Human Rights Protocol Considerations Research Group S. Bortzmeyer
Internet-Draft AFNIC
Intended status: Informational N. ten Oever
Expires: August 27, 2018 University of Amsterdam
February 23, 2018

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

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 27, 2018.

Copyright Notice

Table of Contents

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]

Official identity Government-issued identity, as written on ID cards and passports. We don't use terms like "real names" since a choosen pseudonym, for instance, is not less real than a identity given at birth.

Pseudonymity Derived from pseudonym, a persistent identity which is not the same as the entity's given (or official) name. For all IETF protocols, pseudonimity 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). Easy creation will allow to have one pseudonym per use, thus defeating linkability.

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 indivual from other individuals can be considered as personally identiable 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 requirments 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.

One of the reasons to switch identities might be to make the relationship between this identity and another one (for instance the official one) more difficult. The longer you use a pseudonym, the more clues you give to someone who tries to unveil pseudonymity.

4.3. Selective use

A user might want to retain their anonymity to certain actors / protocols, but identified to others. Also, she may also wish to be identified for some operations but not always.

4.4. User analysis

A user might want to understand which other actors might (potentially) have which level of information about them. This conflicts of course with privacy because the user has to reveal who he is. Example: if a domain name registry does not publish the name of a registrant, the registrant cannot check if the person who did the registration indicated the name of their client, or their own name.

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 explicitely 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
University of Amsterdam

EMail: mail@nielstenoever.net

Human Rights Protocol Considerations Research Group G. Grover
Internet-Draft Centre for Internet and Society
Updates: 8280 (if approved) N. ten Oever
Intended status: InformationalUniversity of Amsterdam & Texas A&M Univer
Expires: May 6, 2021 November 02, 2020

Guidelines for Human Rights Protocol and Architecture Considerations
draft-irtf-hrpc-guidelines-05

Abstract

This document sets guidelines for human rights considerations in networking protocols, similar to the work done on the guidelines for privacy considerations [RFC6973]. This is an updated version of the guidelines for human rights considerations in [RFC8280].

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 May 6, 2021.

Copyright Notice

Table of Contents

1. Introduction

This document 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 potential 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 Human Rights Protocol Considerations (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 concepts 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.

This document is a further iteration of the guidelines that can be found in [RFC8280]. The methods for conducting human rights reviews (Section 3.2), and guidelines for human rights considerations (Section 3.3) in this document are being tested for relevance, accuracy and validity.

2. Vocabulary used

3. Guidelines for developing human rights protocol considerations

3.1. Human rights threats

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

This document 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 security threat analysis. This method is a work in progress and by no means a perfect solution for assessing human rights risks in Internet protocols and systems. Certain specific human rights threats are indirectly considered in Internet protocols as part of the security considerations [BCP72], but privacy considerations [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 the moral and material interests resulting from any scientific, literary or artistic production of which [they are] the author (Art. 27), and privacy (Art. 12)." A partial catalog of human rights related to Information and Communications technologies, 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.

3.2. Conducting human rights reviews

Human rights reviews can take place in different parts of the development process of an Internet Draft. However, generally speaking, it is easier to influence the development of a technology at earlier stages than at later stages. This does not mean that reviews at last-call are not relevant, but they are less likely to result in significant changes in the reviewed document.

Methods for analyzing technology for specific human rights impacts are still quite nascent. Currently five methods have been explored by the Human Rights Review Team, often in conjunction with each other:

3.2.1. Analyzing drafts based on guidelines for human rights considerations model

This analysis of Internet-Drafts uses the model as described below. The outlined categories and questions are used to review an Internet Draft an generally the review is also presented in that order. The advantage of this is that it provides a known overview, and document authors can go back to this document as well as [RFC8280] to understand the background and the context.

3.2.2. Analyzing drafts based on their perceived or speculated impact

When reviewing an Internet-Draft, specific human rights impacts might become apparent by doing a close reading of the draft and seeking to understand how it might affect networks or society. While less structured than the straight use of the human rights considerations model, this analysis might lead to new speculative understandings between human rights and protocols.

3.2.3. Expert interviews

Interviews with document authors, active members of the Working Group, or experts in the field can help explore the characteristics of the protocol and their effects. There are two main advantages to this approach: one the one hand, it allows the reviewer to gain a deeper understanding of the (intended) workings of the protocol; on the other hand, it also allows for the reviewer to start a discussion with experts or even document authors about certain aspects, which might help gain the review gain traction when it is published.

3.2.4. Interviews with impacted persons and communities

Protocols impact users of the Internet. There it might help the review to understand how it impacts the people that use the protocol, and the people whose lives are impacted by the protocol. Since human rights should always be understood from the rights-holder, this approach will improve the understanding of the real world effects of the technology. At the same time, it can be hard to attribute specific changes to a particular protocol, this is of course even harder when a protocol has not been (widely) deployed.

3.2.5. Tracing impacts of implementations

When an Internet Draft is describing running code that has already been implemented, the code could be analyzed either in an experimental setting or on the Internet where its impact can be observed. Other than reviewing a draft, this allows the reviewer to understand how the document works in practice and potentially also what unknown or unexpected effects the technology might have.

3.3. 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 Standards 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 considerations section (following the example set in [RFC6973]).

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.

Also note that while the section uses the word, 'protocol', the principles identified in these questions may be applicable to other types of solutions (extensions to existing protocols, architecture for solutions to specific problems, etc.).

3.3.1. 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]. Using the end-to-end principle in protocol design is important to ensure the reliability and security of data transmissions.

