they please. They also allow for association of specific groups on closed lists. Finally the archival function allows for accountability. The downsides of mailinglists are similar to the ones generally associated with e-mail, except that end-to-end encryption such as OpenPGP [RFC4880] and S/MIME [RFC5751] is not possible because the final recipients are not known. There have been experimental solutions to address this issue such as Schleuder [Schleuder], but this has not been standardized or widely deployed.

6.1.2. Multi-party video conferencing

Multi-party video conferencing protocols such as WebRTC [RFC6176] [RFC7118] allow for robust, bandwidth-adaptive, wideband and super-wideband video and audio discussions in groups. 'The WebRTC protocol was designed to enable responsive real-time communications over the Internet, and is instrumental in allowing streaming video and conferencing applications to run in the browser. In order to easily facilitate direct connections between computers (bypassing the need for a central server to act as a gatekeeper), WebRTC provides functionality to automatically collect the local and public IP addresses of Internet users (ICE or STUN). These functions do not require consent from the user, and can be instantiated by sites that a user visits without their awareness. The potential privacy implications of this aspect of WebRTC are well documented, and certain browsers have provided options to limit its behavior.' [AndersonGuarnieri].

While facilitating freedom of assembly and association multi-party video conferencing tools might pose concrete risks for those who use them. On the one hand WebRTC is providing resilient channels of communications, but on the other hand it also exposes information about those who are using the tool which might lead to increased surveillance, identification and the consequences that might be derived from that. This is especially concerning because the usage of a VPN does not protect against the exposure of IP addresses [Crawford].

The risk of surveillance is also true in an offline space, but this is generally easy to analyze for the end-user. Security and privacy expectations of the end-user could be made more clear to the user (or improved) which would result in a more secure and/or private exercise of the right to freedom of assembly or association.

6.1.3. Internet Relay Chat

Internet Relay Chat (IRC) is an application layer protocol that enables communication in the form of text through a client/server networking model [RFC2810]. In other words, a chat service. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients.

For order to be kept within the IRC network, special classes of users become "operators" and are allowed to perform general maintenance functions on the network: basic network tasks such as disconnecting (temporary or permanently) and reconnecting servers as needed [RFC2812]. One of the most controversial power of operators is the

ability to remove a user from the connected network by 'force', i.e., operators are able to close the connection between any client and server [RFC2812].

IRC servers may deploy different policies for the ability of users to create their own channels or 'rooms', and for the delegation of 'operator'-rights in such a room. Some IRC servers support SSL/TLS connections for security purposes [RFC7194]. This helps stop the use of packet sniffer programs to obtain the passwords of IRC users, but has little use beyond this scope due to the public nature of IRC channels. TLS connections require both client and server support (that may require the user to install TLS binaries and IRC client specific patches or modules on their computers). Some networks also use TLS for server to server connections, and provide a special channel flag (such as +S) to only allow TLS-connected users on the channel, while disallowing operator identification in clear text, to better utilize the advantages that TLS provides.

6.2. Peer-to-peer networks and systems

At the organizational level, peer production is one of the most relevant innovations from Internet mediated social practices. According to [Benkler], it implies 'open collaborative innovation and creation, performed by diverse, decentralized groups organized principally by neither price signals nor organizational hierarchy, harnessing heterogeneous motivations, and governed and managed based on principles other than the residual authority of ownership implemented through contract.' [Benkler].

In his book *The Wealth of Networks*, Benkler significantly expands on his definition of commons-based peer production. According to Benkler, what distinguishes commons-based production is that it doesn't rely upon or propagate proprietary knowledge: "The inputs and outputs of the process are shared, freely or conditionally, in an institutional form that leaves them equally available for all to use as they choose at their individual discretion." [Benkler] To ensure that the knowledge generated is available for free use, commons-based projects are often shared under an open license.

6.2.1. Peer-to-peer system architectures

Peer-to-peer (P2P) is essentially a model of how people interact in real life because "we deal directly with one another whenever we wish to" [Vu]. Usually if we need something we ask our peers, who in turn refer us to other peers. In this sense, the ideal definition of P2P is that "nodes are able to directly exchange resources and services between themselves without the need for centralized servers" and where each participating node typically acts both as a server and as

a client [Vu]. In RFC 5694 P2P has been defined as peers or nodes that should be able to communicate directly between themselves without passing intermediaries, and that the system should be self-organizing and have decentralized control [RFC5694]. With this in mind, the ultimate model of P2P is a completely decentralized system, which is more resistant to speech regulation, immune to single points of failure and have a higher performance and scalability. Nonetheless, in practice some P2P systems are supported by centralized servers and some others have hybrid models where nodes are organized into two layers: the upper tier servers and the lower tier common nodes [Vu].

