INTERNET-DRAFT N. Elkins
Intended Status: Informational EDCO
B. Shein
Software Tool and Die
V. Bertola
Open-Exchange

Expires: April 20, 2019 October 17, 2018

Human Rights Considerations of Internet Filtering
draft-elkins-hrpc-ifilter-00

Abstract

This document is a survey of the filtering of content. The focus is on the human rights involved as cited in the Universal Declaration of Human Rights" which is one of the foundational documents for HRPC. The recent years have seen an increase in content filtering for a variety of reasons including to further the aims of governments who wish to maintain their rule and suppress dissent but also to enforce cultural norms, human rights and compliance with the law. Filters also exist for security (botnets, malware etc.), user-defined policies (parental control, corporate blocking of social networks during work time, etc.), spam control, upload of copyrighted material and other reasons. This document is based on several real world considerations: the existence of national and regional sovereignty, Internet Service Providers (ISPs) and Content Distribution Networks (CDNs) that provide connectivity and content hosting services, Over-the-top (OTTs) and Content Delivery Platforms (CDPs) that play a disproportionate role in capturing the attention and "eyeballs" of many of the users of the Internet.

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

This document explores the use cases and history of filtering of content at a protocol and category level, grouping them by type of entity. The focus is on the human rights involved as cited in the Universal Declaration of Human Rights" [UDHR] which is one of the foundational documents for HRPC. However, any case of content blocking has an impact on online expression, thus the document tries to provide a complete picture of all the reasons and mechanisms that lead to the filtering and removal of content from the Internet.

The recent years have seen an increase in content filtering by for a variety of reasons. States, through different legal instruments and public authorities, require the blocking of Internet content with different aims; undemocratic governments may wish to maintain their rule and suppress dissent, but also democratic governments use blocking to enforce cultural norms, human rights and compliance with the law . Filters are also widely used by network operators and Internet access providers for security (stopping botnets, malware etc.), to implement user-defined policies (parental control, corporate blocking of social networks during work time, etc.), to reject spam and for other reasons.

Over-the-top (OTTs) [WikiOTT] and Content Delivery Platforms (CDPs) - providers like Facebook, Google (YouTube), and Twitter that distribute streaming media or other content and services as a standalone product directly over the Internet, bypassing telecommunications and connectivity providers - implement filters to prevent the upload of copyrighted material or other content that infringes their policies; in some countries, such filters are mandated by law. End users also want to apply content filters or content classification schemes at the edge of the network, for example, to protect underage users of the local network or to prevent the risk of reaching dangerous and inappropriate websites by error.

While filtering usually attracts the highest attention, there are other ways to discriminate content that could be employed, leading to similar results. For example, an access provider may isolate the traffic directed to a specific website or service and slow it down, or apply additional fees for it, up to the point where users desist trying to connect to that destination. Content tagging can also constitute a weaker content discrimination system; even if the content remains accessible, marking it as dangerous or unsafe with prominent advance warnings will discourage users from accessing it.

Some call all content filtering "censorship". For example, the Internet Draft [Censorship] defines blocking of content as: "Censorship is where an entity in a position of power - such as a government, organization, or individual - suppresses communication that it considers objectionable, harmful, sensitive, politically incorrect or inconvenient. (Although censors that engage in censorship must do so through legal, military, or other means, this document focuses largely on technical mechanisms used to achieve network censorship.)"

We find the use of the word "censorship" in this context to have purely negative connotations. That is, the implication of using the word "censorship" implies that filtering of content is always "bad" or as acting against important human rights. The reality of the situation is that filtering of content is done for many reasons, including several which may be regarded as "good": acting to preserve human rights either directly, when hateful and violent content is removed, or, in the case of security filters, indirectly, by providing safer Internet access that can encourage users to spend more time and energies online and enjoy all the deriving opportunities for education, free speech and assembly.

All in all, a balancing of rights is often at stake, and the right to free expression of a content creator is not the only right that has to be considered and protected. We thus feel that the entire subject needs a more nuanced and careful examination, trying to establish principles, guidelines and technical protocols that can increase transparency and user control over these practices, allowing users to distinguish between the bad and the good uses of content classification and filtering schemes.

2 Content Filtering by States and Public Authorities

States may filter content through several legal instruments and by order of different public authorities.

In democratic countries, cases of content blocking are usually defined by a law and justified by an appropriate balancing of rights (see section 2.2) and needs/benefits. Depending on the country, the law may delegate to a specific public authority - either independent, or part of the government - the power to order blocking of websites and other content, or such power may be deferred to court orders following due legal process. In authoritarian countries, such legal basis and processes are often missing, and the blocking is more focused on protecting the authority of the ruler (see section 2.1).

In technical terms, the filtering can either be applied at the IP address level, via firewall rules or routing alterations, or at the DNS level, by altering the results of the queries for the blocked names. The latter method is more precise, avoiding to block all other websites and services hosted on the same IP address, but is also easier to circumvent for end users; thus, democratic countries usually prefer the latter method while undemocratic ones generally prefer the former.

The procedure to apply the filters usually involves the appropriate public authority sending a list of the blocked IP addresses and/or DNS names to all the country’s Internet access providers, requiring them to implement it on their routers and/or DNS resolvers. Providers not complying with these requests usually are subject to fines, to the cancellation of their license to operate (in countries where such license exists) or even to the penal prosecution of their legally responsible managers.

2.1 Filtering to Prevent Freedom of Assembly or Information

What is sometimes informally called "censorship", has to do with the action of some governments to block websites that promote dissent and counter-information and organize protest actions and assemblies to contest the government, or even platforms such as Facebook or Twitter which might enable dissidents to organize protests.

Other filtering is done to suppress knowledge of people who participated in protest movements being harassed, jailed or even killed. Some governments actually shut down the Internet altogether to prevent any witnesses to unfortunate activities.

These activities may all be regarded as acting against basic human rights in [UDHR].

2.2 Filtering to Enforce Cultural Norms

Some filtering is done via legislation to enforce cultural norms, such as blocking sites which promote totalitarian and violent ideologies or falsify history and news in ways that attack and endanger certain parts of society.

For example, in several countries the advocacy of totalitarian regimes such as nazi-fascism and communism, or of racist ideas and practices against religious or ethnic minorities (Holocaust denial, racism against people of African origin, etc.), is forbidden by law. While websites located inside the country can be physically taken down, the groups promoting these ideas often use anonymous hosting services in foreign countries, thus making blocking the access at the Internet provider level the only instrument available to these countries to enforce these laws.

In the general balancing of rights, this type of content - which may be seen as disinformation, and is generally used to promote undemocratic practices and discrimination against specific minorities and ethnic groups - is often considered extremely harmful to the safety and rights of the affected minorities and to democracy and public order in general, up to the point of overcoming the free speech rights of the content authors.

This kind of rights balancing also depends on cultural norms, with countries such as the United States giving priority to the free speech rights even of hateful authors, and countries in Europe and Asia giving priority to the general safety and social peace. Thus, the related filtering practices have to be applied by country, depending on the nationality of the end user and on the applicability of jurisdiction.

2.3 Filtering to Prevent Violence

As an extension of the previous case, filtering often also applies to content inciting violence and promoting terrorism, or making violence easier. Its objective is to protect the right to safety of the general population.

The EU wishes to fine Facebook, Google, etc. for problematic content. [BBCTECH] reads in part:

"If authorities flag content that incites and advocates extremism, the content must be removed from the web within an hour, the proposal from the EU's lead civil servant states. Net firms that fail to comply would face fines of up to 4% of their annual global turnover."

In the United States, a federal court has issued a temporary injunction against publishing plans for 3-d printed guns on the Internet.

2.4 Child Pornography

Another type of content which is often blocked is child pornography, as a way to discourage the exploitation of children for sexual reasons and protect their safety.

[Child-Porn] A number of countries will obtain the IP addresses of visitors to child pornography sites. They will attempt to tie these IP addresses to actual human beings so that they can be prosecuted.

2.5 Unauthorized Gambling and Illegal E-Commerce

In most countries, certain services are regulated and thus a license, often connected to the payment of specific taxes and fees, is required before being allowed to offer them online. While there may also be an economic motivation to this, such regulation is generally justified as protecting the safety and health of the population.

Among the most commonly regulated businesses are:

- Gambling
- Weapons
- Medical products and drugs requiring a doctor’s prescription
- Alcohol
- Cigarettes and tobacco

Some countries - for example Italy [ITALY-REG] - use content filtering to prevent access to websites offering these products for sale without meeting the country’s regulation and/or without having paid the appropriate taxes and fees

2.6 User Generated Content (UGC)

Legislation to attempt to ensure that User Generated Content (UGC) does not violate copyright laws has been proposed. [EUCOPY]

The summary is:

" Tech giants must pay for work of artists and journalists which they use

Small and micro platforms excluded from directive’s scope

Hyperlinks, "accompanied by "individual words" can be shared freely

Journalists must get a share of any copyright-related remuneration obtained by their publishing house"

3 Content Filtering by Internet Service Providers

Internet Service Providers (ISPs) provide access to the Internet to the general public. As such, they are usually required to apply any State-mandated filters, depending on the applicable jurisdiction, as described in section 2.

However, there are additional cases in which ISPs implement filtering, or weaker content discrimination methods, on their own - they will be described in this section.

3.1 Filtering for Network and Computer Security

Most of the common threats to the security of the Internet, both in terms of network security and of security of the end users and of their devices, are based on connections to unsafe websites and services - either services that have been designed for malicious purposes since the beginning, or legitimate services that have been cracked and infected with malicious software.

For example, phishing relies on leading the user's browser to a forgery of the website of one of the user's suppliers, like his bank or her utility provider. Malware, such as ransomware and viruses, is commonly spread by connecting the user's browser to an infected website that downloads the executable to his device and launches it. Botnets rely on stable connections between the clients on user devices (often millions of them) and one or more "command and control" hosts which move over time.

To counter these attacks and protect their users and their network, ISPs often acquire timely lists of malicious hosts from specialized providers and make them inaccessible by filtering them at the connection level, either by IP address or by DNS name.

This practice is becoming even more common and more useful as the so-called Internet of Things (IoT) gains adoption. IoT devices usually are strongly automated but have very little computing power, security features and update capabilities, making them very vulnerable to exploits and takeovers. Thus, protecting the home network rather than the individual device becomes the most viable solution for the security of the Internet.

3.2 Filtering on Behalf of the User

In some cases, the end users actually desire that some content is filtered out and made inaccessible, so that they cannot reach it even by mistake. Three common cases are:

-Security filters: The user explicitly asks the ISP to filter out malicious websites, as per the previous section.

-Parental control filters: From [UK-Controls] The user asks the ISP to block content which is not deemed safe for children. This block is usually customizable by each user, depending on their own desires, and is requested by families with children accessing the Internet from their home network. In some countries, the provision of this service by the ISPs is either mandated by law or required by industry self-regulation efforts.

-Productivity filters: The user - typically a corporate network administrator - asks the ISP to block content which is inappropriate or disallowed on the workplace, as it would endanger the corporate network or reduce productivity. This content usually includes social networks, sports and leisure websites, etc.

These filters can be provided for free, included in the Internet access service, or can constitute a specific additional service requiring opt-in and the payment of an additional fee. Services of this type are commonly available in several European countries, often with millions of customers.