Considering the fact that network quality and conditions vary across geography and time, it is also important to design protocols such that they are reliable even on low bandwidth and high latency connections. [add examples]

Example: Middleboxes (which can be Content Delivery Networks, Firewalls, NATs or other intermediary nodes that provide 'services' besides routing) serve many legitimate purposes. However, protocols relying on middleboxes can create potential for abuse, and intentional and unintentional censoring, thereby influencing individuals' ability to communicate online freely and privately.

Impacts:

- Right to freedom of expression

- Right to freedom of assembly and association

3.3.2. Privacy

Question(s): Did you have a look at the Guidelines in the Privacy Considerations for Internet Protocols [RFC6973] section 7? Does your protocol maintain the confidentiality of metadata? Could your

protocol counter traffic analysis? Does your protocol adhere to data minimization principles? Does your document identify potentially sensitive data logged 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

3.3.3. 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

3.3.4. 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: Security is not a single monolithic property of a protocol or system, but rather 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, security 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

3.3.5. 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 coded character set 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 IETF wants the Internet to be a global network of networks, the protocols should work with languages apart from English and character sets apart from 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

3.3.6. Censorship resistance

Question(s): Does your protocol make it apparent or transparent when access to a resource it 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? Does your protocol introduce new identifiers or reuse existing identifiers (e.g. MAC addresses) that might be associated with persons or content?

Explanation: Censorship resistance refers to the methods and measures to prevent Internet censorship. See [draft-irtf-pearg-censorship] for a survey of censorship techniques employed across the world, which lays out protocol properties that have been exploited to censor access to information.

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. 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. In 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

3.3.7. 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 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 you do without it)? Are you aware of any patents that would prevent your standard from being fully implemented [RFC8179] [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 an "open process", i.e. "any interested person can participate in the work, know what is being decided, and make his or her voice heard on the issue."

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 others 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 fair, reasonable and non-discriminatory terms.

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, that document describes a system that does not rely upon DPI, and is instead based on open IETF standards and open source applications.

Impacts:

- Right to freedom of expression

- Right to participate in cultural life, arts and science

3.3.8. 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 protocols must be allowed for, ranging from the simplest such as remote login up to the most complex such as commit protocols for distributed databases. [RFC1958].

Impacts:

- Right to freedom of expression

- Right to political participation

3.3.9. 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 - is an important feature for many end-users, as it allows them different degrees of disguised identity and privacy online.

Example: While 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 repercussions 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

3.3.10. 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: Sometimes in the design of protocols, websites, web technologies, or web tools, barriers are created that exclude people from using the Web. The Internet should be designed to work for all

people, whatever their hardware, software, language, culture, location, or physical or mental ability. When the Internet technologies meet this goal, it will be accessible to people with a diverse range of hearing, movement, sight, and cognitive ability. [W3CAccessibility]

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

3.3.11. Localization

Question(s): Does your protocol uphold the standards of internationalization? Have you 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

3.3.12. Decentralization

Question(s): Can your protocol be implemented without a 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 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 even if one or several nodes are disabled. With the commercialization of the Internet in the early 1990s, there has been a slow 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

3.3.13. Reliability

Question(s): Is your protocol fault tolerant? Does it downgrade 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' ability to gracefully downgrade 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 acknowledgment 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

3.3.14. 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 the sharing or express individuals' preferences to recipients or intermediaries with regard to the collection, use, or disclosure of their personal data? 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?

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 the use of more recent standards like DNS over TLS [RFC7858] or DNS over HTTPS [RFC8484], 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

3.3.15. 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 from on-path attackers. 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

3.3.16. 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.

At the same time, authentication should not be used as a way to prevent heterogeneity support, as is often done for vendor lock-in or digital rights management.

Example: Authentication of data is important to prevent vulnerabilities, and attacks from on-path attackers. 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.

Impacts:

- Right to privacy

- Right to freedom of expression

- Right to security

3.3.17. Adaptability

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

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

3.3.18. 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 choices 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. Other unexpected outcomes might not be technical, but rather architectural, social or economical.

Impacts:

- Freedom of expression

- Privacy

- Freedom of assembly and association

- Access to information

3.3.19. Anonymity

Question(s): Does your protocol make use of persistent identifiers? Can it be done without them? Did you have a look at the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.1 of that document?

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. Anonymity is an inherent part of the right to freedom of opinion and expression and the right to privacy. Avoid adding identifiers, options or configurations that create or might lead to patterns or regularities that are not explicitly required by the protocol.

If your protocol collects data and distributes it (see [RFC6235]), you should anonymize the data, but keep in mind that "anonymizing" data is notoriously hard. Do not think that just dropping the last byte of an IP address "anonymizes" data. If your protocol allows for identity management, there should be a clear barrier between the identities to ensure that they cannot (easily) be associated with each other.

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.

Example: 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].

Impacts:

- Right to non-discrimination

- Right to political participation

- Right to freedom of assembly and association

- Right to security

3.3.20. Remedy and Attribution

Question(s): Can your protocol facilitate a negatively impacted party’s right to legal remedy without disproportionately impacting other parties’ human rights, especially their right to privacy?

Explanation: Access to legal remedy is a human right that ensures that individuals whose rights have been violated can seek remedies

through a judicial authority. Attribution (i.e. mechanisms in protocols or architectures that are designed to make communications or artifacts attributable to a certain computer or individual) can be a part of this, since it may allow law enforcement agencies to identify a possible violator. However, attribution mechanisms may impede the exercise of the right to privacy. The Special Rapporteur for Freedom of Expression has also argued that anonymity is an inherent part of freedom of expression. [Kaye] Considering the adverse impact of attribution on the right to privacy and freedom of expression, attribution on an individual level may not be consistent with human rights. However, attribution to corporate entities, associations, and/or countries may not directly negatively impact human rights.

