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.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

1 Introduction ........................................ 4  
2 Content Filtering by States and Public Authorities .......... 5  
   2.1 Filtering to Prevent Freedom of Assembly or Information . 6  
   2.2 Filtering to Enforce Cultural Norms ...................... 6  
   2.3 Filtering to Prevent Violence .......................... 7  
   2.4 Child Pornography .................................. 7  
   2.5 Unauthorized Gambling and Illegal E-Commerce .......... 7  
   2.6 User Generated Content (UGC) ........................ 8  
3 Content Filtering by Internet Service Providers .......... 8  
   3.1 Filtering for Network and Computer Security .......... 9  
   3.2 Filtering on Behalf of the User ..................... 9  
   3.3 Filtering for Commercial Reasons ................... 10  
4 Content Filtering by Platforms Providing Content and Services 10  
   4.1 Enforcing Cultural Norms ............................ 11  
   4.2 Blocking Extremist Activity .......................... 12  
   4.3 Blocking Activity Inciting Violence ................... 13  
   4.4 Copyright Protection ............................... 13  
   4.5 Filtering for Network and Computer Security .......... 14  
   4.6 Content Filtering by End-Users ..................... 14  
5 Security Considerations ................................ 14  
6 IANA Considerations .................................... 14  
7 References ............................................. 15  
   7.1 Normative References ............................... 15  
   7.2 Informative References ............................. 15  
Authors’ Addresses ..................................... 16
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 censorn 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


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
Abstract

This document establishes the causal link 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 forum, it provides a global public space despite being built on predominantly private infrastructure. Since Internet protocols play a central role in the management, development and use of the Internet, the relation between protocols and the aforementioned rights should be analyzed and any adverse impacts should be mitigated.

Status of This Memo

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

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

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

This Internet-Draft will expire on August 23, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document.
1.  Introduction

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

The Internet is constantly shaping modern information societies by providing a socio-technical ordering. In other words, the Internet infrastructure and architecture consist of social and technological arrangements [StarRuhleder]. Such ordering is not always apparent because infrastructure is often taken for granted by those using it. It tends to hide itself in the societal woodwork [Mosco], or put
otherwise: ’The most profound technologies are those that disappear’ [Weiser].

Infrastructure therefore is mostly known by an epistemic community of experts [Haas] and only gets recognized by the larger public when it fails. As the Internet grows, decisions made about its architecture are become more important. [RFC8280] established the relationship between human rights and Internet protocols. Following the same methodology, we now seek to uncover the relation between the right to assembly, association and the Internet infrastructure.

One one hand, the right to freedom of assembly and association protects collective expression. Likewise, systems and protocols that enable communal interactions between people and servers allow this right to prosper given that the Internet itself was originally designed as "a medium of communication for machines that share resources with each other as equals" [NelsonHedlun].

The current draft continues the work started in [RFC8280] by investigating the exact impact of Internet protocols on specific human rights, namely the right to freedom of assembly and association, in order to mitigate potential negative impacts.

2. Vocabulary used

Architecture  The design of a structure

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

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

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


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

How does the architecture of the internet enable and/or inhibit the right to freedom of assembly and association?

4. Methodology

The point of departure of the present work is [RFC8280] - an initial effort to establish the relationship between human rights and the Internet architecture, specifically protocols and standards. As
such, [RFC8280] was inductive and explorative in nature, and it ultimately established either causal or deterministic relationships between aforementioned concepts through a series of case studies.

The methodology was based on process tracing, semi-structured interviews and quantitative and qualitative document analysis which has been further validated through confirmatory research in the form of Human Rights Protocol Reviews. The causal relationship, proposed as a hypothesis in [RFC8280] says that there is an inherent relationship between protocols, the Internet architecture, and human rights. The guidelines in [RFC8280] 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.

Taking into consideration the international human rights framework regarding freedom of assembly and association, the present document seeks to deepen the relationship between the Internet architecture, protocols, and standards without creating new guidelines. In that way, we continue the work proposed in [RFC8280] and follow the primary aim 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'. Even though the present work does not seek to create new guidelines, the conclusions could inform the development of new guidelines such as is done in draft-irtf-hrpc-guidelines.