3.3 Filtering for Commercial Reasons

Some ISPs provide limited Internet access services that only allow access to specific types of applications (instant messaging, for example) or do not include access to specific types of applications (video streaming, for example). In these cases, connections to the disallowed content are blocked or slowed down significantly. This kind of filtering could also depend on specific partnerships - for example, an ISP may encourage its users to use a specific search engine by slowing down the connections to the other ones, in exchange for monetary compensation by the preferred search engine.

Due to concerns over the market and competition impact of these practices, including potential limitations of user rights, they have been made illegal in some countries, upholding the so-called "network neutrality" principle.

4 Content Filtering by Platforms Providing Content and Services

In addition to filters at the edge of the Internet, enforced by ISPs either on behalf of the State or on their own, those that manage the content and its delivery inside the network filter content as well. Again, this may happen because of their decisions, or because these companies are incorporated to do business under the laws of one or more nation-states, and therefore are subject to the regulations of such nation-states.

This kind of filtering happens under several forms. For over-the-top and content delivery platforms (OTTs/CDPs), content may be examined and blocked, often automatically, when the user uploads it onto the platform, or may be verified and removed following a request by other users or after a court order. In some cases, for example in search engine results, the content will not be blocked, but will be marked as unsafe with a prominent warning discouraging the user to proceed with the connection, or will not be shown unless the user disables the default "safe" mode.

Many of these platforms also employ policies that lead to the exclusion of a user from the platform after a certain number of breaches to acceptable content guidelines, thus silencing the user permanently (though users may try to open a new account, but losing all their existing followers and connections).

Content Delivery Networks (CDNs) and hosting providers also have the option of taking websites down entirely by shutting down their web service (see section 4.4 for an example). Similarly, domain name registries and registrars may make content temporarily inaccessible by discontinuing the domain name registration for the hostname used in URLs, though, differently from CDNs and OTTs, they cannot actually remove the content from the Internet.

While some of these filters depend on applicable laws, in most cases the content guidelines are self-imposed, and may err on the side of content restrictions to reduce the legal risk for the platform, at the cost of reducing the user’s chances to speak. In some cases these filters are managed by algorithms and artificial intelligence applications, making it hard for the user to even understand why the content has been blocked; often, no explanation and appeal mechanism is provided, or the appeal is untimely and ineffective.

Even when laws apply, given the global nature of these platforms, the applicable laws are often not those of the user’s own country, and it is almost impossible for the user to exert any legal rights or request due judiciary process.

Additionally, the more the specific service is globally consolidated in the hands of a few big competing players and the more these filters become impactful; particularly in the case of OTT social networks, the termination of an account often cannot be adequately replaced by a new account on any competing service or even on the same one.

Some examples of similar situations follow.

4.1 Enforcing Cultural Norms

The article from the Guardian [FBNorms] expresses the thoughts of the authors so well that we will be citing a lengthy passage.

From [FBNorms]:

"Facebook allows people to live-stream their suicide attempts "as long as they are engaging with viewers" but will remove footage "once there’s no longer an opportunity to help the person". Pledges to kill oneself through hashtags or emoticons or those that specify a fixed date "more than five days" in the future shouldn't be treated as a high priority.

These are tiny snippets from a cache of training materials that Facebook content moderators need to absorb, in just two weeks, before policing the world's largest social network.

The guidelines also require moderators to learn the names and faces of more than 600 terrorist leaders, decide when a beheading video is newsworthy or celebratory, and allow Holocaust denial in all but four of the 16 countries where it's illegal - those where Facebook risks being sued or blocked for flouting local law.

The documents detail what is and is not permitted on the platform, covering graphic violence, bullying, hate speech, sexual content, terrorism and self-harm. For the first time the public has a glimpse of the thought process behind some of the company's editorial judgements that go beyond the vague wording of its community standards or statements made in the wake of a live-streamed murder."

The article goes on to posit that this may be the "most important editorial guide sheet the world has ever created".

This use case brings up an issue which we may wish to consider. That is, there is no reason that Facebook, as a private company, needs to share with anyone what its methodology is for filtering. However, considering the enormous impact of Facebook, it is in the public interest to know the methodology. In short, Facebook may be considered a public utility.

4.2 Blocking Extremist Activity

From [BBCTECH], some of the content providers on the Internet are acting to censor content pertaining to potential extremist activity

"In 2017, Google said it would dedicate more than 10,000 staff to rooting out violent extremist content on YouTube

YouTube said staff had viewed nearly two million videos for violent extremism from June to December 2017

YouTube said more than 98% of such material was flagged automatically, with more than 50% of the videos removed having fewer than 10 views

Industry members have worked together since 2015 to create a database of "digital fingerprints" of previously identified content to better detect extremist material. As of December 2017, it contained more than 40,000 such "hashes"

In 2017, Facebook claimed that 99% of all Islamic State and al Qaeda-related content was removed before users had flagged it. The social network said that 83% of the remaining content was identified and removed within an hour

Between August 2015 and December 2017, Twitter said that it had suspended more than 1.2 million accounts in its fight to stop the spread of extremist propaganda. It said that 93% were flagged by internal tools, with 74% suspended before their first tweet."

4.3 Blocking Activity Inciting Violence

[Myanmar] The United Nations report on the genocide of Rohingya muslims ties it to posts on Facebook. Apparently, the Facebook content provider had very few people who could read Burmese. So, posts were not reviewed. The posts by the Myanmar military, intended to incite violence, indeed did so. There was wholesale killing of Rohingya muslims. Facebook is now censoring such posts and has hired many Burmese speakers.

[DailyStormer] In August 2017 Cloudflare, one of the leading global CDNs, terminated the account of the Daily Stormer, a website advocating white supremacy and antisemitism, thus removing the website from the Internet. At the same time, several domain name registrars (GoDaddy, Tucows, Namecheap) discontinued the domain names used by the website. In the end, the website became accessible again by finding registries, registrars and hosters that would accept it, but in practice it was made almost unavailable for several weeks.

4.4 Copyright Protection

Another reason for content filtering by OTTs, CDNs and hosting services is copyright protection.

This has become a particularly active area since the EU adopted its digital copyright rules negotiating position (i.e., still in early stages) on 2018-09-12. Such rules will require all online platforms to implement automated content control at upload and screen the content for copyrighted material. [EU-DIGCOPY]

We may wish to study how the music industry has evolved copyright protection over the past 100+ years in the US and elsewhere.

In brief (US) they rely on designated third-party agencies (such as BMI, ASCAP, Harry J Fox) to provide licensing and collect royalties and distribute those back to copyright owners. Statutory fees were set by the US congress. Private agreements are also possible, and common, of course.

The music industry has developed a sophisticated ecosystem and rather than rely first on threats of criminal prosecution (which is possible in extreme cases) instead tries to convert as much of the problem as possible into civil claims (you used my work, you owe me money!).

This is in stark contrast to the EU directive which approaches the problem via fines etc. and seems to create none of that infrastructure.

4.5 Filtering for Network and Computer Security

Like ISPs, OTTs and CDNs also try to keep the network secure by making malicious or infected websites inaccessible. Search engines will mark results as unsafe; online platforms will disable links; hosting services and CDNs will terminate the web service.

Some of the considerations in section 3.1 also apply here. However, effective filtering measures at the Internet access point fully protect the end user. To obtain the same effectiveness by acting at the core of the network, all the OTTs, hosting services and CDNs of the planet should be effective at taking down malicious content in a timely manner. Currently, this effectiveness varies; even a few "rogue" players being uncooperative to abuse and security takedown requests are enough to provide safe havens for attackers.

4.6 Content Filtering by End-Users

Finally, the users themselves may want to block or mark content for several reasons. The content filtering types and purposes are the same described in section 3.2, but rather than relying on the ISP's infrastructure, they deploy appropriate software on their devices. This also includes user-controlled content classification mechanisms that avoid blocking content entirely, but still allow end users to preselect what they want to see or to miss on the Internet.

5 Security Considerations

No new security vulnerabilities are introduced as a result of this document.

6 IANA Considerations

No IANA actions are requested by this document.

6 References

6.1 Normative References

6.2 Informative References

[Censorship] Hall, J., Aaron, M., Jones, B., Feamster, N., "A Survey of Worldwide Censorship Techniques", https://tools.ietf.org/html/draft-hall-censorship-tech-05, May 2018, Work-in-progress

[BBCTECH] https://www.bbc.com/news/technology-45495544, Sept. 2018

[EU-DIGCOPY] http://www.europarl.europa.eu/news/en/press-room/20180906IPR12103/parliament-adopts-its-position-on-digital-copyright-rules, Sept. 2018

[FBNorms] https://www.theguardian.com/news/2017/may/22/facebook-moderator-guidelines-extreme-content-analysis, May 2017

[Myanmar] https://www.theguardian.com/technology/2018/aug/27/facebook-removes-accounts-myanmar-military-un-report-genocide-rohingya, August 2018

[Child-Porn] https://gizmodo.com/fbis-disturbing-hacking-powers-challenged-in-court-over-1794885187, May 2017

[UDHR] United Nations, "Universal Declaration of Human Rights", 1948, <http:///www.un.org/en/universal-declaration-human-rights/>

[EUCOPY] http://www.europarl.europa.eu/news/en/press-room/20180906IPR12103/parliament-adopts-its-position-on-digital-copyright-rules, September 2018

[ITALY-REG] https://www.adm.gov.it/portale/lagenzia/monopoli-comunica/contrasto-illegalita, January 2007

[UK-Controls] https://www.ispreview.co.uk/index.php/2017/10/uk-gov-softens-stance-mandatory-isp-filters-adult-internet-content.html, October 2017

[DailyStormer] Prince, M., "Why We Terminated Daily Stormer", https://blog.cloudflare.com/why-we-terminated-daily-stormer/, August 2017

[WikiOTT] WikiPedia, "Over-the-top media services", https://en.wikipedia.org/wiki/Over-the-top_media_services, October 2018

Authors' Addresses

Nalini Elkins
Enterprise Data Center Operators (EDCO)
EMail: nalini.elkins@e-dco.com

Barry Shein
Software Tool and Die
EMail: bzs@theworld.com

Vittorio Bertola
Open Exchange
EMail: vittorio.bertola@open-xchange.com

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

N. ten Oever
Univeristy of Amsterdam & Texas A&M University
G. Perez de Acha
Derechos Digitales
S. Couture
University de Montreal
M. Knodel
Center for Democracy & Technology

November 02, 2020

Freedom of Association on the Internet
draft-irtf-hrpc-association-06

Abstract

This document discusses the relationships between the Internet architecture and the ability of people to exercise their right to freedom of assembly and association online. The Internet increasingly mediates our lives, our relationships, and our ability to exercise our human rights. As a global forum, the Internet provides a public space, yet it is predominantly built on private infrastructure. Since Internet protocols play a central role in the management, development, and use of the Internet, we analyze the relation between protocols and the rights to assemble and associate to mitigate infringements on those rights.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

"In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms".

- Annual Report to the UN Human Rights Council by the Special Rapporteur on the rights to freedom of peaceful assembly and of association (2019).

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

The current draft continues the work started in "Research into Human Rights Protocol Considerations" [RFC8280] by investigating the impact of Internet protocols on a specific set of human rights, namely the right to freedom of assembly and association. Taking into consideration the international human rights framework regarding the human right to freedom of assembly and association, the present document seeks to deepen the relationship between this human right and Internet architecture, protocols, and standards. In that way, we continue the work of the Human Rights Protocol Consideration Research Group, as laid out in its charter, where one of the research aims is "to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly" [HRPC-charter]. The conclusions may inform the development of new guidelines for protocol developers in draft-irtf-hrpc-guidelines.

