

Human Rights Protocol Considerations Research Group N. ten Oever
Internet-Draft University of Amsterdam
Intended status: Informational G. Perez de Acha
Expires: 8 September 2022 Derechos Digitales
S. Couture
Université de Montréal
M. Knodel
Center for Democracy & Technology
7 March 2022

Freedom of Association on the Internet
draft-irtf-hrpc-association-09

Abstract

This document explores whether there is a relation between the Internet architecture and the ability of people to exercise their right to peaceful assembly and the right to association online. It does so by asking the question: what are the protocol development considerations for freedom of assembly and association? The Internet increasingly mediates our lives, our relationships, and our ability to exercise our human rights. As a global assemblage, the Internet provides a public space, yet it is predominantly built on private infrastructure. Since Internet protocols and architecture play a central role in the management, development, and use of the Internet, we analyze the relation between protocols, architecture, and the rights to assemble and associate to mitigate infringements on those rights. This document concludes that the way in which infrastructure is designed and implemented impacts people's ability to exercise their freedom of assembly and association. It is therefore recommended that the potential impacts of Internet technologies should be assessed, reflecting recommendations of various UN bodies and norms. Finally, the document remarks that non-interoperable platforms that do not allow for interoperability or data-portability, render 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.

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 8 September 2022.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Vocabulary used	4
3. Research question	5
4. Methodology	5
5. Literature Review	6
5.1. FAA definition and core treaties	6
5.2. FAA in the digital era	9
5.3. Specific questions raised from the literature review . .	13
6. Analysis	13
6.1. Got No Peace: Spam and DDoS	14
6.1.1. Spam	15
6.1.2. DDoS	16
6.2. Holistic Agency: Mailing Lists and Spam	16
6.2.1. Mailing lists	16
6.2.2. Spam	17
6.3. Civics in Cyberspace: Messaging, Conferencing, and Networking	17
6.3.1. Email	18
6.3.2. Mailing lists	18
6.3.3. IRC	18
6.3.4. WebRTC	19
6.3.5. Peer-to-peer networking	20
6.4. Universal Access: The Web	21
6.5. Block Together Now: IRC and Refusals	22

7. Conclusions: Can we learn anything from the previous case studies?	23
8. Acknowledgements	24
9. Work Space	25
10. Security Considerations	25
11. IANA Considerations	25
12. Research Group Information	25
13. Informative References	25
Authors' Addresses	33

1. Introduction

We shape our tools and, thereafter, our tools shape us.

- John Culkin (1967)

Article 21 of the Covenant protects peaceful assemblies wherever they take place: outdoors, indoors and online; in public and private spaces; or a combination thereof.

- General Comment 37 of the Human Rights Committee (2020)

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

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

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

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

2. Vocabulary used

Architecture The design of a structure

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

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

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

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

Connectivity The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958]. Different types of connectivity are further specified in [RFC4084]. The combination of the end-to-end principle, interoperability, distributed architecture, resilience, reliability and robustness are the enabling factors that result in connectivity to and on the Internet.

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

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

Infrastructure Underlying basis or structure for a functioning society, organization or community. Because infrastructure is a precondition for other activities it has a procedural, rather than static, nature due to its social and cultural embeddedness

[PipekWulf] [Bloketal]. This means that infrastructure is always relational: infrastructure always develops in relation to something or someone [Bowker].

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

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

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

An emergent-process-driven thing that is born from the collections of the ASes that happen to be gathered together at any given time. The fact that they tend to interact at any given time means it is an emergent property that happens because they use the protocols defined at IETF.

Right to peaceful assembly 'The right of peaceful assembly protects the non-violent gathering by persons for specific purposes, principally expressive ones.¹ It constitutes an individual right that is exercised collectively.² Inherent to the right is thus an associative element.' [UNGC37]

Right to association 'The right and freedom of association encompasses both an individual's right to join or leave groups voluntarily, the right of the group to take collective action to pursue the interests of its members, and the right of an association to accept or decline membership based on certain criteria.' [FoAdef]

3. Research question

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

4. Methodology

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

methodology looks at some cases of Internet protocols that are relevant to the sub-questions highlighted in the literature review, and analyze how these protocols facilitate and inhibit the right to peaceful assembly and association.