Impacts:

- Right to legal remedy

- Right to security

3.3.21. Misc. considerations

Question(s): Have you considered potential negative consequences (individual or societal) that your protocol or document might have?

Explanation: Publication of a particular RFC under a certain status has consequences. Publication as an Internet Standard as part of the Standards Track may signal to implementers that the specification has a certain level of maturity, operational experience, and consensus. Similarly, publication of a specification an experimental document as part of the non-standards track would signal to the community that the document "may be intended for eventual standardization but [may] not yet [be] ready" for wide deployment. The extent of the deployment, and consequently its overall impact on end-users, may depend on the document status presented in the RFC. See [BCP9] and updates to it for a fuller explanation.

4. Document Status

This RG document is currently documenting best practices and guidelines for human rights reviews of networking protocols and other Internet-Drafts and RFCs

5. Acknowledgements

Thanks to:

- Corinne Cath-Speth for work on [RFC8280].

- Theresa Engelhard, Joe Hall, Avri Doria and the hrpc list for reviews and suggestions.

- Individuals who conducted human rights reviews for their work and feedback: Amelia Andersdotter, Beatrice Martini, Karan Saini and Shivan Kaul Sahib.

6. Security Considerations

As this document 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 [2]

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

9. References

9.1. Informative References

[BCP72] IETF, "Guidelines for Writing RFC Text on Security Considerations", 2003, <https://datatracker.ietf.org/doc/bcp72/>.

[BCP9] Bradner, S. and IETF, "The Internet Standards Process -- Revision 3", 1996, <https://datatracker.ietf.org/doc/rfc2026/>.

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

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

[draft-irtf-pearg-censorship]
Hall, J., Aaron, M., Adams, S., Jones, B., and N. Feamster, "A Survey of Worldwide Censorship Techniques", 2020, <https://tools.ietf.org/html/draft-irtf-pearg-censorship>.

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

[geekfeminism]
Geek Feminism Wiki, "Pseudonymity", 2015, <http://geekfeminism.wikia.com/wiki/Pseudonymity>.

[Hill2014]
Hill, R., "Partial Catalog of Human Rights Related to ICT Activities", 2014, <http://www.apig.ch/UNIGE%20Catalog.pdf>.

[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>.

[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>.

[Kaye] Kaye, D., "The use of encryption and anonymity in digital communications", 2015, <https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>.

[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>.

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

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

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

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc2277>.

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

[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, <https://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, <https://www.rfc-editor.org/info/rfc3935>.

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

[RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <https://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, <https://www.rfc-editor.org/info/rfc4941>.

[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>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://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, <https://www.rfc-editor.org/info/rfc5646>.

[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, <https://www.rfc-editor.org/info/rfc6108>.

[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>.

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

[RFC6701] Farrel, A. and P. Resnick, "Sanctions Available for Application to Violators of IETF IPR Policy", RFC 6701, DOI 10.17487/RFC6701, August 2012, <https://www.rfc-editor.org/info/rfc6701>.

[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>.

[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, <https://www.rfc-editor.org/info/rfc7624>.

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

[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>.

[RFC8179] Bradner, S. and J. Contreras, "Intellectual Property Rights in IETF Technology", BCP 79, RFC 8179, DOI 10.17487/RFC8179, May 2017, <https://www.rfc-editor.org/info/rfc8179>.

[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>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[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.

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

[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>.

[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>.

[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>.

9.2. 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

Gurshabad Grover
Centre for Internet and Society

EMail: gurshabad@cis-india.org

Niels ten Oever
University of Amsterdam & Texas A&M University

EMail: mail@nielstenoever.net

Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 2, 2019

S. Sahib

August 01, 2018

New protocol elements for HTTP Status Code 451
draft-sahib-451-new-protocol-elements-03

Abstract

This document recommends additional protocol elements to Hypertext Transfer Protocol (HTTP) status code 451 (defined by RFC7725).

Discussion of this document was conducted on the Human Rights Protocol Considerations Research Group mailing list https://www.irtf.org/mailman/listinfo/hrpc [1], briefly on the HTTPBIS Working Group mailing list ietf-http-wg@w3.org [2] and on https://lists.ghserv.net/mailman/listinfo/statuscode451 [3].

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 February 2, 2019.

Table of Contents

1. Introduction

[RFC7725] was standardized by the IETF in February 2016. It defined HTTP status code 451 - to be used when "a server operator has received a legal demand to deny access to a resource or to a set of resources".

This document attempts to outline protocol recommendations that would help make the status code more useful to users.

2. New Protocol Elements

2.1. Blocking Authority

An HTTP response with status code 451 should include a "Link" HTTP header field [RFC8288] which has a "rel" parameter whose value is "blocking-authority", in addition to the "blocked-by" header specified in [RFC7725]. It's important to distinguish between the implementer of the block, and the authority that mandated the block in the first place [ERRATA_ID-5181]. This is because these two organizations might not be the same - a government (the blocking authority) could force an Internet Service Provider (the implementer of the block) to deny access to a certain resource. Both provide essential information about the legal block.

2.2. Geographical Scope of Block

HTTP status code 451 is increasingly being used to deny access to resources based on geographical location. The response should contain a provisional header named "geo-scope-block" that specifies the countries in which a resource is blocked. This scope should correspond to a comma-separated list of alpha-2 country codes defined in [ISO.3166-1]. The rationale for keeping the geographical scope to country-level granularity is that most blocks are mandated by national governments [IMPL_REPORT], [AUTOMATTIC_COUNTRY_BLOCK_LIST].

3. Security Considerations

This document does not add additional security considerations to [RFC7725].