The research question of this document is: what are the protocol development considerations for freedom of assembly and association?

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 question

The research question of this document is: what are the protocol development considerations for freedom of assembly and association?

4. Methodology

The point of departure of the present work [RFC8280] is an initial effort to expose the relationship between human rights and the Internet architecture, specifically protocols and standards. As such, [RFC8280] was inductive and explorative in nature. The methodology in this previous work was based on the discourse analysis of RFCs, interviews with members of the IETF community, and participant observation in IETF working groups, with the goal to identify technical concepts that relate to human rights. This work resulted in the proposal of guidelines to describe a relationship between the right to freedom of assembly and association and connectivity, security, censorship resistance, anonymity, pseudonymity, accessibility, decentralization, adaptability, and outcome transparency.

In this document, we deepen our exploration of human rights and protocols by assessing one specific set of human rights: freedom of association and assembly, abbreviated here as FAA. Our methodology for doing so is the following: first, we provide a brief twofold literature review addressing the philosophical and legal definitions of FAA and how this right has already been interpreted or analyzed concerning the digital. This literature review is not exhaustive nor systematic but aims at providing some lines of questioning that could later be used for protocol development. The second part of our methodology looks at some cases of Internet protocols that are relevant to the sub-questions highlighted in the literature review, and analyze how these protocols facilitate and inhibit the right to assembly and association.

5. Literature Review

5.1. FAA definition and core treaties

The rights to freedom of association and assembly are defined and guaranteed in national law and international treaties. Article 20 of the Universal Declaration of Human Rights [UDHR] states for instance that "Everyone has the right to freedom of peaceful assembly and association" and that "No one may be compelled to belong to an association". Article 23 further guarantees that "Everyone has the right to form and to join trade unions for the protection of his interests". In the International Covenant on Civil and Political Rights, article 21 stipulates that "The right of peaceful assembly shall be recognized" and that "No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others" while article 22 states that "Everyone shall have the right to freedom of association with others, including the right to form and join trade unions". Other treaties are sometimes cited as the source and framework to the right to freedom of association and assembly. The Australian government [Australia] for instance refers to Article 5 of the Convention on the Elimination of All Forms of Racial Discrimination [CERD] which stipulates freedom of peaceful assembly and association should be guaranteed "without discrimination as to race, colour, national or ethnic origin"; Article 15 of the Convention on the Rights of the Child [CRC] which recognises to child pending the restrictions cited above; and Article 21 of the Convention on the Rights of Persons with Disabilities [CRPD] which insist on usable and accessible formats and technologies appropriate for persons with different kinds of disabilities.

From a more philosophical perspective, Brownlee and Jenkins [Stanford] make some interesting distinctions in particular regarding the concepts of association, assembly and interaction. On one end, "interaction" refers to any kind of interpersonal and often incidental engagements in daily life, like encountering strangers on a bus. Interaction is seen as a "prerequisite" for association. Assembly on the other end, has a more political connotation and is often used to refer to activists, protesters, or members of a group in a deliberating event. In between the two, association refers to more "persistent connections" that are not necessarily political in nature. The authors thus distinguish between intimate associations, like friendship, love, or family, and collective association like trade unions, commercial business, or "expressive associations" like civil rights organizations or LGBTQIA associations. For Brownlee and Jenkins [Stanford], the right to association is linked to different relative freedoms: permission (to associate or dissociate), claim-right (to oppose others interfering with our conduct), power (to alter the status of our association), immunity (from other people interfering in our right). Freedom of association and assembly thus refers both to the individual right to join or leave a group and to the collective right to form or dissolve a group and to organize itself. These rights, however, are relative and not absolute. Parents, for instance, have limited rights to exclude their underage child from family households. Excluding someone from an association based on its sex, race or other individual characteristic is also often contentious if not illegal. Restrictions on freedom of association can be imposed by states, but only if this is lawful and proportionate. States must document how these limitations are necessary in the interests of national security or public safety, public order, the protection of public health or morals, or the protection of the rights and freedoms of others. Finally, states must also protect participants against possible abuses by non-State actors.

In international law, the right to freedom of assembly and association protects 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 is 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 a 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, both are protected to the same degree. Where 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 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]. Think about civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, or foundations.

When talking about the human right of freedom of association and assembly, one should always take into account that 'all human rights are indivisible, interrelated, unalienable, universal, and mutually reinforcing' [ViennaDeclaration]. This means that in the analysis of the impact of a certain variable on freedom of association and assembly one should take other human rights into account too. When devising an approach to mitigate a possible negative influence on this right, one should also always take into account the possible impact this might have on other rights. For example, the following rights are often impacted in conjunction with freedom of association and assembly: the right to political participation, the right to (group) privacy, the right to freedom of expression, and access to information. For instance, when the right to political participation is hampered, this often happens in conjunction with a limitation of the freedom of association and assembly because political participation is often done collectively. When the right to privacy is hampered, this privacy of particular groups is also impacted (so-called 'group privacy' [Loi], which potentially has consequences for the right to association and assembly. Where the freedom of expression of a group is hampered, such as in protests or through Internet shutdowns, this both hampers other people's ability to receive the information of the group, and impact the right to assembly of the people who seek to express themselves as a group [Nyokabi].

Finally, if the right to association and assembly is limited by national law, this does not mean it is consistent with international human rights law. In such a case, the national law would therefore not be legitimate [Glasius].

5.2. FAA in the digital era

Before discussion freedom of association and assembly as it pertains to digital environments, we must first recognize that the United Nations Human Rights Council adopted Resolution 20/8 2012, which was later adopted by the United Nations General Assembly [UNHRC2016], which affirms "... that the same rights that people have offline must also be protected online ...". Therefore the digital environment is no exception to application of this right by any means. The questions that remain, however, are how these rights should be conceptualized and implemented in different parts and levels of digital environments.

The right to freedom of assembly and association is the subject of increasing discussions and analysis. In 2016, the Council of Europe published a report, "Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet" [CoE] which noted that while the Internet and technologies are not explicitly mentioned in international treaties, these treaties nevertheless apply to "the online environment". The report argue the "Internet is the public sphere of the 21st century", something demonstrated by the fact that informal associations can be gathered at scale in a matter of hours on the Internet, and that digital communication tools often serve to facilitate, publicize or otherwise enable presential associations or assemblies, like a protest or demonstration. They note, on the other hand, the negative ways in which the Internet can also be used to promote or facilitate terrorism, urban violence and hate speech, thus insisting on the "extremely important and urgent" need to fight online terrorist activities such as recruitment or mobilization, while at the same time respecting the right to peaceful assembly and association of other users. The report mentions the following use cases that could be help further our reflection:

- Instances of network shutdowns in the Arab Spring, to prevent people from organising themselves or assembling

- California's Bay Area Rapid Transit (BART) shutdown of mobile phone service, to avoid protester violence and disruption of service

- The wholesale blocking of Google as a violation of freedom of expression

- Telus, a telecom company which blocked customers' access to websites critical of Telus during a Telecommunications Workers Union strike against it

- The targeting of social media users who call for or organise protests though the Internet in Turkey's Gezi Park protests

- Mass surveillance or other interferences with privacy in the context of law enforcement and national security

- Use of VPNs (Virtual Private Networks) to the TOR network to ensure anonymity

- Distributed Denial of Service attacks (DDoS) as civil disobedience.

More recently, the 2019 Annual Report addressed to the UN Human Rights Council by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, also notes the opportunities and challenges posed by digital networks to the rights to freedom of peaceful assembly and of association. The report recommends that international human rights norms and principles should also be used as a framework "that guides digital technology companies' design, control and governance of digital technologies". The report states that "technical standards" in particular can affect the freedom of association and assembly, and makes some recommendations on which the following could be relevant to our discussion here:

- "[Undertake] human rights impact assessments which incorporate the rights to freedom of peaceful assembly and of association when developing or modifying their products and services,"

- "increase the quality of participation in and implementation of existing multi-stakeholder initiatives,"

- "collaborate with governments and civil society to develop technology that promotes and strengthens human rights,"

- "support the research and development of appropriate technological solutions to online harassment, disinformation and propaganda, including tools to detect and identify State-linked accounts and bots," and

- "adopt monitoring indicators that include specific concerns related to freedom of peaceful assembly and association."

In one of their "training kits" [APCtraining], the Association of Progressive Communications addressed different impacts of the internet on association and assembly and raised three particular issues worthy to note here:

1. Organization of protests. Internet and social media are enablers of protests, such as it was seen in the "Arab Spring". Some of these protests - like online petitions or campaigns - are similar to offline association and assembly, but other protest forms are inherent to the Internet capacity like hacking, DDOS and are subject to controversy within the Internet community, some people finding it legitimate, and others not.

2. Surveillance. While the Internet facilitates association, the association in turn leaves a lot of traces that can be used in turn for law enforcement but also for repressing political dissents. As they note, even the threat of surveillance can have deter facilitation.

3. Anonymity and pseudonymity can be useful protection mechanism for those who'd like to attend legitimate association without facing retribution. On the other hand, anonymity can be used to harm society, such as in online fraud or sexual predation.

Online association and assembly are the starting point of group to mobilization in modern democracies, and even more so 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 played a crucial role by providing means for the fast dissemination of information otherwise mediated by the press, 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 an 'open global community' of network designers, operators, vendors, and researchers [RFC3233] is also protected by freedom of assembly and association . 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 a group of assembled network users [HafnerandLyon].

[RFC8280] is a paper by the Human Rights Protocol Consideration Resarch Group in the Internet Research Taskforce on internet protocols and human rights that discusses issues of FAA, specifically:

- The expansion of DNS for generic namespace as an enabler of association for minorities. The paper argues that specifically the expansion of the DNS to allow for new generic Top Level Domains (gTLDs) can have negative impacts on freedom of association because of restrictive policies by some registries and registrars, on the other hand could gTLDs also enable communities to build clearly identifiable spaces for association (such as .gay).

- The impact of Distributed Denial of Service attacks on freedom of association. Whereas DDoS has been used as a tool for protest, in many cases this is infringing on other parties freedom of expression. Furthermore, often devices (such as IoT devices and routers) are inscribed in such DDoS attacks whereas the owner or user did not consent to this. Thus they do not have the possibility to exit this assembly. Therefore the draft concluded that that IETF "should try to ensure that their protocols cannot be used for DDoS attacks"

- The impact of middleboxes on the ability of users to connect to the Internet and therefore their ability to exercise their right to freedom of association and assembly. The lack of connectivity can significantly impact freedom of assembly and association of a user. Especially if this is done in a way that is not knowable for the user and if there is no possibility to for the user to have access to due process to dispute the lack of (secure or private) connectivity in general or to a specific service.

In the 2020 report by the United Nations Special Rapporteur on Human Rights [UN44-24] it is concluded that technologies can be enablers of FAA, but technology is also significantly used to interfere with the ability of people to exercise their right to freedom association and assembly. Specifically, the report mentions network shutdowns, the usage of technology to surveil protests and users. This includes facial recognition, and the uses of other ways to violate the (group) privacy of people engaged in an assembly or association. The report makes it explicit that companies play a significant role enabling, for instance by developing, providing or selling the technology, but also by directly exercising these violations.

5.3. Specific questions raised from the literature review

Here are some questions raised from the literature review that can have implications for protocol design:

1. Should protocols be designed to enable legitimate limitations on association in the interests of "national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others", as stated in the ICCPR article 21 [ICCPR]? Where in the stack do we care for FAS?