5. Literature Review

5.1. FAA definition and core treaties

The rights to peaceful assembly and the freedom of association are defined and guaranteed in national law and international treaties, however, in this document we limit ourselves to international treaties. Article 20 of the Universal Declaration of Human Rights [UDHR] states that "Everyone has the right to freedom of peaceful assembly and association" and that "No one may be compelled to belong to an association". Article 23 further guarantees that "Everyone has the right to form and to join trade unions for the protection of his interests". In the International Covenant on Civil and Political Rights [ICCPR], article 21 stipulates that "The right of peaceful assembly shall be recognized" and that "No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others" while article 22 states that "Everyone shall have the right to freedom of association with others, including the right to form and join trade unions".

General Comment No. 37 on the right of peaceful assembly by the United Nations Human Rights Committee affirms that the right of peaceful assembly protects non-violent online gatherings: "associated activities that happen online or otherwise rely upon digital services [...] are also protected" [UNGCR37]. Interference with emerging communications technologies that offer the opportunity to assemble either wholly or partly online or play an integral role in organizing, participating in and monitoring physical gatherings are assumed to impede assemblies which are protected by this right. Moreover, any restriction on the 'operation of information dissemination systems' must conform with the tests for restrictions on freedom of expression (see below).

Other treaties are sometimes cited as the source and framework to the right to freedom of association and assembly. An example of this is Article 5 of the International Convention on the Elimination of All Forms of Racial Discrimination [CERD] which stipulates freedom of peaceful assembly and association should be guaranteed "without discrimination as to race, colour, national or ethnic origin"; Article 15 of the Convention on the Rights of the Child [CRC] which

recognises to child pending the restrictions cited above; and Article 21 of the Convention on the Rights of Persons with Disabilities [CRPD] which insist on usable and accessible formats and technologies appropriate for persons with different kinds of disabilities. The freedoms of peaceful assembly and association are also protected under regional human rights treaties: article 11 of the European Convention on Human Rights, articles 15 and 16 of the American Convention on Human Rights, article 10 and 11 of the African Charter on Human and Peoples' Rights.

From a more philosophical perspective, Brownlee and Jenkins [Stanford] make some interesting distinctions in particular regarding the concepts of association, assembly and interaction, deviating somewhat from what is established in interpretations of international human rights law. "Interaction" refers to any kind of interpersonal and often incidental engagements in daily life, like encountering strangers on a bus. Interaction is seen as a "prerequisite" for association. Assembly, according to Brownlee and Jenkins has a more political connotation and is often used to refer to activists, protesters, or members of a group in a deliberating event. The authors refer to association as more "persistent connections" and distinguish between intimate associations, like friendship, love, or family, and collective association like trade unions, commercial business, or "expressive associations" like civil rights organizations or LGBTQIA associations. For Brownlee and Jenkins [Stanford], the right to association is linked to different relative freedoms: permission (to associate or dissociate), claim-right (to oppose others interfering with our conduct), power (to alter the status of our association), immunity (from other people interfering in our right). Freedom of association thus refers both to the individual right to join or leave a group and to the collective right to form or dissolve a group.

Freedoms of association and peaceful assembly, however, are relative and not absolute. Excluding someone from an association based on its sex, race or other individual characteristic is also often contentious if not illegal. As mentioned above, international human rights law provides the framework for legitimate restrictions on these rights, as well as the right to privacy and the right to freedom of expression and opinion. Restrictions can be imposed by states, but only if this is lawful and proportionate. States must document how these limitations are necessary in the interests of national security or public safety, public order, the protection of public health or morals, or the protection of the rights and freedoms of others. Finally, states must also protect participants against possible abuses by non-state actors.