Given that our current research proposition is that "the Internet infrastructure significantly impacts the ability of people to exercise the human rights to freedom of association and assembly", we therefore aim to test the causal relationship through a case-selection method, where we have adopted a purposive sampling approach, aimed at the typicality and paradigmatic nature of the cases [SeawrightGerring] to help us achieve an attempt at an ethnography of infrastructure [Star]. Subsequently we analyze the cases through the theoretical framework provided in the literature review and based on that provide recommendations based on the findings.

5. Literature Review

The right to freedom of assembly and association protects and enables collective action and expression [UDHR] [ICCPR]. It’s purpose is to ensure that everyone in a society has the opportunity to express opinions they hold in common with others. As such, it is a tool that facilitates dialogue among citizens, as well as with political
leaders or governments [OSCE]. In a democracy, causes and opinions are more widely heard when a group of people come together behind the same cause or issue [Tocqueville].

In international law, the 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. What constitutes a definition of "peaceful" is outside the scope of the present document.

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.

Even if privacy and freedom of expression are the most discussed human rights when it comes to the online world, the right to freedom of assembly and association is quintessential for the Internet. 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 a 'open global community' of network designers, operators, vendors, and researchers is also protected by freedom of assembly and association [RFC3233]. Discussions, comments
and consensus around RFCs are possible because of the collective expression that freedom of association and assembly allow. The very word "protocol" found its way into the language of computer networking based on the need for collective agreement among network users [HafnerandLyon].

We are aware that some of 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, given that protocols are a part of the socio-technical ordering of reality, we do recognize that in some cases the line between them and applications, implementations, policies and offline realities are often blurred and hard—if not impossible—to differentiate.

6. Cases and examples

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 also indicate, per case, the interrelation with issues in [RFC8280].

6.1. Conversing

An interactive conversation between two or more people forms the basis to organize and associate. According to Anderson "the relationship between political conversation and engagement in the democratic process is strong." [Anderson]. A conversation is inherently of social nature. Therefore, by these definitions the core of the "political" is essentially assembly or association: a basis for the development of social cohesion in society.

6.1.1. Mailing Lists

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

In 1971, four years after the invention of email, the first mailing list was created to talk about the idea of using Arpanet for discussion. What had initially propelled the Arpanet project forward
as a resource sharing platform was gradually replaced by the idea of a network as a means of bringing people together [Abbate]. More than 45 years after, mailing lists are pervasive and help communities to engage, have 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 [APC].

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. Furthermore, the archival function of mailing lists allows for posterior accountability and analysis. The downsides of mailing lists are similar to the ones generally associated with e-mail, except that end-to-end encryption such as OpenPGP [RFC4880] and S/MIME [RFC5751] are not possible because the final recipients are not known. There have been experimental solutions to address this issue such as Schleuder [Schleuder], but this has not been standardized or widely deployed.

This case relates to the following considerations in [RFC8280]: - Security - Privacy - Decentralization - Censorship Resistance - Open Standards - Confidentiality

6.1.2. Multi-party video conferencing

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 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.

This case relates to the following considerations in [RFC8280]: -
Security - Privacy - Decentralization - Censorship Resistance - Open
Standards - Anonymity - Confidentiality

6.1.3. Internet Relay Chat

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

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

IRC servers may deploy different policies for the ability of users to
create their own channels or 'rooms', and for the delegation of
'operator'-rights in such 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.
This case relates to the following considerations in [RFC8280]: -
Security - Privacy - Censorship Resistance

6.2. Peer-to-peer networks and systems

At the organizational level, peer production is one of the most
relevant innovations from Internet mediated social practices.
According to [Benkler] 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, Benkler 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." [Benkler] To ensure that the knowledge
generated is available for free use, commons-based projects are often
shared under an open license.