4. IANA Considerations

The Link Relation Type Registry should be updated with the following entry:

- Relation Name: blocking-authority
- Description: Identifies the authority that has issued the block.
- Reference: this document

In addition, IANA should be updated with the following provisional header:

- Header field name: geo-scope-block
- Applicable protocol: http
- Status: provisional
- Specification document(s): this document

Acknowledgements

Thanks to Alp Toker, Niels ten Oever, Stephane Bortzmeyer, Corinne Cath, Christine Runnegar, and many others on the HRPC mailing list (linked above) for reviewing and brainstorming.

6. References

6.1. Normative References

[ERRATA_ID-5181]
Bortzmeyer, S., "[Technical Errata Reported] RFC7725 (5181)", 2017, <https://www.rfc-editor.org/errata/eid5181>.

[ISO.3166-1]
International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions - Part 1: Country code", ISO Standard 3166-1:1997 , 1997.

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

[RFC8288] Nottingham, M., "Web Linking", RFC 8288, DOI 10.17487/RFC8288, October 2017, <https://www.rfc-editor.org/info/rfc8288>.

6.2. Informative References

[AUTOMATTIC_COUNTRY_BLOCK_LIST]
"Automattic - Country Block List", 2018, <https://transparency.automattic.com/country-block-list/>.

[IMPL_REPORT]
Abraham, S., Canales, MP., Hall, J., Khrustaleva, O., ten Oever, N., Runnegar, C., and S. Sahib, "Implementation Report for HTTP Status Code 451", 2017, <https://tools.ietf.org/html/draft-451-imp-report-00>.

6.3. URIs

[1] https://www.irtf.org/mailman/listinfo/hrpc

[2] mailto:ietf-http-wg@w3.org

[3] https://lists.ghserv.net/mailman/listinfo/statuscode451

Author's Address

Shivan Kaul Sahib

EMail: shivankaulsahib@gmail.com

Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft University of Amsterdam
Intended status: Informational G. Perez de Acha
Expires: November 30, 2018 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.

Table of Contents

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 excercised. 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 visbility 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 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 delibration, 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 accountabilty. 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. One 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 excercise 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 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 clases 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 achitectures

Peer-to-peer (P2P) is esentially 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 unpredicable: 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 asseses 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 dividied 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. Acording 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, propietary, 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 at linguistical 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 visbility 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 is 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/mailinglists.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/doaj/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

Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft University of Amsterdam
Intended status: Informational A. Andersdotter
Expires: December 20, 2018 ARTICLE 19
June 18, 2018

On the Politics of Standards
draft-tenoever-hrpc-political-05

Abstract

The IETF cannot ordain which standards or protocols are to be used on network, but the standards developing process in the IETF has a normative effect. Among other things the standardisation work at the IETF has implications on what is perceived as technologically possible and useful where networking technologies are being deployed, and its standards output reflect was is considered by the technical community as feasible and good practice. Because mediates many aspects of modern life, and therefore contributes to the ordering of societies and communities, the consideration of the politics and (potential) impact of protocols should be part of the standardization and development process.

Table of Contents

1. Introduction

"Science and technology lie at the heart of social asymmetry. Thus technology both creates systems which close off other options and generate novel, unpredictable and indeed previously unthinkable, option. The game of technology is never finished, and its ramifications are endless.

- Michel Callon

The design of the Internet through protocols and standards is a technical issue with great political and economic impacts [RFC0613]. The early Internet community already realized that it needed to make decisions on political issues such as Intellectual Property, Internationalization [BramanI], diversity, access [RFC0101] privacy and security [RFC0049], and the military [RFC0164] [RFC0316], governmental [RFC0144] [RFC0286] [RFC0313] [RFC0542] [RFC0549] and non-governmental [RFC0196] uses, which has been clearly pointed out by Braman [BramanII].

Recently there has been an increased discussion on the relation between Internet protocols and human rights [RFC8280] which spurred the discussion on the political nature of standards. The network infrastructure is on the one hand designed, described, developed, standardized and implemented by the Internet community, but the Internet community and Internet users are also shaped by the affordances of the technology. Companies, citizens, governments, standards developing bodies, public opinion and public interest groups all play a part in these discussions. In this document we aim to outline different views on the relation between standards and politics and seek to answer the question whether standards are political, and if so, how.

2. Vocabulary Used

Politics (from Greek: Politika: Politika, definition "affairs of the commons") is the process of making decisions applying to all members of a diverse group with conflicting interests. More narrowly, it refers to achieving and exercising positions of governance or organized control over a community. Furthermore, politics is the study or practice of the distribution of power and resources within a given community as well as the interrelationship(s) between communities. (adapted from [HagueHarrop])

Affordances The possibilities that are provided to an actors through the ordering of an environment by a technology.

Protocols 'Protocols are rules governing communication between devices or applications, and the creation or manipulation of any logical or communicative artifacts concomitant with such communication.' [Sisson]

Standards 'An Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is

recognizably useful in some or all parts of the Internet.' [RFC2026]

3. Research Question

Are protocols political? If so, should the politics of protocols need to be taken into account in their development process?

4. Technology and Politics: a literature review

In 1993 the Computer Professionals for Social Responsibility stated that 'the Internet should meet public interest objectives', similarly [RFC3935] states that 'The Internet isn't value-neutral, and neither is the IETF.'. Ethics and the Internet was already a topic of an RFC by the IAB in 1989 [RFC1097]. Nonetheless there has been a recent uptick in discussions around the impact of Internet protocols on human rights [RFC8280] in the IETF and more general about the impact of technology on society in the public debate.

This document aims to provide an overview of the spectrum of different positions that have been observed in the IETF and IRTF community, during participatory observation, through 39 interviews with members of the community, the Human Rights Protocol Considerations Research Group mailinglist and during and after the Technical Plenary on Protocols and Human Rights during IETF98. Without judging them on their internal of external consistency they are represented here, where possible we sought to engage with academic literature on this topic.