Since the ARPANET project, the original idea behind the Internet was conceived as what we would now call a peer-to-peer system [RFC0001]. Over time it has increasingly shifted towards a client/server model with "millions of consumer clients communicating with a relatively privileged set of servers" [NelsonHedlun].

Whether for resource sharing or data sharing, P2P systems are enabling freedom of assembly and association. Not only do they allow for effective dissemination of information, but because they leverage computing resources by diminishing costs allowing for the formation of open collectives at the network level. At the same time, in completely decentralized systems the nodes are autonomous and can join or leave the network as they want, which also makes the system unpredictable: a resource might be only sometimes available, and some other resources might be missing or incomplete [Vu]. Lack of information might in turn make association or assembly more difficult.

Additionally, when one architecturally assesses the role of P2P systems one can say that: "The main advantage of centralized P2P systems is that they are able to provide a quick and reliable resource locating. Their limitation, however, is that the scalability of the systems is affected by the use of servers. While decentralized P2P systems are better than centralized P2P systems in this aspect, they require a longer time in resource locating. As a result, hybrid P2P systems have been introduced to take advantage of both centralized and decentralized architectures. Basically, to maintain the scalability, similar to decentralized P2P systems, there are no servers in hybrid P2P systems. However, peer nodes that are more powerful than others can be selected to act as servers to serve others. These nodes are often called super peers. In this way, resource locating can be done by both decentralized search techniques and centralized search techniques (asking super peers), and hence the systems benefit from the search techniques of centralized P2P systems." [Vu]

6.2.2. Version control

Ever since developers needed to collaboratively write, maintain and discuss large code basis for the Internet there have been different approaches of doing so. One approach is discussing code through mailing lists, but this has proven to be hard in case of maintaining the most recent versions. There are many different versions and characteristics of version control systems.

A version control system is a piece of software that enables developers on a software team to work together and also archive a complete history of their work [Sink]. This allows teams to be working simultaneously on updated versions. According to Sink, broadly speaking, the history of version control tools can be divided into three generations. In the first one, concurrent development meant that only one person could be working on a file at a time. The second generation tools permit simultaneous modifications as long as users merge the current revisions into their work before they are allowed to commit. The third generation tools allow merge and commit to be separated [Sink].

Interestingly no version control system has ever been standardized in the IETF whereas the version control systems like Subversion and Git are widely used within the community, as well as by working groups. There has been a spirited discussion on whether working groups should use centralized forms of the Git protocol, such as those offered by Gitlab or Github. Proponents argue that this simplifies the workflow and allows for a more transparent workflow. Opponents argue that the reliance on a centralized service which is not merely using the Git protocol, but also uses non-standardized options like an Issue-Tracker, makes the process less transparent and reliant on a third party.

The IETF has not made a decision on the use of centralized instances of Git, such as Github or Gitlab. There have been two efforts to standardize the workflow vis a vis these third party services, but these haven't come to fruition: [Wugh] [GithubIETF].

6.3. Grouping together (identities)

Collective identities are also protected by freedom of association and assembly. According to Melucci these are 'shared definitions produced by several interacting individuals who are concerned with the orientation of their action as well as the field of opportunities and constraints in which their action takes place.' [Melucci] In this sense, assemblies and associations are an important base in the maintenance and development of culture, as well as preservation of minority identities [OSCE].

6.3.1. DNS

Domain names allow hosts to be identified by human parsable information. Whereas an IP address might not be the expression of an identity, a domain name can be, and often is. On the other hand the grouping of a certain identity under a specific domain or even a Top Level Domain brings about risks because connecting an identity to a hierarchically structured identifier systems creates a central attack surface. Some of these risks are the surveillance of the services running on the domain, domain based censorship [RFC7754], or impersonation of the domain through DNS cache poisoning. Several technologies have been developed in the IETF to mitigated these risks such as DNS over TLS [RFC7858], DNSSEC [RFC4033], and TLS [RFC5246]. These mitigations would, when implemented, not make censorship impossible, but rather make it visible. The use of a centralized authority always makes censorship through a registry or registrar possible, as well as by using a fake resolver or using proposed standards such as DNS Response Policy Zones [RPZ].