2. Can protocols facilitate agency of membership in associations, assemblies and interactions?

3. What are the features of protocols that enable freedom of association and assembly?

4. Does protocol development sufficiently consider usable and accessible formats and technologies appropriate for all persons, including those with different kinds of disabilities?

5. Can a protocol be designed to legitimately exclude someone from an association?

In the following sections we attempt to answer these questions with specific examples of standardized protocols in the IETF.

6. Cases and examples

As the Internet mediates collective action and collaboration, it impacts on freedom of association and assembly. To answer our research question regarding how internet architecture enable and/or inhibits such human right, we researched several independent and typical cases related to protocols that have been either adopted by the IETF, or are widely used on the Internet. Our goal is to figure out whether they facilitate freedom of assembly and association, or whether they inhibit it through their design or implementation.

We are aware that some of the following examples go beyond the use of Internet protocols and flow over into the application layer or examples in the offline world whereas the purpose of the current document is to break down the relationship between Internet protocols and the right to freedom of assembly and association. Nonetheless, 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.

We use the literature review to guide our process of inquiry for each case, and to dive deeper in what can be found interesting about each case as it relates to freedom of association.

6.1. Got No Peace: Spam and DDoS

Should protocols be designed to enable legitimate limitations on association in the interests of "national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others", as stated in the ICCPR article 21{ICCPR}}? Where in the stack do we care for FAA?

The 2020 report by the United Nations Special Rapporteur on Human Rights [UN44-24] described how technology is often used to limit freedom of assembly and association, such as for instance through network shutdowns and the surveillance of groups. Because access to the Internet is crucial not only for freedom of association and assembly, but also for the right to development, and the right to freedom of expression and information [Nyokabi], the United Nation Special Rapporteur argues that:

(b) Avoid resorting to disruptions and shutdowns of Internet or telecommunications networks at all times and particularly during assemblies, including those taking place in electoral contexts and during times of unrest;

Whereas the states have the obligation to protect human rights, there has been an increasing call for non-state actors, such as companies, to respect human rights [UNGP]. This includes a chain-responsibility of actors, which means that not just the company's own processes should not negatively impact human rights, but they should also engage in due diligence processes, such as human rights impact assessments. This includes an assessment of whether the products that are sold, or the services that are provided, can be used to engage in human rights violations, or whether human rights violations occur in any stage of the supply chain of the company. If this is the case, measures should be taken to mitigate this.

In the case of dual-use technologies, this means that technology could be used for legitimate purposes, but could also be used to limit freedom of association or assembly, it might mean that producers or sellers should limit the parties they sell to, or even better, ensure that the illegitimate use of the technology is not technically possible anymore, or made more difficult.

6.1.1. Spam

In the 1990s as the internet became more and more commercial, spam came to be defined as irrelevant or unsolicited messages that were posted many times to multiple news groups or mailing lists {Marcus}}. Here the question of consent, but also harm, are crucial. In the 2000s a large part of the discussion revolved around the fact that certain corporations. protected by the right to freedom of association, considered spam to be a form of "commercial speech", thus encompassed by free expression rights [Marcus]. Yet spam can be not only a nuisance, but a threat to systems and users.

This leaves us with an interesting case: spam is currently handled mostly by mail providers on behalf of the user, next to that countries are increasingly adopting opt-in regimes for mailing lists and commercial e-mail, with a possibility of serious fines in case of violation. Yet many ask is spam not the equivalent of the fliers and handbills ever present in our offline world? The big difference between the proliferation of such messages offline and online is the scale. It is not hard for a single person to message a lot of people, whereas if that person needed to go house by house the scale and impact of their actions would be much smaller. Inversely if it were a common practice to expose people to unwanted messages online, users would be drowned in such messages, and no expression would be possible anymore. Allowing illimited sending of unsolicited messages would be a blow against freedom of speech: when everyone talks, nobody listens.

Here the argument is very similar to DDoS attacks, considered next: Legitimate uses of online campaigning, or online protesting, are drowned out by a malicious use which constitutes an attack on the internet infrastructure and thus the assembly or association itself.

6.1.2. DDoS

Distributed Denial of Service attacks are leveled against a server or service by a controller of a host or multiple hosts by overloading the server or service's bandwidth or resources (volume-based floods) or exploit protocol behaviours (protocol attacks). DDoS attacks can thus stifle and complicate the rights to assemble online for media and human rights organisations whose websites are the target of DDoS. At the same time there are comparisons made between DDoS attacks and sit-in protests [Sauter]. However the main distinction is significant: only a small fragment of "participants" (from controllers to compromised device owners) in DDoS attacks are aware or willing [RFC8280]. Notably DDoS attacks are increasingly used to commit crimes such as extortion, which infringe on others' human rights.

Because of the interrelation of technologies, it cannot be said that there is one point in the technical stack that there are characteristics of "peaceful" or "non-peaceful" association visible to protocol developers. As we can see from the cases of spam blocking and DDoS mitigation that "peaceful or non-peaceful" is not a meaningful heuristic, or even characteristic, of problematic content. If anything, their commonality is scale and volume.

6.2. Holistic Agency: Mailing Lists and Spam

Can protocols facilitate agency of membership in associations, assemblies and interactions?

6.2.1. 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 discussions, share information, ask questions, and build ties. Even as social media and discussion forums grow, mailing lists continue to be widely used [AckermannKargerZhang] and are still a crucial tool to organise groups and individuals around themes and causes [APC3].

Mailing lists' pervasive use are partly explained because they allow for "free" association: people subscribe (join) and unsubscribe (leave) as they please. Mailing lists also allow for association of specific groups on closed lists. This free association online enables agency of membership, a key component of freedom of association and assembly.

6.2.2. Spam

As we mentioned before, there are interesting implications for freedom of association and assembly when looking at spam mitigation. Here we want to specifically note that if we consider that the rights to assembly and association also mean that "no one may be compelled to belong to an association" [UDHR], spam infringes both rights if an op-out mechanism is not provided and people are obliged to receive unwanted information, or be reached by people they do not know.

6.3. Civics in Cyberspace: Messaging, Conferencing, and Networking

What are the features of protocols that enable freedom of association and assembly?

Civic participation is often expressed as the freedom to associate and assemble, along with a whole other set of enabling rights such as freedom of expression and the right to privacy. UN Special Rapporteur David Kaye established a strong relationship between technology that allows anonymity and uses encryption have positive effects on freedom of expression [Kaye]. Here we look at messaging, such as email, mailing lists and internet relay chat; video conferencing and peer-to-peer networking protocols to investigate the common features that enable freedom of association and assembly online.

6.3.1. Email

Similarly to freedom of expression's enabling and universal right to impart one's ideas openly, "the right to whisper", or confidentiality, is the ability to limit to whom one imparts one's ideas. An encrypted email project, the LEAP Encryption Access Project, says, "like free speech, the right to whisper is a necessary precondition for a free society. Without it, civil society languishes and political freedoms are curtailed. As the importance of digital communication for civic participation increases, so too does the importance of the ability to digitally whisper." [LEAP]

6.3.2. Mailing lists

Not only are mailing lists a good example of how protocols can facilitate the necessary ingredient of agency in freedom of association, mailing lists are an example of messaging technology that has other features that enable freedom of association and assembly.

The archival function of mailing lists allows for posterior accountability and analysis. The ubiquity and interoperability of email, and by extension email lists, provides a low barrier to entry to an inclusive medium.

Association and assembly online can be undermined when right to privacy is at risk. And one of the downsides of mailing lists are similar to the privacy and security concerns generally associated with email. At least with email, end-to-end encryption such as OpenPGP [RFC4880] and S/MIME [RFC5751] can keep user communications authenticated and confidential. With mailing lists, this protection is not as possible because with many lists the final recipients are typically too many for . There have been experimental solutions to address this issue such as Schleuder [Schleuder], but this has not been standardized or widely deployed.

6.3.3. IRC

Internet Relay Chat (IRC) is an application layer protocol that enables communication in the form of text through a client/server networking model [RFC2810]. In other words, a chat service. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients. Features of IRC include: federated design, transport encryption, one-to-many routing, creation of topic-based "channels", and spam or abuse moderation.

For the purposes of civic participation and freedom of association and assembly in particular it is critical that IRC's federated design allows many interoperable, yet customisable, instances and basic assurance of confidentiality through transport encryption. We investigate the particular aspect of agency in membership through moderation in the section 'Block Together Now: IRC and Refusals' below.

6.3.4. WebRTC

Multi-party video conferencing protocols like 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].

Even though some multi-party video conferencing tools facilitate freedom of assembly and association, their own configuration might 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 either improved or made explicit. This in turn would result in a more secure and/or private exercise of the right to freedom of assembly or association.

6.3.5. Peer-to-peer networking

At the organizational level, peer production is one of the most relevant innovations from Internet mediated social practices. According to [Benkler] these networks imply '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, [Benkler2] significantly expands on his definition of commons-based peer production. In his view, 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." [Benkler2]. To ensure that the knowledge generated is available for free use, commons-based projects are often shared under an open license

Peer-to-peer (P2P) is essentially a model of how people interact in real life because "we deal directly with one another whenever we wish to" [Vu]. Usually if we need something we ask our peers, who in turn refer us to other peers. In this sense, the ideal definition of P2P is that "nodes are able to directly exchange resources and services between themselves without the need for centralized servers" where each participating node typically acts both as a server and as a client [Vu]. [RFC5694] has defined it 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 has 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 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 -a characteristic that makes the system unpredictable: a resource might be only sometimes available, and some other resources might be missing or incomplete [Vu]. Lack of information might in turn makes association or assembly more difficult.

Additionally, when architecturally assessing the role of P2P systems we could 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].

6.4. Universal Access: The Web

Does protocol development sufficiently consider usable and accessible formats and technologies appropriate for persons with different kinds of disabilities?

The W3C has done significant work to ensure that the Web is accessible to people with diverse physical abilities [W3C]. The implementation of these accesibility standards for instance help people can't have issues with seeing or rendering an images to understand what the image actually contains.

The IETF uses English as its primary working language, both in its documentation and in its communication. This is also the case for reference implementations. Whereas it is estimated that roughly 20% of the Earth's population speaks English, whereas only 360 million speak English as their first language. [RFC2277] describes that '"Internationalization is for humans. This means that protocols are not subject to internationalization; text strings are.", this implies that protocol developers, as well as people that work with protocols, are not people, or that protocol developers are all in command of the English language. This means that it is significantly easier for people who have a command of the English language to become a protocol developer - and it might lead to the development of separate protocols that are developed within large language communities that are not using the English language or the Latin script. This makes it harder for people who seek to shape their own space of association and assembly on the Internet to do so. And is thus driving these communities into, often proprietary and non-interoperable services such as Facebook.

When Ramsey Nasser developed the Arabic programming language قلب (transliterated Qalb, Qlb and Alb) [Nasser] he called it 'engineering performance art' instead of engineering, because he knew that his language would not work. In part this is because all modern programming tools are based on the ASCII character set, which encodes Latin Characters and was originally based on the English Language. This highlights cultural biases of computer science and engineering. Despite long significant efforts, it is still largely impossible to register an email address in a language such as Devanagari, Arabic, or Chinese. Even if it is possible - it is to be expected that there will be a significant failure rate in sending and receiving emails with other services. This makes it harder for people who do not speak English and/or don't use the written Latin script to exercise their freedom of association and assembly.