4.1. Technology is value neutral

This position starts from the premise that the technical and political are differentiated fields and that technology is 'value free'. This is also put more explicitly by Carey: "electronics is neither the arrival of apocalypse nor the dispensation of grace. Technology is technology; it is a means for communication and transportation over space, and nothing more." [Carey]. In this view protocols only become political when it is actually being used by humans. So the technology itself is not political, the use of the technology is. This view sees technology as instrument; "technologies are 'tools' standing ready to serve the purposes of their users. Technology is deemed 'neutral,' without valuative content of its own.'" [Feenberg]. Feenberg continues: "technology is not inherently good or bad, and can be used to whatever political or social ends desired by the person or institution in control. Technology is a 'rational entity' and universally applicable. One may make exceptions on moral grounds, but one must also understand

that the "price for the achievement of environmental, ethical, or religious goals...is reduced efficiency." [Feenberg].

4.2. Some protocols are political some times

This stance is a pragmatic approach to the problem. It states that some protocols under certain conditions can themselves have a political dimension. This is different from the claim that a protocol might sometimes be used in a political way; that view is consistent with the idea of the technology being neutral (for the human action using the technology is where the politics lies). Instead, this position requires that each protocol and use be evaluated for its political dimension, in order to understand the extent to which it is political.

4.3. All protocols are political sometimes

While not an absolutist standpoint it recognizes that all design decisions are subject to the law of unintended consequences. The system consisting of the Internet and its users is vastly too complex to be predictable; it is chaotic in nature; its emergent properties cannot be predicted. This concept strongly hinges on the general purpose aspect of information technology and its malleability. Whereas not all (potential) behaviours, affordances and impacts of protocols can possible be predicted, on could at least consider the impact of proposed implementations.

4.4. The network has its own logic and values

While humans create technologies, this does not mean that they are forever under human control. A technology, once created, has its own logic that is independent of the human actors that either create or use the technology.

From this perspective, technologies can shape the world. As Martin Heidegger says, "The hydroelectric plant is not built into the Rhine River as was the old wooden bridge that joined bank with bank for hundreds of years. Rather the river is dammed up into the power plant. What the river is now, namely, a water power supplier, derives from out of the essence of the power station." [Heidegger] (p 16) The dam in the river changes the world in a way the bridge does not, because the dam alters the nature of the river.

In the same way -in another and more recent example- the very existence automobiles impose physical forms on the world different from those that come from the electric tram or the horse-cart. The logic of the automobile means speed and the rapid covering of distance, which encourages suburban development and a tendency toward

conurbation. But even if that did not happen, widespread automobile use requires paved roads, and parking lots and structures. These are pressures that come from the automotive technology itself, and would not arise without that technology.

In much same way, then, networking technology, such as protocols, creates its own demands. One of the most important conditions for protocol success is its incremental deployability [RFC5218]. This means that the network already contains constrains on what can be deployed into it. In this sense the network creates its own paths, but also has its own objective. According to this view the goal of the network is interconnection and connectivity; more connectivity is good for the network. Proponents of this positions also often describe the Internet as an organism with its own unique ecosystem.

In this position it is not necessarily clear where the 'social' ends and the 'technical' begins, and it could be argued that the distinction itself is a social construction [BijkerLaw] or that a real-life distinction between the two is hard to be made [Bloor].

4.5. Protocols are inherently political

This position argues the opposite of 'technological neutrality'. This position can be illustrated with Postman where he writes: 'the uses made of technology are largely determined by the structure of the technology itself' [Postman]. He states that the medium itself 'contains an ideological bias'. He continues to argue that technology is non-neutral:

(1) because of the symbolic forms in which information is encoded, different media have different intellectual and emotional biases; (2) because of the accessibility and speed of their information, different media have different political biases; (3) because of their physical form, different media have different sensory biases; (4) because of the conditions in which we attend to them, different media have different social biases; (5) because of their technical and economic structure, different media have different content biases.

Recent scholars of Internet infrastructure and governance have also pointed out that Internet processes and standards have become part and parcel of political processes and public policies. Several concrete examples are found within this approach, for instance, the IANA transition or global innovation policy [DeNardis]. The Raven process in which the IETF refused to standardize wiretapping -which resulted in [RFC2804]- was an instance where an international governance body took a position that was largely political, although driven by a technical argument. The process that led to [RFC6973] is similar: the Snowden disclosures which occured in the political

space, engendered the IETF to act. This is summarized in [Abbate] who says: "protocols are politics by other means", emphasizing the interests that are at play in the process of designing standards.

This position further holds that protocols can never be understood without their contextual embeddedness: protocols do not exist solely by themselves but always are to be understood in a more complex context - the stack, hardware, or nation-state interests and their impact on civil rights. Finally, this view is that that protocols are political because they affect or sometimes effect the socio-technical ordering of reality. The latter observation leads Winner to conclude that the reality of technological progress has too often been a scenario where the innovation has dictated change for society. Those who had the power to introduce a new technology also had the power to create a consumer class to use the technology 'with new practices, relationships, and identities supplanting the old, --and those who had the wherewithal to implement new technologies often molded society to match the needs of emerging technologies and organizations.' [Winner].

5. IETF: Protocols as Standards

In the previous section we gave an overview of the different existing positions of the impact of Internet protocols in the Internet community. In the following section we will consider the standards setting process and its consequences for the politics of protocols.

Standards enabling interoperating networks, what we think of today as the Internet, were created as open, formal and voluntary standards. A platform for internet standardisation, the Internet Engineering Task Force (IETF), was created in 1992 to enable the continuation of such standardisation work. The IETF has sought to make the standards process transparent (by ensuring everyone can access standards, mailing-lists and meetings), predictable (by having clear procedures and reviews) and of high quality (by having draft documents reviewed by members from its own epistemic community). This is all aimed at increasing the accountability of the process and the quality of the standard.