The Human Rights Committee explores a few restrictions related to associated activities online or reliant upon digital services, that are also protected under article 21, and stipulates that "States parties must not, for example, block or hinder Internet connectivity in relation to peaceful assemblies. The same applies to geotargeted or technology-specific interference with connectivity or access to content.". Additionally, "States should ensure that the activities of Internet service providers and intermediaries do not unduly restrict assemblies or the privacy of assembly participants." [UNGC37].

Interpreting international law, the right to freedom of peaceful assembly and the right to freedom of association protects any collective, gathered either permanently or temporarily for "peaceful" purposes, online and offline. 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. 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" [UNGA]. Association has a more formal and established nature and refer to a group of individuals or legal entities brought together in order to collectively act, express, promote, pursue, or defend a field of common interests [UNSRFOAA2012]. Think about civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, or foundations.

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

expression of a group is hampered, such as in protests or through Internet shutdowns, this both hampers other people's ability to receive the information of the group, and impact the right to assembly of the people who seek to express themselves as a group [Nyokabi].

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

5.2. FAA in the digital era

Before discussing freedom of association and assembly as it pertains to digital environments, we must first recognize that the United Nations Human Rights Council adopted resolutions on the promotion, protection and enjoyment of human rights on the Internet in 2012, 2014, 2016 and 2018, affirming and reaffirming "... that the same rights that people have offline must also be protected online ..." [UNHRC2018]. Therefore the digital environment is no exception to application of this right by any means. Various other resolutions and report have established the online applicability of the freedoms of association and assembly, most recently and authoritatively by the Human Rights Committee in General Comment 37 (2020) [UNG37]. The questions that remain, however, are how these rights should be conceptualized and implemented in different parts and levels of digital environments.

The right to freedom of assembly and association online is the subject of increasing discussions and analysis. Especially since social media played an important role in several revolutions in 2011, which has led to increasing and ever more sophisticated attacks by autocratic governments on online communities and other associational activities occurring on the Internet [RutzenZenn]. In 2016, the Council of Europe published a report, "Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet" [CoE] which noted that while the Internet and technologies are not explicitly mentioned in international treaties, these treaties nevertheless apply to "the online environment". The report argue the "Internet is the public sphere of the 21st century", something demonstrated by the fact that informal associations can be gathered at scale in a matter of hours on the Internet, and that digital communication tools often serve to facilitate, publicize or otherwise enable presential associations or assemblies, like a protest or demonstration. They note, on the other hand, the negative ways in which the Internet can also be used to promote or facilitate terrorism, urban violence and hate speech, thus insisting on the "extremely important and urgent"

need to fight online terrorist activities such as recruitment or mobilization, while at the same time respecting the right to peaceful assembly and association of other users. The report mentions the following examples that could be help further our reflection:

- * Instances of network shutdowns in the Arab Spring, to prevent people from organising themselves or assembling
- * California's Bay Area Rapid Transit (BART) shutdown of mobile phone service, to prevent potential property destruction by protesters and disruption of service
- * The wholesale blocking of Google as a violation of freedom of expression
- * Telus, a telecom company which blocked customers' access to websites critical of Telus during a Telecommunications Workers Union strike against it
- * The targeting of social media users who call for or organise protests though the Internet in Turkey's Gezi Park protests
- * Mass surveillance or other interferences with privacy in the context of law enforcement and national security
- * Use of VPNs (Virtual Private Networks) and the Tor network to ensure anonymity
- * Distributed Denial of Service attacks (DDoS) as civil disobedience.