6.5. Block Together Now: IRC and Refusals

Can a protocol be designed to legitimately exclude someone from an association?

Previously we spoke about the privacy protecting features of IRC that enable freedom of association and assembly, including transport security. But now we turn to the ability to block users and effectively moderate discussions on IRC as a key feature of the technology that enables agency in membership, a key aspect of freedom of association and assembly.

For order to be kept within the IRC network, special classes of users become "operators" and are allowed to perform general maintenance functions on the network: basic network tasks such as disconnecting (temporary or permanently) and reconnecting servers as needed [RFC2812]. One of the most controversial power of operators is the ability to remove a user from the connected network by 'force', i.e., operators are able to close the connection between any client and server [RFC2812].

IRC servers may deploy different policies for the ability of users to create their own channels or 'rooms', and for the delegation of 'operator'-rights in such spaces. Some IRC servers support SSL/TLS connections for security purposes [RFC7194] which 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.

7. Conclusions: Can we learn anything from the previous case studies?

Communities, collaboration and joint action lie at the heart of the Internet. Even at at a linguistic level, the words "networks" and "associations" are closely related. Both are 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.

Given that the Internet itself was originally designed as a medium of communication for machines that share resources with each other as equals [RFC0903], the Internet is now one of the most basic infrastructures for the right to freedom of assembly and association. Since Internet protocols and the Internet architecture 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.

After reviewing several cases representative of FAA considerations inherent in protocols standardized at the IETF, we can conclude that the way in which infrastructure is designed and implemented impacts people's ability to exercise their freedom of assembly and association. This is because different technical designs come with different properties and characteristics. These properties and characteristics on the one hand enable people to assemble and associate, but on the other hand also adds limiting, or even potentially endangering, characteristics. More often than not, this depends on the context. A clearly identified group for open communications, where messages are sent in cleartext and where peoples persistent identities are visible, can help to facilitate an assembly and build trust, but in other contexts the same configuration could pose a significant danger. Endangering characteristics should be mitigated, or at least clearly communicated to the users of these technologies.

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 interoperability or data-portability. The use of social-media platforms has enabled groups to associate, but it has also rendered users unable to change platforms, therefore leading to a sort of "forced association" that inhibits people to fully exercise their freedom of assembly and association.

8. 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 and Gurshabad for finding a lot of typos.

- Gurshabad Grover and an anonymous reviewer for a full review.

- The hrpc mailinglist at large for a very constructive discussion on a hard topic.

9. Security Considerations

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

10. IANA Considerations

This document has no actions for IANA.

11. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research Group is located at the e-mail address hrpc@ietf.org [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]

12. References

12.1. 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>.

[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>.

[APC3] Association for Progressive Communications, "Closer than ever", 2020, <https://www.apc.org/en/node/36145/#tools>.

[APCtraining]
Sauter, D. and Association for Progressive Communications, "Multimedia training kit", 2013, <http://itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_FOA_Handout.pdf>.

[Australia]
Australian Government, Attorney-General's Department, "Right to freedom of assembly and association", 2020, <https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/right-freedom-assembly-and-association#topofpage>.

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

[Benkler2]
Benkler, Y., "The wealth of Networks - How social production transforms markets and freedom", New Haven and London - Yale University Press , 2006, <http://is.gd/rxUpTQ>.

[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.

[CERD] United Nations, "Convention on the Elimination of all forms of Racial Discrimination", 1966, <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/2F70352A0B65EB67CA256B6E0075FE13>.

[CoE] Council of Europe, "Freedom of assembly and association on the Internet", 2015, <https://mk0rofifiqa2w3u89nud.kinstacdn.com/wp-content/uploads/COE-report-on-FOAA-rights-on-the-internet-.pdf>.

[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/>.

[CRC] Wikipedia, ., "Lorum", 2000, <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/E123F4F71DCAE3E7CA256B4F007F2905>.

[CRPD] United Nations, "Convention on the Rights of Persons with Disabilities", 2007, <http://www.austlii.edu.au/au/other/dfat/treaties/2008/12.html>.

[Glasius] Glasius, M., Schalk, J., and M. De Lange, "Illiberal Norm Diffusion: How Do Governments Learn to Restrict Nongovernmental Organizations?", 2020, <https://academic.oup.com/isq/article/64/2/453/5823498>.

[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>.

[HRPC-charter]
Human Rights Protocol Consideration RG, ., "Charter for Research Group", 2015, <https://datatracker.ietf.org/doc/charter-irtf-hrpc/>.

[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>.

[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>.

[LEAP] LEAP, "The Right to Whisper", 2020, <https://leap.se/en/about-us/vision>.

[Loi] Loi, M. and M. Christen, "Two Concepts of Group Privacy", 2020, <https://link.springer.com/article/10.1007/s13347-019-00351-0>.

[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>.

[Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and the first amendment", 1998, <http://www.cardozoaelj.com/wp-content/uploads/2013/02/Marcus.pdf>.

[Nasser] Nasser, R., "قلب", 2013, <https://nas.sr/%D9%82%D9%84%D8%A8/>.

[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>.

[Nyokabi] Nyokabi, D., Diallo, N., Ntesang, N., White, T., and T. Ilori, "The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa", 2019, <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1582/3.Global%20article%20HRDA_2_2019.pdf?sequence=4&isAllowed=y>.

[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>.

[RFC0903] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", STD 38, RFC 903, DOI 10.17487/RFC0903, June 1984, <https://www.rfc-editor.org/info/rfc903>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

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

[Schleuder] Nadir, "Schleuder - A gpg-enabled mailinglist with remailing-capabilities.", 2017, <https://schleuder.nadir.org/>.

[Stanford]
Brownlee, K. and D. Jenkins, "Freedom of Association", 2019, <https://plato.stanford.edu/entries/freedom-association/>.

[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>.

[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>.

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

[UN44-24] Wikipedia, ., "Lorum", 2000, <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx>.

[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>.

[UNGP] United Nations, "Guiding Principles on Business and Human Rights", 2011, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

[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>.

[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>.

[ViennaDeclaration]
United Nations, "Vienna Declaration and Programme of Action", 1993, <https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx>.

[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>.

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

12.2. 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
Univeristy of Amsterdam & Texas A&M University

EMail: mail@nielstenoever.net

Gisela Perez de Acha
Derechos Digitales

EMail: gisela@derechosdigitales.org

Stephane Couture
University de Montreal

EMail: stephane.couture@umontreal.ca

Mallory Knodel
Center for Democracy & Technology

EMail: mknodel@cdt.org

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

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

Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft University of Amsterdam
Intended status: Informational September 28, 2019
Expires: March 31, 2020

Notes on networking standards and politics
draft-irtf-hrpc-political-07

Abstract

The IETF cannot ordain what standards or protocols are to be used on networks, but the standards development process in the IETF does have an impact on society through its normative standards setting process. This document aims to bring about a better understanding on the political nature of standards and protocols. Among other things, the IETF's work affects what is perceived as technologically possible and useful where networking technologies are being deployed, and its standards reflect what is considered by the technical community to be feasible and good practice. Whereas there might not be agreement among the Internet protocol community on the specific political nature of the technological development process and its outputs, it is generally agreed that standards and protocols are both products of a political process, and they can also be used for political means.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

"Standards are recipes for reality."

– Lawrence Busch

"As standards emerge from contested contexts, that immediately function as a means of control within the political and economic order."

– Andrew L. Russell

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

–{{RFC3935}}

Recently there has been increased discussion in the IRTF and IETF on the relation between Internet protocols and human rights [RFC8280], which spurred discussion of the value neutrality and political nature of standards. The network infrastructure is on the one hand designed, described, developed, standardized and implemented by the Internet community, while on the other hand the Internet community and Internet users are affected by the technology. Companies, citizens, governments, standards development bodies, public opinion and public interest groups all play a part in these discussions. This document outlines different views on the relation between politics, standards, and protocols, and seeks explore the question whether standards and protocols are political, and if so, how.

This question in not necessarily a new one. The design of the Internet, and its codification through protocols and standards, is a technical issue with great political and economic impacts, as is described in [RFC0613] and [RFC3271]. The early Internet community already realized that it needed to make decisions on political issues such as:

- internationalization, expanding the network outside of the United States [BramanI];

- access, how people are able to access the network, and who has control [RFC0101];

- privacy and security, what level of secrecy should be considered and expected on the network [BramanIII];

as well as use of the network by different groups with different needs and requirements, such as:

- the military [RFC0164] [RFC0316];

- governments [RFC0144] [RFC0286] [RFC0313] [RFC0542] [RFC0549];

- and non-governmental entities [RFC0196].

Sandra Braman has foregrounded these political consideration in historical RFC in her extensively analysis of these documents [BramanII]. This document seeks to understand how this is relevant for current day Internet standardization and protocol design. The coordinating of 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, although this process is not exclusively undertaken by transnational corporations. Conformance to certain standards is often a basic condition of participation so there are strong economic and political incentives to conform, even in the absence of legal requirements [Russell].

This documents builds on that research and seeks to increase understanding about what this means in the context of Internet protocols and the entities that design, develop, and standardize them.

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 actor through the ordering of an environment by a technology. This means that a technology does not determine what is possible, but that it invites specific kinds of behavior, and in that process shapes the behavior of users, without aboslutely determining it.

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 'A standard is an agreed-upon way of doing something or measuring something.' [Sisson]

Internet 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

To bring about a better understanding on the political nature of standards and protocols, this documents asks the questions: If, and if so how, are protocols, standards, and politics interrelated? Exploring this question aims to inform discussions in the IETF, IRTF, and the wider Internet infrastructure and architecture community.

4. Technology and Politics: a review of literature and community positions

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 [RFC1087], when the Internet was still looking entirely different. Nonetheless there has been a recent uptick in discussions within the IETF and IRTF about the impact of Internet protocols on human rights [RFC8280], and more generally in public debate about the impact of technology on society.

This document aims to provide an overview of the spectrum of different positions that have been observed in the IETF and IRTF community, and have been observed during interviews, mailinglist exchanges, and during research group sessions. These positions were observed during participatory observation, through 39 interviews with members of the community, the Human Rights Protocol Considerations Research Group mailing list, and during and after the Technical Plenary on Protocols and Human Rights during IETF98.

Without judging them on their internal or external consistency they are represented here. Where possible we also sought to engage with the 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 sometimes

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 implies that protocols could 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, especially in a context where the interrelation between protocols is hard to predict. The system consisting of the Internet and its users is vastly complex; it is chaotic in nature; standards are voluntary; and therefore 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 possibly be predicted, one could, as a point of departure, consider the impact of proposed implementations.

4.4. The network of networks 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 of automobiles imposes 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 a protocol's success is its incremental deployability [RFC5218]. This means that the network already contains constraints on what can be deployed into it. In this sense the network of networks creates its own paths, but also has its own objective. According to this view the goal of the network of networks is interconnection and connectivity; more connectivity is good for the network of networks. 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 make [Bloor].