The IETF implements what has been referred to as an "informal ex ante disclosure policy" for patents [Contreras], which includes the possibility for participants to disclose the existence of a patent relevant for the standard, royalty-terms which would apply to the implementors of that standard should it enter into effect, as well as other licensing terms that may be interesting for implementors to know. The community ethos in the IETF seems to lead to 100% royalty-free disclosures of prior patents which is a record number, even among other comparable standard organisations [Contreras].

5.1. Competition and collaboration

Standards exist for nearly everything: processes, technologies, safety, hiring, elections, and training. Standards provide blue-prints for how to accomplish a particular task in a similar way for others that are trying to accomplish the same thing, while reducing overhead and inefficiencies. Although there are different types and configurations of standards, they all enhance competition by allowing different entities to work from a commonly accepted baseline.

On the first types of standards than can be found are "informal" ones -agreed upon normal ways of interacting within a specific community. For example, the process through which greetings to a new acquaintance are expressed through a bow, a handshake or a kiss. On the other hand "formal" standards, are normally codified in writing. The next subsection will ---

Within economy studies, _de facto_ standards arise in market situations where one entity is particularly dominant; downstream competitors are therefore tied to the dominant entity's technological solutions [Ahlborn]. Under EU anti-trust law, de facto standards have been found to restrict competition for downstream services in PC software products [CJEU2007], as well as downstream services dependent on health information [CJEU2004].

Even in international law, the World Trade Organisation (WTO) uses standards, although it recognises a difference between standards and technical regulations. The former are voluntary formal codes to which products or services may conform, while technical regulations are mandatory requirements to be fullfilled for a product to be accessible on one of the WTO country markets. These rules have implications for how nation states bounded by the WTO agreements can impose specific technical requirements on companies. Nonetheles, there are many standardisation groups that were originally launched by nation states or groups of nation states. ISO, BIS, CNIS, NIST, ABNT and ETSI are examples of institutions that are, wholly or partially, sponsored by public money in order to ensure smooth development of formal standards. Even if under WTO rules these organisations cannot create the equivalent of a technical regulation, they have important normative functions in their respective countries. No matter what form, all standards enhance competition and collaboration because they define a common approach to a problem. This potentially allows different instances to interoperate or be evaluated according to the same indicators.

The development of formal standards faces a number of economic and organisational challenges. Mainly, the cost and difficulty of organising many entities around a mutual goal, as well as the cost of

research and development leading up to a mutually beneficial technological platform. In addition, deciding what the mutual goal is can also be a problem. These challenges may be described as inter-organisational costs. Even after a goal is decided upon, coordination of multiple entities requires time and money. One needs communication platforms, processes and a commitment to mutual investment in a higher good. They are not simple tasks, and the more different communities are affected by a particular standardisation process, the more difficult the organisational challenges become.

5.2. IETF standards setting externalities

In spite of a strong community ethos and transparent procedures, the IETF is not immune to externalities.

5.2.1. Finance

Sponsorship to the IETF is varied, but is also of the nature that ongoing projects that are in the specific interest of one or some group of corporations may be given more funding than other projects (see [draft-finance-thoughts]). The IETF has faced three periods of decreased commitment from participants in funding its meetings in the past ten years, leading, naturally, to self-scrutiny, see for instance [IAOC69], [IAOC77], [IAOC99].

5.2.2. Interoperability and backward compatability

The need for interoperability, and backward compatability makes engineering work harder. And once a standard is designed, it does not automatically mean it will be broadly adopted at a fast pace. Examples of this are IPv6, DNSSEC, DKIM, etc. The need for interoperability means that a new protocol needs to take into account a much more diverse environment than early protocols, and also be amendable to different needs: protocols needs to relate and negotiate in a busy agora, as do the protocol developers. This means that some might get priority, whereas others get dropped.

5.2.3. Competition between layers

There is a competition between layers, and even contestation about what the borders of different layers are. This leads to competition between layers and different solutions for similar problems on different layers, which in its turn leads to further ossification, which leads to more contestation.

5.3. How voluntary are open standards?

Coordinating transnational stakeholders in a process of negotiation and agreement through the development of common rules is a form of global governance [Nadvi]. Standards are among the mechanisms by which this governance is achieved. Conformance to certain standards is often a basic condition of participation in international trade and communication, so there are strong economic and political incentives to conform, even in the absence of legal requirements [Russell]. [RogersEden] argue:

"As unequal participants compete to define standards, technological compromises emerge, which add complexity to standards. For instance, when working group participants propose competing solutions, it may be easier for them to agree on a standard that combines all the proposals rather than choosing any single proposal. This shifts the responsibility for selecting a solution onto those who implement the standard, which can lead to complex implementations that may not be interoperable. On its face this appears to be a failure of the standardization process, but this outcome may benefit certain participants-- for example, by allowing an implementer with large market share to establish a de facto standard within the scope of the documented standard."

6. The need for a positioning

It is indisputable that the Internet plays an increasingly important role in the lives of individuals. The community that produces standards for the Internet therefore also has an impact on society, which it itself has recognised in a number of previously adopted documents [RFC1958].

The IETF cannot ordain which standards are to be used on the networks, and it specifically does not determine the laws of regions or countries where networks are being used, but it does set open standards for interoperability on the Internet, and has done so since the inception of the Internet. Because a standard is the blue-print for how to accomplish a particular task in a similar way to others, the standards adopted have a normative effect. The standardisation work at the IETF will have implications on what is perceived as technologically possible and useful where networking technologies are being deployed, and its standards output reflect was is considered by the technical community as feasible and good practice.