In 2019 the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, notes the opportunities and challenges posed by digital networks to the rights to freedom of peaceful assembly and of association [UNSRFAA2019]. The report recommends that international human rights norms and principles should also be used as a framework "that guides digital technology companies' design, control and governance of digital technologies". The report states that "technical standards" in particular can affect the freedom of association and assembly, and makes some recommendations which could be relevant, including:

- * "[Undertake] human rights impact assessments which incorporate the rights to freedom of peaceful assembly and of association when developing or modifying their products and services,"
- * "increase the quality of participation in and implementation of existing multi-stakeholder initiatives,"

- * "collaborate with governments and civil society to develop technology that promotes and strengthens human rights,"
- * "support the research and development of appropriate technological solutions to online harassment, disinformation and propaganda, including tools to detect and identify State-linked accounts and bots," and
- * "adopt monitoring indicators that include specific concerns related to freedom of peaceful assembly and association."

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

1. Organization of protests. Internet and social media are enablers of protests, such as it was seen in the "Arab Spring". Some of these protests - like online petitions or campaigns - are similar to offline association and assembly, but other protest forms are inherent to the Internet capacity like hacking, DDOS and are subject to controversy within the Internet community, some people finding it legitimate, and others not.
2. Surveillance. While the Internet facilitates association, the association in turn leaves a lot of traces that can be used in turn for law enforcement but also for repressing political dissents. As they note, even the threat of surveillance can have deter facilitation.
3. Anonymity and pseudonymity can be useful protection mechanism for those who'd like to attend legitimate association without facing retribution. On the other hand, anonymity can be used to harm society, such as in online fraud or sexual predation.

Online association and assembly are the starting point of civic mass-mobilization in modern democracies, and even more so where physical gatherings have been impossible or dangerous [APC]. Throughout the world -from the Arab Spring to Latin American student movements and the #WomensMarch- the Internet has played a crucial role by providing means for the fast dissemination of information otherwise mediated by the press, or even forbidden by the government [Pensado]. According to Hussain and Howard the Internet helped to "build solidarity networks and identification of collective identities and goals, extend the range of local coverage to international broadcast networks" and as platform for contestation for "the future of civil society and information infrastructure" [HussainHoward]. The IETF itself, defined as an 'open global community' of network designers,

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

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

- * The expansion of DNS for generic namespace as an enabler of association for minorities. The paper argues that specifically the expansion of the DNS to allow for new generic Top Level Domains (gTLDs) can have negative impacts on freedom of association because of restrictive policies by some registries and registrars, on the other hand could gTLDs could also enable communities to build clearly identifiable spaces for association (such as .gay).
- * The impact of Distributed Denial of Service attacks on freedom of association. Whereas DDoS has been used as a tool for protest, in many cases this is infringing on other parties freedom of expression. Furthermore, often devices (such as IoT devices and routers) are inscribed in such DDoS attacks whereas the owner or user did not consent to this. Thus they do not have the possibility to exit this assembly. Therefore the draft concluded that that IETF "should try to ensure that their protocols cannot be used for DDoS attacks"
- * The impact of middleboxes on the ability of users to connect to the Internet and therefore their ability to exercise their right to freedom of association and assembly. Lack of connectivity can significantly impact freedom of assembly and association of a user. Especially if the user cannot retrieve the reason for their inability to connect, and if there thus is no possibility to for the user to have access to due process to dispute the lack of (secure or private) connectivity in general or to a specific service.

In June 2020, the United Nations High Commissioner for Human Rights concluded that technologies can be enablers of the exercise of FAA, but technology is also significantly used to interfere with the ability of people to exercise their right to freedom of association and assembly. Specifically, the report mentions network shutdowns, the usage of technology to surveil or crack down on protesters,

leading to human rights violations. This includes facial recognition technology, and the uses of other ways to violate the (group) privacy of people engaged in an assembly or association. The report makes it explicit that companies play a significant role enabling, for instance by developing, providing or selling the technology, but also by directly exercising these violations [UNHRC2020].

5.3. Specific questions raised from the literature review

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

1. Should protocols be designed to enable legitimate limitations on association in the interests of "national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others", as stated in the ICCPR article 21 [ICCPR]? Where in the stack do we care for FAA?
2. Can protocols facilitate agency of membership in associations, assemblies and interactions?
3. What are the features of protocols that enable freedom of association and assembly?
4. Does protocol development sufficiently consider usable and accessible formats and technologies appropriate for all persons, including those with different kinds of abilities?
5. Can a protocol be designed to legitimately exclude someone from an association?