4.5. Protocols are inherently political

This position argues the opposite of 'technological neutrality'. This position is illustrated by Postman when 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;

(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 perceived by many as political, although driven by a technical argument. The process that led to [RFC7258] is similar: the Snowden disclosures, which occurred in the political space, engendered the IETF to act. While [RFC2804] was a statement about how a protocol for wiretapping would _not_ be developed, [RFC7258] was a statement that contributed to the development of protocols such as [RFC7858], [RFC8226], and [RFC8404]. The impact of political tensions on protocol development 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 protocols are political because they influence the socio-technical workings of reality and society. The latter observation leads Winner to conclude that the reality of technological progress has too often been a scenario where innovation has dictated change for society. Those who had the power to introduce a new technology also had the power to largely frame the uses of 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. Discussion

Economics, competition, collaboration, openness, and political impact have been an inherent part of the work of the IETF since its early beginnings [Russell] [BramanII] [Abbate]. 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 for many of the Internet's formative years. Because a standard is the blue-print for how to accomplish a particular task, the adopted standards have a normative effect. The standardization work at the IETF has direct implications on what is perceived as technologically possible and useful where networking technologies are being deployed, and thus its standards reflect what is considered by the technical community as feasible and good practice.

Whereas there might not be agreement among the Internet protocol community on the specific political nature of the technological development process and its outputs, there is a general consensus among scholars in the fields of Science and Technology Studies and Philosopht of Technology, that technology in general, and standards in specific can be:

- a mean for political activity (for instance by using a tool (or protocol) to suppress freedom of expression or enhance citizenship participation),

- an object of political activity or deliberation (this can be foregrounded by asking who is making the decision about protocols? Is it democratic and legitimate? Who is excluded in these spaces of decision about protocols/standards? Who should be included, why, and how?), ans as

- the setting of political activity (this is analyzing by asking what are the constraints and possibilities of our particular technological culture? How is the history of this technological culture affecting our choices today? [Barney]

This opinion is not widely shared with the IRTF and IETF. There it is generally agreed that standards and protocols can be products of a political process, and they can be used for political means, but that this is not always the case.

6. Conclusion

While understanding that 'standards emerge from contested contexts, they immediately function as a means of control within the political and economic order' [Russell], protocols and standards as abstract isolated artefacts might not be political, but their design, development, deployment, and implementation often is. Therefore we might need to give a qualified answer to the research question, in the sense that protocols can only be understood in part outside of their actual shaping, use, and applied function, which is political. There is no consensus with the Human Rights Protocol Consideration Research Group whether this is always the case, or only in specific cases.

Further research could explore how the political nature of the design, development, standardization, and deployment of protocols can be taken into account in the standards development process in order to (1) to minimize negative unintended social consequences, (2) ensure clear understanding of the intended consequences, (3) maintain importance of the IETF as open standards body that facilitates global interoperability.

7. 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.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgments

Thanks to Michael Rogers, Joe Hall, Andrew Sullivan, Brian Carpenter, Mark Perkins, S Moonesamy, Stephen Farrell, Amelia Andersdotter, Stephane Couture, and all contributors and reviewers on the hrpc mailinglist. Special thanks to Gisela Perez de Acha for some thorough editing rounds.

10. 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]

11. References

11.1. Informative References

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

[Barney] Barney, D., "One nation under google", Hart House Lecture 2007 , 2007, <http://darinbarneyresearch.mcgill.ca/Work/One_Nation_Under_Google.pdf>.

[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://people.tamu.edu/~Braman/bramanpdfs/43_internationalization.pdf>.

[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://people.tamu.edu/~Braman/bramanpdfs/50_theframingyears.pdf>.

[BramanIII] Braman, S., "Privacy by design: Networked computing, 1969-1979", New Media & Society, 14(5), 798-814, 2011. , 2011, <http://people.tamu.edu/~Braman/bramanpdfs/59_privacybydesign.pdf>.

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

[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>.

[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.

[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>.

[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.

[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>.

[RFC1087] Defense Advanced Research Projects Agency and Internet Activities Board, "Ethics and the Internet", RFC 1087, DOI 10.17487/RFC1087, January 1989, <https://www.rfc-editor.org/info/rfc1087>.

[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>.

[RFC3271] Cerf, V., "The Internet is for Everyone", RFC 3271, DOI 10.17487/RFC3271, April 2002, <https://www.rfc-editor.org/info/rfc3271>.

[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>.

[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>.

[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>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

[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>.

[RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of Pervasive Encryption on Operators", RFC 8404, DOI 10.17487/RFC8404, July 2018, <https://www.rfc-editor.org/info/rfc8404>.

[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/>.

[Winner] Winner, L., "Upon opening 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.

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

Author's Address

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net

Human Rights Protocol Considerations Research Group B. Martini
Internet-Draft Harvard Kennedy School
Intended status: Informational N. ten Oever
Expires: April 25, 2019 University of Amsterdam
October 22, 2018

QUIC Human Rights Review
draft-martini-hrpc-quichr-00

Abstract

QUIC is a new transport protocol that provides low-latency communication and security. QUIC's key features include faster connection establishment, stream-based multiplexing, improved loss recovery, and no head-of-line blocking. This document assesses the potential human rights implications emerging from the deployment of QUIC. The assessment is done based on the methodology articulated in [RFC8280].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This is a review done within the framework of the Human Rights Review Team, and it was conducted by Beatrice Martini and Niels ten Oever. The Human Rights Review Team aims to implement and improve the guidelines for human rights considerations provided in [RFC8280], and seeks to mitigate potentially adverse human rights impacts that IETF and IRTF documents might have.

Human Rights Reviews are developed by a group of individuals in the IRTF and IETF. They work collaboratively and provide their knowledge and input to the assessments, in an effort to contribute to the IETF open review process. Human Rights Reviews are individual contributions. The authors hope that the comments will be taken into consideration by the draft authors, Working Groups and the IESG.

This review concerns the QUIC protocol in general, and the following drafts in particular: draft-ietf-quic-transport-12, draft-ietf-quic-tls-12, draft-ietf-quic-invariants-01.

2. Vocabulary Used

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

Censorship Technical mechanisms, including both blocking and filtering, that state or private actors can use to block or degrade Internet traffic. For further details on the various elements of Internet censorship, see [Halletal].

Censorship resistance Methods and measures to mitigate Internet censorship.

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

Connectivity The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958]. Different types of connectivity are further specified in [RFC4084].

Content agnosticism Treating network traffic identically regardless of content.

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

As a result, per [FIArch], the heterogeneity principle proposed in [RFC1958] needs to be supported by design.

Human rights Principles and norms that are indivisible, interrelated, inalienable, universal, and mutually reinforcing. Human rights have been codified in national and international bodies of law. The Universal Declaration of Human Rights [UDHR] is the most well-known document in the history of human rights. The aspirations from [UDHR] were later codified into treaties such as the International Covenant on Civil and Political Rights [ICCPR] and the International Covenant on Economic, Social and Cultural Rights [ICESCR], after which signatory countries were required to reflect them in their national bodies of law. It is also broadly recognized that not only states, but also non-state actors must respect human rights.

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

Linkability Establishing the identity of a host across several IP addresses.

Open standards As stated in [RFC2026]: "Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be 'open external standards' for the purposes of the Internet Standards Process."

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

Ossification The increasing inflexibility of the network which results in the inability to deploy a new protocol or protocol extensions due to the unchangeable nature of infrastructure components that have come to rely on particular features of current protocols.

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

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

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

Privacy is a broad concept regarding the protection of individual or group autonomy and the relation between an individual or group and society, including government, companies, and private individuals. It encompasses a wide range of rights, including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognized as a core right that underpins human dignity and other values such as freedom of association and freedom of speech. The right to privacy is also recognized in nearly every national constitution and in most international human rights treaties. The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.

Pseudonymity The ability to use a persistent identifier that is not immediately linked to an individual's offline identity. Pseudonymity is an critical feature for many end users, as it allows them different degrees of disguised identity and privacy online. "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]

3. Review Methodology and Process

This section describes how the review was undertaken.

We started our review by examining the Internet Drafts which were active on June 7, 2018 on the QUIC Working Group Datatracker (https://datatracker.ietf.org/wg/quic/documents).

Inferential reading of the documents resulted in the decision to focus our efforts on three specific drafts: draft-ietf-quic-transport-12, draft-ietf-quic-tls-12, draft-ietf-quic-invariants-01.

From the study of these documents through the perspective of the Guidelines for Human Rights Protocol Considerations outlined in [RFC8280], we formulated a questionnaire, to be used as a tool to guide semi-structured interviews with QUIC Working Group chairs and document authors.

We engaged in a total of seven interviews, which took place during IETF102 (July 14-20, 2018). These were then transcribed and analyzed. The analysis focused on the identification of potential positive or negative impacts on human rights, and on the categorization of our findings according to the Guidelines for Human Rights Protocol Considerations outlined in [RFC8280].

One particular aspect that is critical to consider is the pace at which the QUIC Working Group operates, which is regarded across the IETF community as notably faster than usual. This means that while the general design that is outlined in the QUIC Internet Drafts is fairly stable, numerous details are in constant change. When it comes to conducting an interview-based research, this also means that some of the expressed points of view might be overtaken by intervening changes. To address this specific characteristic of the work on the QUIC protocol, we decided to set a time point to examine active Internet Drafts and current Working Group discussions. The time point is June 7, 2018. In addition to that, we also kept discussing with the interviewees, reviewing notes from the following New York interim meeting (September 19-20), and following selected mailing list threads, until our final review of this very document, on October 17, 2018.

The content examined until the set time point (June 7, 2018) is what should be considered the core subject of our examination. However, as we aim to helpfully contribute to the efforts of the QUIC Working Group, we also decided to monitor potential updates and emerging discussions which took place in the following months, with the aim to provide relevant and applicable feedback.

4. Human Rights Considerations

The Human Rights Protocols Considerations Research Group (HRPC) welcomes the drafts draft-ietf-quic-transport, draft-ietf-quic-tls, draft-ietf-quic-invariants.

In particular, we welcome the efforts to improve connectivity on high latency, low bandwidth and high loss connections, and the application of encryption by default. Conclusions and recommendations can be found at the end of this document.

No implications for Accessibility ([RFC8280], sec. 6.2.11), Localization ([RFC8280], sec. 6.2.12), Decentralization ([RFC8280], sec. 6.2.13), and Reliability ([RFC8280], sec 6.2.14) have been found.

4.1. Connectivity

Overall, QUIC is expected to result in a greatly improved Internet service for users worldwide, and in particular for those who currently do not have high bandwidth or lossless connections. Regions that currently do not benefit from reliable connectivity, would be provided with a significantly improved service. These advancements have positive implications in regards to human rights such as freedom of expression, freedom of association, right to political participation.

4.1.1. Latency

QUIC was designed as a new transport protocol to provide connections with lower latency than previous protocols.

One of the most important differences between TCP and QUIC connections is that QUIC connection establishment takes 0 RTTs when a server is known by a client and up to a few RTTs for the first connection to an unknown server.

By allowing for Zero-Round Trip Time (0-RTT) resumption of connections, QUIC performs better than TCP on high latency and high loss connections. When a web client uses TCP and TLS, it requires two to three round trips with a server to establish a secure connection before the browser can send a request. With QUIC, if a client has communicated with a server before (within a specific time period), it can start sending data without any round trips, so that web pages will load faster.

An example of QUIC's performance can be observed on a well-optimized site like Google Search, where connections are often pre-established, and QUIC's faster connections can only speed up some requests. Still, QUIC improves mean page load time by 8% globally, and up to 13% in regions where latency is higher. [Behretal]

4.1.2. Congestion Control and Loss Recovery

QUIC's congestion control is based on TCP NewReno [RFC6582], a congestion window based congestion control. The signals QUIC provides for congestion control are generic and are designed to support different algorithms. In this way, QUIC can be configured to fit best in different contexts.