6.2.1. Peer-to-peer system architectures

Peer-to-peer (P2P) is essentially a model of how people interact in
real life because "we deal directly with one another whenever we wish
to" [Vu]. Usually if we need something we ask our peers, who in turn
refer us to other peers. In this sense, the ideal definition of P2P
is that "nodes are able to directly exchange resources and services
between themselves without the need for centralized servers" where
each participating node typically acts both as a server and as a
client [Vu]. RFC 5694 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]

This case relates to the following considerations in [RFC8280]: - Security - Privacy - Decentralization - Censorship Resistance - Open Standards - Anonymity - Heterogeneity Support - Integrity - Authenticity - Adaptability

6.2.2. Version control

Ever since developers needed to collaboratively write, maintain and discuss large code basis for the Internet there have been different approaches of doing so. The easiest approach has been discussing code through mailing lists even though this has proven to be hard when maintaining the most recent versions, which is why version control systems ultimately make sense.

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

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

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

This case relates to the following considerations in [RFC8280]: - Security - Decentralization - Open Standards - Heterogeneity Support - Integrity - Authenticity - Adaptability

6.3. Grouping together (identities)

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

6.3.1. DNS

Domain names allow hosts to be identified by human parsable information. Whereas an IP address might not be the expression of an identity, a domain name can be and often is. The grouping of certain identities under specific domains or even Top Level Domains are risky: connecting an identity to a hierarchically structured
identifier systems creates a central attack surface which allows for an easier surveillance of the services running on the domain, domain based censorship [RFC7754], or impersonation of the domain through DNS cache poisoning. The use of a centralized authority always makes censorship through a registry or registrar possible, as well as by using a fake resolver or using proposed standards such as DNS Response Policy Zones [RPZ]. Several technologies have been developed in the IETF to mitigate these risks such as DNS over TLS [RFC7858], DNSSEC [RFC4033], DNS over HTTPS [RFC8484]. When these mitigations are implemented, censorship will not be made impossible but it will be made visible.

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

This case relates to the following considerations in [RFC8280]: - Security - Privacy - Decentralization - Censorship Resistance - Anonymity - Heterogeneity Support - Integrity - Authenticity - Adaptability - Outcome Transparency

6.3.2. Autonomous Systems

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

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

In practice, the user must accept policies of ASes he has no relationship with, and didn’t choose. For instance, there is no way to direct the packets to avoid the Five Eyes, not even to know after the fact where the packet went. [FiveEyes] [SchengenRouting] (Traceroutes give you an idea but the path may change before and after the traceroute.) Given that it is not trivial for an edge-user...
to operate an AS and engage in peering relation with other ASes, there might not be another way for the edge-user to connect to the network of networks. In this case, users are forced into accepting the policies of a specific network. Such design, combined with the increased importance of the Internet to make use of basic services, forces edge-users to associate with a specific network without consenting—or even knowing—the policies of the network.

Additionally, it can be noted that there is no standard and deployed way for the edge-user to choose the routes her packets will go through. [RFC0791] section 3.1 standardized "source routing" and "record route" but neither were deployed, mainly because of serious security issues.

This case relates to the following considerations in [RFC8280]: - Security - Privacy - Decentralization - Censorship Resistance - Anonymity - Heterogeneity Support - Integrity - Authenticity - Adaptability - Outcome Transparency

7. Discussion: Establishing the relation

The case studies show that the Internet infrastructure, the combination of architecture and protocols, facilitates freedom of association and assembly, by allowing groups of people to converse, collaborate, exchange, and build and maintain identities in both structural and occasional manners. The structural forms of group activities are more related to freedom of association, whereas freedom of assembly often has a more incidental nature. The difference between the two, as mentioned, is a gradual one. This is equally true to the infrastructural mediations of these rights.

Whereas we established that the Internet infrastructure facilitates freedom of association and assembly, by its very technical and material nature, it both creates and limits the spaces for it. This is an interesting tension because juridically only lawful limitations to the rights are allowed, and even then only if they are necessary, and proportionate. This exposes legal implications of the characteristics of the Internet infrastructure.