This calls for providing a methodology in the IETF community to evaluate which routes forward should indeed be feasible, what constitutes the "good" in "good practice" and what trade-offs between different feasible features of technologies are useful and should

therefore be made possible. Such an analysis should take societal implication into account.

The risk of not doing this is threefold: (1) the IETF might make decisions which have a political impact that was not intended by the community, (2) other bodies or entities might make the decisions for the IETF because the IETF does not have an explicit stance, (3) other bodies that do take these issues into account might increase in importance to the detriment of the influence of the IETF.

This does not mean the IETF does not have a position on particular political issues. The policies for open and diverse participation [RFC7704], the anti-harassment policy [RFC7776], as well as the Guidelines for Privacy Considerations [RFC6973] are proof of this. Nonetheless, these are all examples of positions about the IETF's work processes or product. What is absent is a way for IETF participants to evaluate their role with respect to the wider implications of that IETF work.

7. Conclusion

Economics, competition, collaboration, openness, and political impact have been an inherent part of the work of the IETF since its early beginnings, by its nature as standards developing organization, through the contributions of the members of the Internet community, and because the ordering effect the Internet has on society. Whereas there might not be agreement in the Internet community on what the specific political nature is of technological development, it is undispited that standards and protocols are both product of a political process, and they can also be used for political means. Whereas there is no need for a unified philosophy of Internet protocols, it is in the benefit of the IETF, the Internet and arguably society at large to take this into account in the standards development process.

8. The way forward

There are instruments that can help the IETF develop an approach to address the politics of standards. Part of this can be found in [RFC8280] as well as the United National Guiding Principles for Business and Human Rights [UNGP]. But there is not a one-size-fits-all solution. The IETF is a particular organization, with a particular mandate, and even if a policy is in place, its success depends on the implementation of the policy by the community.

Since 'de facto standardization is reliant on market forces' [Hanseth] we need to live with the fact standards bodies have a political nature [Webster]. This does not need to be problematic as

long as there are sufficient accountability and transparency mechanisms in place. The importance of these mechanisms increases with the importance of the standards and their implementations. The complexity of the work inscribes a requirement of competence in the work in the IETF, which forms an inherent barrier for end-user involvement. Even though this might not be intentional, it is a result of the interplay between the characteristics of the epistemic community in the IETF and the nature of the standard setting process.

Instead of splitting hairs about whether 'standards are political' [Winner] [Woolgar] we argue that we need to look at the politics of individual standards and invite document authors and reviewers to take these dynamics into account.

9. Security Considerations

As this draft concerns a research document, there are no security considerations as described in [RFC3552], which does not mean that not addressing the issues brought up in this draft will not impact the security of end-users or operators.

10. IANA Considerations

This document has no actions for IANA.

11. Acknowledgements

Thanks to Andrew Sullivan, Brian Carpenter, Mark Perkins and all contributors and reviewers on the hrpc mailinglist. Special thanks to Gisela Perez de Acha for some thorough editing rounds.

12. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations 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]

13. References

13.1. Informative References

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

[Ahlborn] Ahlborn, C., Denicolo, V., Geradin, D., and A. Padilla, "Implications of the Proposed Framework and Antitrust Rules for Dynamically Competitive Industries", DG Comp's Discussion Paper on Article 82, DG COMP, European Commission , 2006, <http://curia.europa.eu/juris/liste.jsf?num=T-201/04>.

[BijkerLaw] Bijker, W. and J. Law, "Shaping Technology/ Building Society: Studies in Sociotechnical Change", Cambridge, MA: MIT Press , 1992.

[Bloor] Bloor, D., "Knowledge and Social Imagery", London: Routeledge & Kegan Paul , 1976.

[BramanI] Braman, S., "Internationalization of the Internet by design: The first decade", Global Media and Communication, Vol 8, Issue 1, pp. 27 - 45 , 2012, <http://dx.doi.org.proxy.uba.uva.nl:2048/10.1177%2F1742766511434731>.

[BramanII] Braman, S., "The Framing Years: Policy Fundamentals in the Internet Design Process, 1969-1979", The Information Society Vol. 27, Issue 5, 2011 , 2010, <http://dx.doi.org.proxy.uba.uva.nl:2048/10.1080/01972243.2011.607027>.

[Carey] Carey, J., "Communication As Culture", p. 139 , 1992.

[CJEU2004] Court of Justice of the European Union, ., "ECLI:EU:C:2004:257, C-418/01 IMS Health", Cambridge, UK: Cambridge University Press , 2004, <http://curia.europa.eu/juris/liste.jsf?num=C-418/01>.

[CJEU2007] Court of Justice of the European Union, ., "ECLI:EU:T:2007:289, T-201/04 Microsoft Corp.", Cambridge, UK: Cambridge University Press , 2007, <http://curia.europa.eu/juris/liste.jsf?num=T-201/04>.

[Contreras] Contreras, J., "Technical Standards and Ex Ante Disclosure: Results and Analysis of an Empirical Study", Jurimetrics: The Journal of Law, Science & Technology, vol. 53, p. 163-211 , 2013.

[DeNardis]
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>.

[draft-finance-thoughts]
Arkko, J., "Thoughts on IETF Finance Arrangements", 2017, <https://datatracker.ietf.org/doc/html/draft-arkko-ietf-finance-thoughts>.

[Feenberg]
Feenberg, A., "Critical Theory of Technology", p.5-6 , 1991.

[HagueHarrop]
Hague, R. and M. Harrop, "Comparative Government and Politics: An Introduction", Macmillan International Higher Education. pp. 1-. ISBN 978-1-137-31786-5. , 2013.