The structuring of DNS as a hierarchical authority structure also brings about a specific characteristic, namely the possibility of centralized policy making vis a vis the management and operation of Top Level Domains, which is what (in part) happens at ICANN. The impact of ICANN processes on human rights will not be discussed here.

6.3.2. Autonomous Systems

In order for edge-users to connect to the Internet, they need to be connected to an Automous System (AS) which, in turn, has peering or transit relations with other AS'es. This means that in the process of accessing the Internet, edge-users need to accept the policies and practices of the intermediary that provides them access to the other networks. In other words, for users to be able to join the 'network of networks', they always need to connect through an intermediary.

While accessing the Internet through an intermediary, the user is forced to accept the policies, practices and principles of a network. This could impede the rights of the edge-user, depending on the implemented policies and practices on the network and how (if at all) they are communicated to them. For example: filtering, blocking, extensive logging, slowing down connection or specific services, or other invasive practices that are not clearly communicated to the user.

In some cases it also means that there is no other way for the edge-user to connect to the network of networks, and is thus forced into accepting the policies of a specific network, because it is not trivial for an edge-user to operate an AS and engage in peering

relation with other ASes. This design, combined with the increased importance of the Internet to make use of basic services, forces edge-user to engage in association with a specific network eventhough the user does not consent to the policies of the network.

It can be noted also that there is no standard and deployed way for the edge-user to choose the routes her packets will go through. [RFC0791], section 3.1, standardized "source routing" but it was never deployed, mostly because of serious security issues. There is not even a way for the edge-user to know about the routes that packets have actually taken, and which ASes a packet has traversed. [RFC0791], section 3.1, standardized "record route" but it was never deployed. In practice, the user must accept policies of ASes he has no relationship with, and didn't choose. For instance, there is no way to direct the packets to avoid the Five Eyes, not even to know after the fact where the packet went. [FiveEyes] [SchengenRouting] (Traceroutes give you an idea but the path may change before and after the traceroute.)

7. Discussion: Protocols vs Platforms

The Internet is increasingly becoming a vehicle for commercial, proprietary, non-interoperable platforms. The Internet has always allowed for closed-off networks, but the current trend show the rise of a small number of very large non-interoperable platforms. Chat has moved from XMPP and IRC to Facebook Messenger, Whatsapp and WeChat and there has been a strong rise of social media networks with large numbers of users, such as Facebook, Twitter and Instagram. A similar trend can be found among e-mail providers, with the significant difference that e-mail is interoperable.

Often these non-interoperable platforms are built on open-protocols but do not allow for inter-operability or data-portability. In the case of these large platforms this leads to strong network externalities, also know as a network effect; because the users are there, users will be there. The use of social-media platforms has enabled groups to associate, but is has also led to a 'tactical freeze' because of the inability to change the platforms [Tufekci]. Whereas these networks are a ready-to-hand networked public sphere, they do not allow their inhabitants to change, or fully understand, their workings.

This potentially has a significant impact on the distributed nature of the Internet [RFC1287].

8. Conclusions

This document scopes the relation between Internet protocols and the right to freedom of assembly and association. For this reason, the current research started out with two main questions. First, how does the internet architecture enable and/or inhibit freedom of association and assembly? And secondly: if the Internet is used to exercise the right to freedom of association, what are the implications for its architecture and infrastructure?

Communities, collaboration and joint action lie at the heart of the Internet. Even at a linguistic level, the words "networks" and "associations" are close synonyms. Both interconnected groups and assemblies of people depend on "links" and "relationships" [Swire]. Taking legal definitions given in international human rights law jurisprudence, we could assert that the right to freedom of assembly and association protect collective expression. These rights protect any collective, gathered either permanently or temporarily for "peaceful" purposes. It is voluntary and uncoerced.

Regarding the first question, we argued that given that the Internet itself was originally designed as a medium of communication for machines that share resources with each other as equals, the Internet is one of the most basic infrastructures for the right to freedom of assembly and association. Since Internet protocols play a central role in the management, development and use of the Internet, we established the relation between some protocols and the right to freedom of assembly and association.