These preliminary finding suggest that the properties and characteristic through which the Internet infrastructure enables and inhibits freedom of assemblies and association should also be analyzed from a legal lens. The case studies have pointed out several caveats in implementations, that might not necessarily be understood by people while exercising their right to association of assembly, and which thus should either be mitigated, or at least, be communicated to the rights holders.
8. Discussion: Protocols and Platforms

Whereas the Internet is a network of networks, and can therefore be understood as an assembly, applications on top of the Internet do not necessarily inherit the same structure. Quite the opposite, the Internet increasingly becomes a vehicle for commercial, proprietary and non-interoperable platforms. This lack of interoperation is harming the ability of people to set or negotiate their own terms on which they would like to assemble or associate, or host their own interoperating services.

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

Often these non-interoperable platforms are built on open-protocols but do not allow for inter-operability or data-portability. In the case of large private platforms, this in turn leads to strong network externalities also know as a network effect; because the users are there, users will be there. Even though social-media platforms have enabled groups to associate, they have also led to a 'tactical freeze' because of the inability to change the platforms [Tufekci].

Whereas these networks are a ready-to-hand networked public sphere, they do not allow their inhabitants to change or fully understand their workings. In a near future, this could potentially impact infrastructure itself and the distributed nature of the Internet [RFC1287].

9. Conclusions

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

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

10. 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.
11. Security Considerations

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

12. IANA Considerations

This document has no actions for IANA.

13. 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]

14. References

14.1. Informative References


14.2. URIs

[1] mailto:hrpc@ietf.org


Authors’ Addresses

Niels ten Oever
University of Amsterdam
EMail: mail@nielstenoeever.net

Gisela Perez de Acha
Derechos Digitales
EMail: gisela@derechosdigitales.org
Guidelines for Human Rights Protocol and Architecture Considerations
draft-irtf-hrpc-guidelines-03

Abstract

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

Status of This Memo

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

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

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

This Internet-Draft will expire on December 9, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

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

1. Introduction .............................................. 3
2. Vocabulary used ......................................... 3
3. Guidelines for developing human rights protocol considerations .......................... 3
   3.1. Human rights threats ................................... 3
   3.2. Conducting human rights reviews ......................... 5
      3.2.1. Analyzing drafts based on guidelines for human rights considerations model ........................................ 5
      3.2.2. Analyzing drafts based on their perceived or speculated impact ........................................ 5
      3.2.3. Expert interviews .................................... 5
      3.2.4. Interviews with impacted persons and communities ........ 6
      3.2.5. Tracing impacts of implementations ..................... 6
   3.3. Guidelines for human rights considerations .................. 6
      3.3.1. Connectivity ........................................ 7
      3.3.2. Privacy ............................................. 7
      3.3.3. Content agnosticism ................................ 8
      3.3.4. Security ............................................. 8
      3.3.5. Internationalization ................................ 9
      3.3.6. Censorship resistance ................................ 10
      3.3.7. Open Standards ....................................... 11
      3.3.8. Heterogeneity Support ................................. 12
      3.3.9. Pseudonymity ......................................... 13
      3.3.10. Accessibility ........................................ 14
      3.3.11. Localization .......................................... 15
      3.3.12. Decentralization ..................................... 15
      3.3.13. Reliability .......................................... 16
      3.3.14. Confidentiality ...................................... 17
      3.3.15. Integrity ........................................... 18
      3.3.16. Authenticity ........................................ 19
      3.3.17. Adaptability ........................................ 20
      3.3.18. Outcome Transparency ................................ 20
      3.3.19. Anonymity ........................................... 21
4. Document Status ............................................ 22
5. Acknowledgements .......................................... 22
6. Security Considerations .................................... 23
7. IANA Considerations ........................................ 23
8. Research Group Information .................................. 23
9. References ................................................ 23
   9.1. Informative References ................................ 23
   9.2. URIs .................................................. 28
Authors’ Addresses ............................................. 28
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 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 extrajudicial 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 rightsholder, 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 Standard might benefit from a documented discussion of potential human rights risks arising from potential misapplications of the protocol or technology described in the RFC. This might be coupled with an Applicability Statement for that RFC.

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

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]. The end-to-end principle is important for the robustness of the network and innovation. Such robustness of the network is crucial to enabling human rights like freedom of expression.