[Hanseth] Hanseth, O. and E. Monteiro, "Insribing Behaviour in Information Infrastructure Standards", Accounting, Management and Infomation Technology 7 (14) p.183-211 , 1997.

[Heidegger]
Heidegger, M., "The Question Concerning Technology and Other Essays", Garland: New York, 1977 , 1977, <http://ssbothwell.com/documents/ebooksclub.org__The_Question_Concerning_Technology_and_Other_Essays.pdf>.

[IAOC69] IAOC, ., "IAOC Report Chicago", 2007, <https://iaoc.ietf.org/documents/IAOC-Report-Chicago-69.pdf>.

[IAOC77] IAOC, ., "IAOC Report Anaheim", 2010, <https://iaoc.ietf.org/documents/IAOC-Report-Anaheim-77.pdf>.

[IAOC99] IAOC, ., "IAOC Report Prague", 2017, <https://iaoc.ietf.org/documents/IAOCReportinAdvanceofIETF99.pdf>.

[Nadvi] Nadvi, K. and F. Waeltring, "Making sense of global standards", In: H. Schmitz (Ed.), Local enterprises in the global economy (pp. 53-94). Cheltenham, UK: Edward Elgar. , 2004.

[Postman] Postman, N., "Technopoly: the Surrender of Culture to Technology", Vintage: New York. pp. 3-20. , 1992.

[RFC0049] Meyer, E., "Conversations with S. Crocker (UCLA)", RFC 49, DOI 10.17487/RFC0049, April 1970, <https://www.rfc-editor.org/info/rfc49>.

[RFC0101] Watson, R., "Notes on the Network Working Group meeting, Urbana, Illinois, February 17, 1971", RFC 101, DOI 10.17487/RFC0101, February 1971, <https://www.rfc-editor.org/info/rfc101>.

[RFC0144] Shoshani, A., "Data sharing on computer networks", RFC 144, DOI 10.17487/RFC0144, April 1971, <https://www.rfc-editor.org/info/rfc144>.

[RFC0164] Heafner, J., "Minutes of Network Working Group meeting, 5/16 through 5/19/71", RFC 164, DOI 10.17487/RFC0164, May 1971, <https://www.rfc-editor.org/info/rfc164>.

[RFC0196] Watson, R., "Mail Box Protocol", RFC 196, DOI 10.17487/RFC0196, July 1971, <https://www.rfc-editor.org/info/rfc196>.

[RFC0286] Forman, E., "Network Library Information System", RFC 286, DOI 10.17487/RFC0286, December 1971, <https://www.rfc-editor.org/info/rfc286>.

[RFC0313] O'Sullivan, T., "Computer based instruction", RFC 313, DOI 10.17487/RFC0313, March 1972, <https://www.rfc-editor.org/info/rfc313>.

[RFC0316] McKay, D. and A. Mullery, "ARPA Network Data Management Working Group", RFC 316, DOI 10.17487/RFC0316, February 1972, <https://www.rfc-editor.org/info/rfc316>.

[RFC0542] Neigus, N., "File Transfer Protocol", RFC 542, DOI 10.17487/RFC0542, August 1973, <https://www.rfc-editor.org/info/rfc542>.

[RFC0549] Michener, J., "Minutes of Network Graphics Group meeting, 15-17 July 1973", RFC 549, DOI 10.17487/RFC0549, July 1973, <https://www.rfc-editor.org/info/rfc549>.

[RFC0613] McKenzie, A., "Network connectivity: A response to RFC 603", RFC 613, DOI 10.17487/RFC0613, January 1974, <https://www.rfc-editor.org/info/rfc613>.

[RFC1097] Miller, B., "Telnet subliminal-message option", RFC 1097, DOI 10.17487/RFC1097, April 1989, <https://www.rfc-editor.org/info/rfc1097>.

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

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

[RFC2804] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, DOI 10.17487/RFC2804, May 2000, <https://www.rfc-editor.org/info/rfc2804>.

[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>.

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

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/info/rfc5218>.

[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>.

[RFC7704] Crocker, D. and N. Clark, "An IETF with Much Diversity and Professional Conduct", RFC 7704, DOI 10.17487/RFC7704, November 2015, <https://www.rfc-editor.org/info/rfc7704>.

[RFC7776] Resnick, P. and A. Farrel, "IETF Anti-Harassment Procedures", BCP 25, RFC 7776, DOI 10.17487/RFC7776, March 2016, <https://www.rfc-editor.org/info/rfc7776>.

[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>.

[RogersEden] Rogers, M. and G. Eden, "The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures", International Journal of Communication 11(2017), 802–823 , 2017, <http://ijoc.org/index.php/ijoc/article/view/5525/1941>.

[Russell] Russell, A., "Open standards and the digital age: History, ideology, and networks", Cambridge, UK: Cambridge University Press , 2014.

[Sisson] Sisson, D., "Standards and Protocols", 2000, <https://philosophe.com/design/standards/>.

[UNGP] Ruggie, J. and United Nations, "United Nations Guiding Principles for Business and Human Rights", 2011, <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[Webster] Webster, J., "Networks of Collaboration or Conflict? The Development of EDI", The social shaping of inter-organizational IT systems and data interchange, eds: I. McLougling & D. Mason, European Commission PICT/COST A4 , 1995.

[Winner] Winner, L., "Upon openig the black box and finding it empty: Social constructivism and the philosophy of technology", Science, Technology, and Human Values 18 (3) p. 362–378 , 1993.

[Woolgar] Woolgar, S., "Configuring the user: the case of usability trials", A sociology of monsters. Essays on power, technology and dominatior, ed: J. Law, Routeledge p. 57–102. , 1991.

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

Amelia Andersdotter
ARTICLE 19

EMail: amelia@article19.org