Regarding the second question, after reviewing protocols that allow mailing lists, to multi-party video conferencing, IRC, peer-to-peer architectures, version control or the functioning of autonomous systems, we can conclude that the way in which infrastructure is designed and implemented impacts the exercise of freedom of assembly and association. This is because different architectural designs come with different affordances, or characteristics. If a decentralized architecture protects anonymity and privacy, both freedoms in the online environment will be enabled. On the other hand, centralized solutions have allowed users to group together and visibilise groups. enabled people to group together in recognizable places and helped the visibility of groups.

Lastly, the increasing shift towards closed and non-interoperable platforms in chat and social media networks have a significant impact on the distributed and open nature of the Internet. Often these non-interoperable platforms are built on open-protocols but do not allow for inter-operability or data-portability. The use of social-media platforms has enabled groups to associate, but it has also rendered

users unable to change platforms, therefore leading to a sort of "forced association" that stirs faraway from freedom.

9. Acknowledgements

- Fred Baker, Jefsey, and Andrew Sullivan for work on Internet definitions
- Stephane Bortzmeyer for several concrete text suggestions that found their way in this document (such as the AS filtering example)
- Mark Perkins for finding a lot of typos
- the hrpc mailinglist at large for a very constructive discussion on a hard topic.

10. Security Considerations

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

11. IANA Considerations

This document has no actions for IANA.

12. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research Group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at <https://www.irtf.org/mailman/listinfo/hrpc> [2]

Archives of the list can be found at: <https://www.irtf.org/mail-archive/web/hrpc/current/index.html> [3]

13. References

13.1. Informative References

- [Abbate] Janet Abbate, ., "Inventing the Internet", Cambridge: MIT Press (2013): 11. , 2013,
<<https://mitpress.mit.edu/books/inventing-internet>>.

[AckermannKargerZhang]

Ackerman, M., Karger, D., and A. Zhang, "Mailing Lists: Why Are They Still Here, What's Wrong With Them, and How Can We Fix Them?", Mit. edu (2017): 1. , 2017, <<https://people.csail.mit.edu/axz/papers/maillinglists.pdf>>.

[Anderson]

Andersson, E., "The political voice of young citizens Educational conditions for political conversation - school and social media", Utbildning & Demokrati: Tidskrift foer Didaktik och Utbildningspolitik, Volume 21, Number 1, 2012, pp. 97-119(23) , 2012, <<http://www.ingentaconnect.com/content/doi/11026472/2012/00000021/00000001/art00006>>.

[AndersonGuarnieri]

Anderson, C. and C. Guarnieri, "Fictitious Profiles and WebRTC's Privacy Leaks Used to Identify Iranian Activists", 2016, <<https://iranthreats.github.io/resources/webrtc-deanonymization/>>.

[APC]

Association for Progressive Communications and . Gayathry Venkiteswaran, "Freedom of assembly and association online in India, Malaysia and Pakistan. Trends, challenges and recommendations.", 2016, <https://www.apc.org/es/system/files/FOAA_online_IndiaMalaysiaPakistan.pdf>.

[Benkler]

Benkler, Y., "Peer Production and Cooperation", 2009, <<http://www.benkler.org/Peer%20production%20and%20cooperation%2009.pdf>>.

[Bloketal]

Blok, A., Nakazora, M., and B. Winthereik, "Infrastructuring Environments", Science as Culture 25:1, 1-22. , 2016.

[Bowker]

Bowker, G., "Information mythology and infrastructure", In: L. Bud (Ed.), Information Acumen: The Understanding and use of Knowledge in Modern Business, Routledge, London, 1994, pp.231-247 , 1994.

[Crawford]

Crawford, D., "The WebRTC VPN "Bug" and How to Fix", 2015, <<https://www.bestvpn.com/the-webrtc-vpn-bug-and-how-to-fix-it/>>.