Example: Middleboxes (which can be Content Delivery Networks, Firewalls, NATs or other intermediary nodes that provide '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." {{W3Cill8nDef}}

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.

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 an 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.
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

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 for work on [RFC8280].
- Theresa Engelhard, Joe Hall, Avri Doria and the hrpc list for reviews and suggestions.
- The Human Rights Review Team for implementing and improving the guidelines.
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


9.2. URIs

[1] mailto:hrpc@ietf.org


Authors’ Addresses

Niels ten Oever
University of Amsterdam
EMail: mail@nielstenoever.net

Gurshabad Grover
Centre for Internet and Society
EMail: gurshabad@cis-india.org
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. 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 undisputed that standards and protocols are both products of a political process, and they can also be used for political means.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 18, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

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

- Michel Callon

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

-{{RFC3935}}
The design of the Internet through protocols and standards is a technical issue with great political and economic impacts [RFC0613]. The early Internet community already realized that it needed to make decisions on political issues such as intellectual property; internationalization [BramanI]; diversity; access [RFC0101]; privacy and security [RFC0049]; and the military [RFC0164] [RFC0316], governmental [RFC0144] [RFC0286] [RFC0313] [RFC0542] [RFC0549] and non-governmental [RFC0196] uses of the network. This has been clearly pointed out by Braman [BramanII].

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 also shaped by the affordances of the technology. Companies, citizens, governments, standards development bodies, public opinion and public interest groups all play a part in these discussions. In this document we aim to outline different views on the relation between standards and politics, and seek to answer the question of whether standards are political, and if so, how.

2. Vocabulary Used

Politics (from Greek: 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 that invites specific kinds of behavior, and in that process shapes it.

3. Research Question

Are protocols political?
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 [RFC1097]. 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 valutative 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 requires that each protocol and use be evaluated for its political dimension, in order to understand the extent to which it is political.

4.3. All protocols are political sometimes

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

4.4. The network has its own logic and values

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

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

In the same way - in another and more recent example - the very existence 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 creates its own paths, but also has its own objective. According to this view the goal of the network is interconnection and connectivity; more connectivity is good for the network. Proponents of this positions also often describe the Internet as an organism with its own unique ecosystem.

In this position it is not necessarily clear where the ‘social’ ends and the ‘technical’ begins, and it could be argued that the distinction itself is a social construction [BijkerLaw] or that a real-life distinction between the two is hard to 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, different media have different intellectual and emotional biases;

(2) because of the accessibility and speed of their information, different media have different political biases;

(3) because of their physical form, different media have different sensory biases;

(4) because of the conditions in which we attend to them, different media have different social biases;

(5) because of their technical and economic structure, different media have different content biases.

Recent scholars of Internet infrastructure and governance have also pointed out that Internet processes and standards have become part and parcel of political processes and public policies. Several concrete examples are found within this approach, for instance, the IANA transition or global innovation policy [DeNardis]. The Raven process in which the IETF refused to standardize wiretapping – which
resulted in [RFC2804] - was an instance where an international governance body took a position that was largely political, although driven by a technical argument. The process that led to [RFC6973] is similar: the Snowden disclosures, which occurred in the political space, engendered the IETF to act. This is summarized in [Abbate] who says: "protocols are politics by other means," emphasizing the interests that are at play in the process of designing standards.

This position further holds that protocols can never be understood without their contextual embeddedness: protocols do not exist solely by themselves but always are to be understood in a more complex context - the stack, hardware, or nation-state interests and their impact on civil rights. Finally, this view is that 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 create a consumer class to use the technology "with new practices, relationships, and identities supplanting the old, -- and those who had the wherewithal to implement new technologies often molded society to match the needs of emerging technologies and organizations." [Winner].

5. IETF: Protocols as Standards

In the previous section we gave an overview of the different existing positions of the impact of Internet protocols in the Internet protocol community. In the following section we will review the standards setting process and its consequences for the politics of protocols, through the lens of existing literature on standards setting.