Compared to TCP, QUIC offers more detailed feedback information for loss detection. For example, it uses a monotonically increasing packet number and does not retransmit on the packet-level but on the content-level. This allows QUIC to distinguish retransmissions from the originally sent packets, avoiding retransmission ambiguities.

Overall, comparing it to previously existing protocols, QUIC implements better estimation of connection RTTs and detects and recovers from loss more efficiently.

4.1.3. Reduced Head-Of-Line Blocking

HTTP/2 allows multiple objects to be fetched over the same connection, using multiple streams within a single flow.

In TCP, if a loss occurs in one stream, all streams stall while waiting for packet recovery. Differently, QUIC allows other streams to continue to exchange packets even if one stream is blocked due to a missing packet [MolaviKakhkietal].

4.1.4. Resources

QUIC is relatively expensive to implement, both in terms of code (size and complexity) and processing (including memory overheads). This can represent a barrier to adoption and the benefits that come with that.

4.2. Privacy

4.2.1. Encryption

QUIC incorporates the key negotiation features of TLS 1.3, requiring all connections to be encrypted.

Encryption improves the security and privacy of user data. It is built into QUIC, using AEAD algorithms such as AES-GCM and ChaCha20 for both privacy and integrity. QUIC authenticates the parts of its headers that it does not encrypt, so attackers cannot modify any part of a message [Behretal].

Furthermore, in addition to improving privacy, encryption helps to address the ossification of network protocols caused by middleboxes that assume certain information to be present in the clear [Kuehlewindetal].

4.2.2. Transparent Proxying

Many cellular and high-latency networks use transparent TCP proxies to reduce end-to-end delays and improve loss recovery. However, by encrypting the transport headers, QUIC prevents transparent proxying, thus protecting their integrity [MolaviKakhkietal].

4.2.3. Multiple Streams

By establishing connection with multiple streams, QUIC creates higher opacity for the observer.

Comparing QUIC to TLS over TCP, QUIC significantly reduces the amount of information that an observer can acquire about communications they are looking at.

In TCP, all of the information regarding the protocol flow at a transport layer is exposed, and can be used to identify active communications.

In QUIC, it is possible to have an established connection with an end point and to run multiple streams over that connection. Consequently, an observer who is looking at someone's connection, would not be able to tell the difference between the streams.

4.2.4. Packet Number Encryption

In QUIC packet numbers are encrypted.

From a general standpoint, the number assigned to each packet carries very little information. For example, it is possible to observe that a packet sent a certain time and the packet that was sent immediately after probably have increasing packet numbers.

But when traffic is carried over multiple paths, it becomes observable at many points, and this has privacy implications. For example, as stated in [draft-huitema-quic-mpath-req-01]: "[...] if packets belonging to a given connection carry some unique identifiers, observers could use these identifiers to track client migrations through several paths, and thus potentially expose the successive locations of a particular user."

4.2.5. Padding

Bit padding is the addition of one or more extra bits to a transmission or storage unit to make it conform to a standard size.

QUIC (like HTTP/2 and TLS) offers a padding mechanism that can be used as a defense against traffic analysis for protected packets. It is important to note that its use is discretionary by implementations.

4.2.6. Lawful Intercept

The lawful intercept of content in QUIC works similarly to TLS over TCP. An intercept can: force the acceptance of an alternate certificate; cooperate with or coerce the non-monitored endpoints to obtain session keys for decryption of traffic; exploit endpoint vulnerabilities to place monitoring devices directly on the endpoint on the other side of the crypto boundary.

Forcing TLS 1.3 avoids some common exploit vectors in TLS 1.2 and strengthens the ciphersuites.

4.2.7. Spin Bit

When Google offered the IETF the opportunity to take the work on QUIC and produce an open standard that could be used by all [Wilketal], it sparked off a debate within the IETF as to how much transport information should be deliberately kept unknown to the network.

As an explicit design goal, QUIC provides far less information about its operation to devices on path than TCP does. In TCP, the sequence and acknowledgement numbers and timestamps (if the respective option is in use) can be seen by on-path observers, and used to estimate end-to-end latency.

Differently from previous transport protocols, QUIC splits the information it uses for its own operation from its wire image. As a consequence, QUIC's wire image currently does not expose any information that can be used for passive latency measurement techniques [draft-ietf-quic-spin-exp-00].

At the June 2017 interim meeting of the QUIC Working Group, a proposal was made to add a latency spin bit to QUIC's wire image, in order to allow for passive measurability of RTT equivalent to TCP [Trammell01].

The spin bit is an explicit signal for passive measurability of round-trip time. It causes one bit in the header to 'spin', generating one edge (a transition from 0 to 1 or from 1 to 0) once per end-to-end RTT.

During the following months, the proposal to add this facility to the QUIC protocol has been further discussed and researched. At IETF101 the Working Group agreed upon the reservation of three bits for experimentation with passive RTT measurement, with the result of this experimentation to inform an eventual working group decision whether to include the bit in the shipping version 1 of the protocol, scheduled to be complete by November 2018. [Trammell02]

From its designers' perspective, the spin bit was formulated to be a minimal-risk, maximum-utility signal fit for a single purpose: on-path measurement of end-to-end RTT, to generate RTT samples for a variety of passive latency measurement tasks.

The key argument in favor of the spin bit originates from the notion that measurement is fundamental to the operation of networks and at-scale services, whether for management, security, optimization, and that if it is at all possible to safely design passive measurability of any metric explicitly into a protocol, this signal represents how to do it. [Trammell01]

The argument made by those who are not in favor of the addition of the spin bit to the protocol, is that the exposure of any information beyond the IP header and the base essentials of a UDP header is not necessary and not safe. They point out that how this bit may be used, were it to be added to the protocol, is unknown.

This could represent an infringement of the user privacy. Furthermore, an exposed bit might cause for ossification of the bit itself, which would, to some extent, defeat QUIC's efforts to elude the intrusive and ossifying grip of network middleware. [Huston]

4.2.8. Packet Injection

It is viable for network operators to add data to packets in order to do traffic monitoring and/or management. It is not uncommon for network operators to routinely tag packets as they enter the network for their own purposes, and simply erase the tag when they leave the network. Packet modification or injection cannot be prevented in QUIC. However, the protocol takes steps to ensure that its own state is not affected by this kind of activity.

4.3. Content Agnosticism

The QUIC protocol itself is content agnostic. While it is currently being optimized for HTTP traffic, it can also be used with other application layer protocols (e.g. see [draft-huitema-quic-dnsoquic-05]).

4.4. Security

QUIC improves security by making encryption an inherent part of the transport protocol, instead of adding it as a optional layer on top of it. This protects the integrity of the data by preventing tampering on the path, and ensures end-to-end confidentiality between the two communicating hosts. Furthermore, it ensure that no on-path party can emulate an endpoint.

By encrypting all Internet traffic by default it is harder for researchers and network operators to analyze network traffic. This is a specific design goal, but it also makes research into the promulgation of malware, cookies and other artefacts much harder, since in this case access to the stream needs to be provided by the end point.

4.5. Internationalization

[draft-ietf-quic-transport-12] does not define human readable strings, except for where it states that the Reason Phrase in the CONNECTION_CLOSE and APPLICATION_CLOSE frames "SHOULD be a UTF-8 encoded string [RFC3629]". The QUIC protocol demands that this SHOULD be an UTF-8 string, while UTF-8 is actually not required. Also, there is currently no space to declare the charset used. So it is recommended that this SHOULD becomes a MUST.

[draft-ietf-quic-transport-12] does not allow for the use of language tags. If it would request these tags, it would allow implementations to signal in which language Reason Phrases are rendered.

4.6. Censorship Resistance

Encryption makes monitoring and filtering of the traffic more complex, thus hindering fine-grained censorship.

Furthermore, in QUIC it is also harder to terminate connections, since in the protocol the only parties that can terminate the connection are those actually involved in the connection once it exists. This means that a middlebox cannot reset a connection, but needs to continue to block it, keeping state. Considering this, it can be stated that QUIC makes censorship harder because it requires the censor to invest more resources and efforts.

QUIC is also improving the protection against DDoS through observation of the handshake for connection confirmation, and through the need to validate new connections in case of a connection migration.

It is worth noting that it is almost impossible to make the handshake resilient to injection attacks, and the general consensus has been not to spend cycles trying. This means that handshakes can easily be disrupted by a censor. Post-handshake, QUIC is very resilient to attempts to reset the connection by a third party.

4.7. Open Standards

QUIC is published as open standard.

4.8. Heterogeneity Support

The design of the QUIC transport protocol is currently specifically tailored to be used with TLS1.3 and HTTP2. It is explicitly constructed in a modular manner and is designed to support other application layer protocols in the future as well.

4.9. Anonymity

Persistent static identifiers, consistently linking to a particular person or small, well-defined group of people, are one of the main threats to anonymity. This is especially concerning when the identifier is used in repeatedly used in multiple contexts, thus raising an issue of linkability.

In QUIC, linkability would occur in case a connection ID was used on multiple network paths. In order to provide some protection against linkability in case of connection migration, QUIC uses different connection IDs when different local addresses are used. Furthermore, packet numbers are encrypted to ensure they are not used to establish a link between different connection IDs.

However, it is important to note that traffic analysis might still allow to correlate different streams.

4.10. Pseudonymity

Keeping different identities isolated from each other is critical to protect and preserve pseudonymity. QUIC contributes to this by using different connections IDs for different local addresses.

4.11. Confidentiality

Through the use of cryptography, QUIC integrates security, confidentiality, authenticity, and integrity directly into the transport protocol rather than having them layered on top of it. Any server that offers QUIC to benefit from its latency improvements will automatically provide all the aforementioned attributes to their user.

4.12. Integrity

The use of TLS1.3 in QUIC makes on-path attacks either visible or nearly impossible to carry out. So, if an actor forces the traffic to go through one middlebox and decrypt the traffic itself, their action is made detectable. This also protects the integrity of the datastream, prevents tampering, and averts the injection of extra data in the stream.

4.13. Authenticity

Except for the initial handshake, the encryption in QUIC is provided by TLS1.3, which uses asymmetric cryptography to authenticate the hosts. This enables verification of authenticity.

4.14. Adaptability

QUIC has a modular approach, and is designed for adaptation. The only commitments in the protocol are the requirement to run on UDP, the packet header, and the version negotiation phase. The remainder of the protocol is quite flexible and can be further adapted.

By preventing the ossification of the protocol by middleboxes through the encryption of transport headers, QUIC enhances the adaptability of the architecture.

As a transport protocol, QUIC tries to be agnostic for application layer protocols, even though it is currently tailored to work with HTTP/2.

4.15. Outcome Transparency

Outcome transparency concerns the intelligibility of the effects of a protocol in relation to its users, protocol developers, and implementers, and its potential consequences (e.g. lack of authenticity may lead to lack of integrity and negative externalities)[RFC8280].

QUIC represents a remarkable evolution of the transport layer with significant impact on the Internet architecture and, most importantly, the service provided to users.

4.15.1. Encryption

The IETF has reached consensus on the fact that pervasive monitoring is an attack (see [RFC7258]), and that a response to mitigate this is represented by ubiquitous encryption, which would also reinforce the end-to-end nature of the network [RFC2775] [RFC3724] [RFC7754].

With the advent of QUIC, encryption becomes the default on the transport level. This has a critical impact on the protection of user privacy.

Furthermore, it has implications concerning network operators that had previously used visible parts of protocols to, among other things, manage, operate, and secure their networks [RFC8404].

Encryption also improves the integrity of the datastream, as QUIC allows to protect users against injections of ads by network operators.