- [FiveEyes] Wikipedia, ., "Five Eyes", 2018, <https://en.wikipedia.org/wiki/Five_Eyes>.
- [GithubIETF] Thomson, M. and A. Atlas, "Using GitHub at the IETF", 2017.
- [Haas] Haas, P., "Introduction: epistemic communities and international policy coordination", International Organization, special issue: Knowledge, Power, and International Policy Coordination, Cambridge Journals. 46 (1): 1-35. , 1992.
- [HafnerandLyon] Hafnerand, K. and M. Lyon, "Where Wizards Stay Up Late. The Origins of the Internet", First Touchstone Edition (1998): 93. , 1998, <<https://doi.org/10.1111/misr.12020>>.
- [HussainHoward] Hussain, M. and P. Howard, "What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring", Int Stud Rev (2013) 15 (1): 48-66. , 2013, <<https://doi.org/10.1111/misr.12020>>.
- [ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1966, <<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>>.
- [Mainwaringetal] Mainwaring, S., Chang, M., and K. Anderson, "Infrastructures and Their Discontents: Implications for Ubicomp", DBLP Conference: Conference: UbiComp 2004: Ubiquitous Computing: 6th International Conference, Nottingham, UK, September 7-10, 2004. Proceedings , 2004, <<http://www.dourish.com/classes/readings/Mainwaring-Infrastructure.pdf>>.
- [Melucci] Melucci, A., "The Process of Collective Identity", Temple University Press, Philadelphia , 1995.
- [Mosco] Mosco, V., "The Digital Sublime: Myth, Power, and Cyberspace", 2005, <<https://mitpress.mit.edu/books/digital-sublime>>.

[NelsonHedlun]

Minar, N. and M. Hedlun, "A Network of Peers: Models Through the History of the Internet", Peer to Peer: Harnessing the Power of Disruptive Technologies, ed: Andy Oram , 2001, <http://library.uniteddiversity.coop/REconomy_Resource_Pack/More_Inspirational_Videos_and_Useful_Info/Peer_to_Peer-Harnessing_the_Power_of_Disruptive_Technologies.pdf>.

[OSCE]

OSCE Office for Democratic Institutions and Human Rights, "Guidelines on Freedom of Peaceful Assembly", page 24 , 2010, <<https://www.osce.org/odihr/73405?download=true>>.

[Pensado]

Jaime Pensado, ., "Student Activism. Utopian Dreams.", ReVista. Harvard Review of Latin America (2012). , 2012, <<http://revista.drclas.harvard.edu/book/student-activism>>.

[PipekWulf]

Pipek, V. and W. Wolf, "Infrastructuring: Towards an Integrated Perspective on the Design and Use of Information Technology", Journal of the Association for Information Systems (10) 5, pp. 306-332 , 2009.

[RFC0001]

Crocker, S., "Host Software", RFC 1, DOI 10.17487/RFC0001, April 1969, <<https://www.rfc-editor.org/info/rfc1>>.

[RFC0155]

North, J., "ARPA Network mailing lists", RFC 155, DOI 10.17487/RFC0155, May 1971, <<https://www.rfc-editor.org/info/rfc155>>.

[RFC0791]

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

[RFC1211]

Westine, A. and J. Postel, "Problems with the maintenance of large mailing lists", RFC 1211, DOI 10.17487/RFC1211, March 1991, <<https://www.rfc-editor.org/info/rfc1211>>.

[RFC1287]

Clark, D., Chapin, L., Cerf, V., Braden, R., and R. Hobby, "Towards the Future Internet Architecture", RFC 1287, DOI 10.17487/RFC1287, December 1991, <<https://www.rfc-editor.org/info/rfc1287>>.

[RFC1771]

Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, DOI 10.17487/RFC1771, March 1995, <<https://www.rfc-editor.org/info/rfc1771>>.

- [RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <<https://www.rfc-editor.org/info/rfc1930>>.
- [RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <<https://www.rfc-editor.org/info/rfc1958>>.
- [RFC2810] Kalt, C., "Internet Relay Chat: Architecture", RFC 2810, DOI 10.17487/RFC2810, April 2000, <<https://www.rfc-editor.org/info/rfc2810>>.
- [RFC2812] Kalt, C., "Internet Relay Chat: Client Protocol", RFC 2812, DOI 10.17487/RFC2812, April 2000, <<https://www.rfc-editor.org/info/rfc2812>>.
- [RFC3233] Hoffman, P. and S. Bradner, "Defining the IETF", BCP 58, RFC 3233, DOI 10.17487/RFC3233, February 2002, <<https://www.rfc-editor.org/info/rfc3233>>.
- [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, <<https://www.rfc-editor.org/info/rfc4033>>.
- [RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <<https://www.rfc-editor.org/info/rfc4084>>.
- [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <<https://www.rfc-editor.org/info/rfc4271>>.
- [RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <<https://www.rfc-editor.org/info/rfc4880>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <<https://www.rfc-editor.org/info/rfc5246>>.