Standards enabling interoperating networks, what we think of today as the Internet, were created as open, formal and voluntary standards. A platform for Internet standardization, the Internet Engineering Task Force (IETF), was created in 1986 to enable the continuation of such standardization work. The IETF has sought to make the standards process transparent (by ensuring everyone can access standards, mailing-lists and meetings), predictable (by having clear procedures and reviews) and of high quality (by having draft documents reviewed by experts from its own community). This is all aimed at increasing the accountability of the process and the quality of the standard.

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

5.1. Competition and collaboration

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

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

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

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

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

5.2. How voluntary are open standards?

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

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

6. Conclusion

Economics, competition, collaboration, openness, and political impact
have been an inherent part of the work of the IETF since its early
beginnings. The IETF cannot ordain which standards are to be used on
the networks, and it specifically does not determine the laws of
regions or countries where networks are being used, but it does set
open standards for interoperability on the Internet, and has done so since the inception of the Internet. Because a standard is the blueprint 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, it is undisputed that standards and protocols are both products of a political process, and they can also be used for political means. Therefore protocols and standards are not ‘value-neutral, and neither is the IETF’ [RFC3935]. Thus we can answer the research question ‘are protocols political’ in affirmative fashion.

Further research could explore how the political nature 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. Acknowledgements

Thanks to Michael Rogers, Joe Hall, Andrew Sullivan, Brian Carpenter, Mark Perkins and all contributors and reviewers on the hrpc mailinglist. Special thanks to Gisela Perez de Acha for some thorough editing rounds, and Amelia Andersdotter for significant text contributions.
10. Research Group Information

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

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

11. References

11.1. Informative References


11.2. URIs

[1] mailto:hrpc@ietf.org


Author’s Address

Niels ten Oever  
University of Amsterdam  

EMail: mail@nielstenoever.net
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

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

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

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

This Internet-Draft will expire on April 25, 2019.

Copyright Notice

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

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

Table of Contents

1. Introduction ............................................. 3
2. Vocabulary Used .......................................... 3
3. Review Methodology and Process ............................ 5
4. Human Rights Considerations ............................... 7
   4.1. Connectivity ......................................... 7
       4.1.1. Latency ........................................ 7
       4.1.2. Congestion Control and Loss Recovery .......... 8
       4.1.3. Reduced Head-Of-Line Blocking ................. 8
       4.1.4. Resources ...................................... 8
   4.2. Privacy ............................................... 8
       4.2.1. Encryption ...................................... 8
       4.2.2. Transparent Proxying ............................ 9
       4.2.3. Multiple Streams ................................ 9
       4.2.4. Packet Number Encryption ....................... 9
       4.2.5. Padding ......................................... 10
       4.2.6. Lawful Intercept ................................ 10
       4.2.7. Spin Bit ........................................ 10
       4.2.8. Packet Injection ................................ 11
   4.3. Content Agnosticism ................................... 12
   4.4. Security .............................................. 12
   4.5. Internationalization .................................. 12
   4.6. Censorship Resistance ................................. 12
   4.7. Open Standards ....................................... 13
   4.8. Heterogeneity Support ................................. 13
   4.9. Anonymity ............................................. 13
   4.10. Pseudonymity ........................................ 13
   4.11. Confidentiality ...................................... 14
   4.12. Integrity ............................................ 14
   4.13. Authenticity ........................................ 14
   4.15. Outcome Transparency ................................ 14
       4.15.1. Encryption .................................... 15
       4.15.2. Permissionless Innovation and Its Challenges ........................................ 15
       4.15.3. Privacy, Power and Consolidation ............ 16
       4.15.4. Transparency and IoT ............................ 17
   5. Conclusions and Recommendations ....................... 18
6. Acknowledgements .......................................... 19
7. Security Considerations ................................... 19
8. IANA Considerations ....................................... 19
9. Review Team Information ................................... 19
10. References ............................................... 19
    10.1. Informative References ............................... 19
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


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. [Behrelal]

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 [Trammell10].
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 ensures 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.


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]


10.2. URIs

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


Authors’ Addresses

Martini & ten Oever  Expires April 25, 2019