4.15.2. Permissionless Innovation and Its Challenges

As suggested by interviewees during the research phase of this review, and to acquire a more contextualized understanding of protocol development efforts over time, it is relevant to pay attention to the history of SCTP (Stream Control Transmission Protocol). SCTP is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network, standardized in [RFC4960].

As outlined in the comparison between SCTP and QUIC presented in [draft-joseph-quic-comparison-quic-sctp-00], the deployment of SCTP is not particularly widespread. In-network devices, like NAT gateways for example, do not support SCTP well. NAT gateways need to be upgraded to be SCTP-aware, the modification of middleboxes is very expensive, and Internet service providers, focusing on the sustainability of their business, update the devices in accordance with the benefit that this can represent for their revenues.

Furthermore, an early version of QUIC (now popularly called gQUIC) was initially designed and deployed by a large content provider, Google. It was implemented in 2012, and the company invested significant resources to develop it, for example conducting thorough A/B-testing in order to assess how the protocol would interact with the network, and how the middleboxes would respond. QUIC is now widely used in Chrome clients accessing Google services.

In 2015, an Internet Draft of a specification for QUIC was submitted to the IETF for standardization, and the following year the QUIC Working Group was established. A growing number of contributors from the corporate, academic, nonprofit sector have joined the protocol development work since, and what has been achieved to date is the result of a notable and labor-intensive collaborative effort.

So, on one hand, the history of QUIC shows that permissionless innovation is still possible. On the other hand, it also shows what remarkable efforts and resources are needed to carry out such an ambitious project. While permissionless innovation still exists, the threshold and costs for innovation seem to rise significantly and increasingly.

Also, a look at the actors and dynamics involved in QUIC's history should not underestimate the power of Google's authority. A different developing actor might have been able to invest a similar amount of resources into the development of a protocol. Still, without an impressive user base and traffic stream as Google's, they might have received a less supportive response from network operators.

Having said that, it is expected that QUIC will improve the current situation by providing a more capable transport which aims to overcome ossification and allow for changes in the protocol due to its modularity.

4.15.3. Privacy, Power and Consolidation

The most relevant privacy advantage provided by QUIC is gained by users who have different kinds of traffic relations with one end point. In fact, QUIC does not allow network providers to easily differentiate between, for instance, HTTP requests, DNS requests and real time voice packets, thus strengthening user privacy, and also improving performance. It is important to note, though, that QUIC does not actually hide or attempt to hide the application protocol being used on a connection. The ALPN offered by the client is protected only by a key which can be calculated by any party who can work with the QUIC version in use.

On the other hand, this creates a concentration of different kinds of traffic with one end point, thus giving the service provider access to more categories of privacy sensitive information.

In the current reality of the Internet, the biggest hosts are controlled by large, consolidated, transnational corporations. This creates an extreme power differential between end users on the one hand, and service providers and content operators on the other hand.

In order to protect privacy and secure information, it is important that the user makes a careful and informed decision about the hosting provider and plan they choose.

While ubiquitous encryption changes the relation between service providers and content operators, placing them at the same end of the spectrum, it remains to be seen whether if it can help users take and retain control within the overall power structures of Internet governance and economics.

One of the problems with deploying fully encrypted protocols like QUIC is that deployment is far easier for organizations that already have integrated observability, traceability, and tooling in their back-ends, which not surprisingly happen to be the big players.

If there was any chance to make running a QUIC server relatively easy, thus enabling a greater diversification of end points, QUIC could contribute to a power shift in favor of the end user.

However, running a QUIC infrastructure is currently expected to be more demanding than running a HTTP/2 or HTTP/1 infrastructure. It would be truly compelling if this consideration could be discussed further, and ideally addressed by the development and release of openly available tooling allowing for more accessible ways to run a QUIC server.

4.15.4. Transparency and IoT

End-to-end encryption on the transport layer makes monitoring and filtering of the traffic more complex, and can lead to the adoption of other network management practices to obtain this information.

This has implications on the management of Internet of Things (IoT) devices. If an IoT device adopts QUIC, it will be harder for the user who owns the device to monitor what data is communicated with third parties. It would also be more difficult to conduct research into the promulgation of malware, cookies and other artefacts.

Adequate tooling to protect the right to privacy of IoT users has not yet been developed.

5. Conclusions and Recommendations

The QUIC protocol provides significant human rights improvements for end users.

It dramatically improves connectivity for users on high-loss, high-latency connections. Users will benefit from lower latencies and will not need to restart sessions as often. And in those cases in which they will need to restart a session, they will able to do so without having to re-do the initial handshake.

Another key improvement is represented by the use of encryption by default, which provides authentication, stream integrity, adaptability of the protocol by overcoming ossification, and improved protection from third party monitoring and metadata analysis.

The following is a list of potential improvements that we invite the QUIC Working group to take into consideration, wishing for the protocol to have even greater positive implications for human rights.

- As the QUIC Working Group is expected to deliberate on the potential inclusion of the spin bit in the main specification of the protocol at the upcoming IETF103 (November 3-9, 2018), we suggest to consider not to include it. Our recommendation is motivated by the concerns raised in regards to its implications on user privacy, as reported in this very document, and also shared by some of the interviewees.

- Consider deploying IP header encryption as an optional extension.

- Evaluate the addition of language tagging and charset identification in the case of Reason Phrase in the CONNECTION_CLOSE and APPLICATION_CLOSE.

- Examine the opportunity to translate the QUIC specification into other languages.

- Discuss the viability to make tooling for running QUIC servers openly available.

- Observe and iteratively assess the implications of QUIC on the power relations between end user on one end of the spectrum, and network operators and service providers on the other one.

6. Acknowledgements

The authors thank (in alphabetical order) Mike Bishop, Janardhan Iyengar, Daniel Kahn Gillmor, Mirja Kuehlewind, Mark Nottingham, Martin Thomson, and Brian Trammell for their generous contribution to our research and review. This document does not necessarily reflect their opinion, but solely that of the authors.

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. Review Team Information

The discussion list for the Human Rights Review Team is located at the e-mail address hr-rt@irtf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hr-rt [2]

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

10. References

10.1. Informative References

[Behretal]
Behr, M. and I. Swett, "Introducing QUIC Support for HTTPS Load Balancing", June 2018, <https://cloudplatform.googleblog.com/2018/06/Introducing-QUIC-support-for-HTTPS-load-balancing.html>.

[Cuietal] Cui, Y., Li, T., Liu, C., Wang, X., and M. Kuehlewind, "Innovating Transport with QUIC: Design Approaches and Research Challenges", IEEE Internet Computing, Vol 21(2), pp. 72-76 , March 2017, <https://mami-project.eu/wp-content/uploads/2017/03/QUIC.pdf>.

[draft-huitema-quic-dnsoquic-05]
Huitema, C., Shore, M., Mankin, A., Dickinson, S., and J. Iyengar, "Specification of DNS over Dedicated QUIC Connections (work in progress)", June 2018, <https://tools.ietf.org/html/draft-huitema-quic-dnsoquic-05>.

[draft-huitema-quic-mpath-req-01]
Huitema, C., "QUIC Multipath Requirements (work in progress)", January 2018, <https://tools.ietf.org/html/draft-huitema-quic-mpath-req-01>.

[draft-ietf-quic-invariants-01]
Thomson, M., "Version-Independent Properties of QUIC (work in progress)", March 2018, <https://tools.ietf.org/html/draft-ietf-quic-invariants-01>.

[draft-ietf-quic-spin-exp-00]
Trammell, B. and M. Kuehlewind, "The QUIC Latency Spin Bit (work in progress)", April 2018, <https://tools.ietf.org/html/draft-ietf-quic-spin-exp-00>.

[draft-ietf-quic-tls-12]
Thomson, M. and S. Turner, "Using Transport Layer Security (TLS) to Secure QUIC (work in progress)", May 2018, <https://tools.ietf.org/html/draft-ietf-quic-tls-12>.

[draft-ietf-quic-transport-12]
Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport (work in progress)", May 2018, <https://tools.ietf.org/html/draft-ietf-quic-transport-12>.

[draft-joseph-quic-comparison-quic-sctp-00]
Joseph, A., Li, T., He, Z., Cui, Y., and L. Zhang, "A Comparison Between SCTP and QUIC (work in progress)", March 2018, <https://tools.ietf.org/html/draft-joseph-quic-comparison-quic-sctp-00>.

[FIArch] Future Internet Architecture (FIArch) Group, "Future Internet Design Principles", January 2012, <https://pdfs.semanticscholar.org/0f33/5e6df68193367b0d0ea5430c043919477508.pdf>.

[Gratzer] Gratzer, F., ""QUIC - Quick UDP Internet Connections"", Seminar Innovative Internet-Technologien und Mobilkommunikation SS2016 , 2016, <https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2016-09-1/NET-2016-09-1_06.pdf>.

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

[Huston] Huston, G., "Just One QUIC Bit", APNIC , March 2018, <https://blog.apnic.net/2018/03/28/just-one-quic-bit/>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", December 1966, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

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

[Kuehlewindetal] Kuehlewind, M., Buehler, T., Trammell, B., Neuhaus, S., Muentener, R., and G. Fairhurst, "A Path Layer for the Internet: Enabling Network Operations on Encrypted Protocols", IEEE International Conference on Network and Service Management (CNSM) , November 2017, <https://nsg.ee.ethz.ch/fileadmin/user_upload/CNSM_2017.pdf>.

[MolaviKakhkietal] Molavi Kakhki, A., Jero, S., Choffnes, D., Nita-Rotaru, C., and A. Mislove, "Taking a Long Look at QUIC", Proceedings of IMC ’17, London, United Kingdom , November 2017, <https://david.choffnes.com/pubs/long-look-at-quic-imc17.pdf>.

[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>.

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

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[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>.

[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>.

[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>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[RFC6582] Henderson, T., Floyd, S., Gurtov, A., and Y. Nishida, "The NewReno Modification to TCP's Fast Recovery Algorithm", RFC 6582, DOI 10.17487/RFC6582, April 2012, <https://www.rfc-editor.org/info/rfc6582>.

[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>.

[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>.

[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>.

[RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of Pervasive Encryption on Operators", RFC 8404, DOI 10.17487/RFC8404, July 2018, <https://www.rfc-editor.org/info/rfc8404>.

[Trammell01] Trammell, B., "Explicit Passive Measurability and the QUIC Spin Bit", APNIC , May 2018, <https://blog.apnic.net/2018/05/11/explicit-passive-measurability-and-the-quic-spin-bit/>.

[Trammell02] Trammell, B., "And Yet, It Spins", March 2018, <https://trammell.ch/post/2018-03-29-and-yet-it-spins>.

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

[Wilketal] Wilk, A., Hamilton, R., and I. Swett, "A QUIC Update on Google's Experimental Transport", April 2015, <https://blog.chromium.org/2015/04/a-quic-update-on-googles-experimental.html>.

[Ziewitzetal] Ziewitz, M. and I. Brown, "A Prehistory of Internet Governance", Research Handbook on Governance of the Internet, ed I. Brown, 3-26. Cheltenham: Edward Elgar , 2013.

10.2. URIs

[1] mailto:hr-rt@irtf.org

[2] https://www.irtf.org/mailman/listinfo/hr-rt

[3] https://www.irtf.org/mail-archive/web/hr-rt/current/index.html

Authors' Addresses

Beatrice Martini
Harvard Kennedy School

EMail: mail@beatricemartini.it

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net