- [RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, DOI 10.17487/RFC5694, November 2009, <<https://www.rfc-editor.org/info/rfc5694>>.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <<https://www.rfc-editor.org/info/rfc5751>>.
- [RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March 2011, <<https://www.rfc-editor.org/info/rfc6176>>.
- [RFC7118] Baz Castillo, I., Millan Villegas, J., and V. Pascual, "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)", RFC 7118, DOI 10.17487/RFC7118, January 2014, <<https://www.rfc-editor.org/info/rfc7118>>.
- [RFC7194] Hartmann, R., "Default Port for Internet Relay Chat (IRC) via TLS/SSL", RFC 7194, DOI 10.17487/RFC7194, August 2014, <<https://www.rfc-editor.org/info/rfc7194>>.
- [RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <<https://www.rfc-editor.org/info/rfc7754>>.
- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<https://www.rfc-editor.org/info/rfc7858>>.
- [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <<https://www.rfc-editor.org/info/rfc8280>>.
- [RPZ] Vixie, P. and V. Schyver, "DNS Response Policy Zones (RPZ)", 2017, <<https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00>>.
- [SchengenRouting] Wikipedia, ., "Schengen Routing", 2018, <https://en.wikipedia.org/wiki/Schengen_Routing>.

- [Schleuder] Nadir, "Schleuder - A gpg-enabled mailinglist with remailing-capabilities.", 2017, <<https://schleuder.nadir.org/>>.
- [Sink] Sink, E., "Version Control by Example", 2011, <<http://ericsink.com/vcbe/>>.
- [Star] Star, S., "The Ethnography of Infrastructure", American Behavioral Scientist, Volume 43 (3), 377-391. , 1999, <<http://journals.sagepub.com/doi/abs/10.1177/00027649921955326>>.
- [StarRuhleder] Star, S. and K. Ruhleder, "Steps toward an ecology of infrastructure: Design and access for large information spaces", Information Systems Research 7 (1) (1996) 111-134. , 1996.
- [Swire] Peter Swire, ., "Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection", North Carolina Law Review (2012) 90 (1): 104. , 2012, <<https://ssrn.com/abstract=1989516> or <http://dx.doi.org/10.2139/ssrn.1989516>>.
- [Tocqueville] de Tocqueville, A., "Democracy in America", 1840, <http://classiques.uqac.ca/classiques/De_tocqueville_alexis/democracy_in_america_historical_critical_ed/democracy_in_america_vol_2.pdf p. 304>.
- [Troncosoetal] Troncoso, C., Isaakdis, M., Danezis, G., and H. Halpin, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments", Proceedings on Privacy Enhancing Technologies ; 2017 (4):307-329 , 2017, <<https://www.petsymposium.org/2017/papers/issue4/paper87-2017-4-source.pdf>>.
- [Tufekci] Tufekci, Z., "Twitter and Tear Gas: The Power and Fragility of Networked Protest", 2017, <<https://www.twitterandteargas.org/>>.
- [UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <<http://www.un.org/en/documents/udhr/>>.

- [UNGA] Hina Jilani, ., "Human rights defenders", A/59/401 , 2004, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/401 para. 46>.
- [UNHRC] Maina Kiai, ., "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", A/HRC/20/27 , 2012, <http://freeassembly.net/wp-content/uploads/2013/10/A-HRC-20-27_en-annual-report-May-2012.pdf>.
- [Vu] Vu, Quang Hieu, ., Lupu, Mihai, ., and . Ooi, Beng Chin, "Peer-to-Peer Computing: Principles and Applications", 2010, <<https://www.springer.com/cn/book/9783642035135>>.
- [Weiser] Weiser, L., "The Computer for the 21st Century", Scientific American Ubicomp Paper after Sci Am editing , 1991, <<https://web.archive.org/web/20141022035044/http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>>.
- [Wugh] Nottingham, M., "Using Third Party Services for IETF Work", 2017, <<https://datatracker.ietf.org/doc/draft-nottingham-wugh-services/>>.

13.2. URIs

- [1] <mailto:hrpc@ietf.org>
- [2] <https://www.irtf.org/mailman/listinfo/hrpc>
- [3] <https://www.irtf.org/mail-archive/web/hrpc/current/index.html>

Authors' Addresses

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net

Gisela Perez de Acha
Derechos Digitales

EMail: gisela@derechosdigitales.org