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

6. Analysis

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 enables and/or inhibits such human rights, 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 how they facilitate freedom of assembly and association, or how they inhibit it through their design or implementation.

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

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

6.1. Got No Peace: Spam and DDoS

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

The 2020 report by the United Nations Special Rapporteur on Human Rights [UNHRC2020] described how technology is often used to limit freedom of assembly and association, such as for instance through network shutdowns and the surveillance of groups. Because access to the Internet is crucial not only for freedom of association and assembly, but also for the right to development, and the right to freedom of expression and information [Nyokabi], the United Nation Special Rapporteur argues that:

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

Whereas the states have the obligation to protect human rights, there has been an increasing call for non-state actors, such as companies, to respect human rights [UNGPBHR]. The UN adopted guiding principles on business and human rights [UNGPBHR] and talks within the HRC are ongoing about an international legally binding instrument to regulate the activities of transnational corporations and other business enterprises. This includes a chain-responsibility of actors, which means that not just the company's own processes should not negatively impact human rights, but they should also engage in due diligence processes, such as human rights impact assessments. This includes an assessment of whether the products that are sold, or the services that are provided, can be used to engage in human rights violations, or whether human rights violations occur in any stage of the supply chain of the company. If this is the case, measures should be taken to mitigate this.

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

6.1.1. Spam

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

This leaves us with an interesting case around spam mitigation: spam is currently handled mostly by mail providers on behalf of the user. Next to that, countries are increasingly adopting regulatory opt-in regimes for mailing lists and commercial e-mail, with a possibility of serious fines in case of violation. Yet many ask is spam not the equivalent of the fliers and handbills ever present in our offline world? The big difference between the proliferation of such messages offline and online is the scale. It is not hard for a single person to message a lot of people online, whereas if that person needed to go house by house the scale and impact of their actions would be much smaller. Inversely if it were a common practice to expose people to unlimited unwanted messages online, users would be drowned in such messages. This puts a large burden on filtering, and in both

filtering and sifting through many message, other expressions would be drowned out and would be severely hampered. Allowing illimited sending of unsolicited messages would be a blow against freedom of speech: when everyone talks, nobody listens.

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

6.1.2. DDoS

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

Because of the interrelation of technologies, it cannot be said that there is one point in the technical stack where one can locate the characteristics of "peaceful" or "non-peaceful" association visible to protocol developers. In the cases of spam blocking and DDoS mitigation, "peaceful or non-peaceful" is not a meaningful heuristic, or even characteristic, of problematic content. If anything, their commonality is their unrequested and nature, next to scale and volume. This allows us to draw the conclusion that DDoS and spam are not examples of freedom of association or assembly.

6.2. Holistic Agency: Mailing Lists and Spam

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

6.2.1. Mailing lists

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

In 1971 four years after the invention of email, the first mailing list was created to talk about the idea of using Arpanet for discussion. What had initially propelled the Arpanet project forward as a resource sharing platform was gradually replaced by the idea of a network as a means of bringing people together [Abbate]. More than 45 years after, mailing lists are pervasive and help communities to engage, have discussions, share information, ask questions, and build ties. Even as social media and discussion forums grow, mailing lists continue to be widely used [AckermannKargerZhang] and are still a crucial tool to organise groups and individuals around themes and causes [APC3].

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

6.2.2. Spam

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

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

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

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

6.3.1. Email

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

6.3.2. Mailing lists

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

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

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

6.3.3. IRC

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

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

6.3.4. WebRTC

Multi-party video conferencing protocols like WebRTC [RFC6176] [RFC7118] allow for robust, bandwidth-adaptive, wideband and super-wideband video and audio discussions in groups. However, it comes with many different configuration options, which can leave users open to unexpected privacy leakages:

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. On the one hand WebRTC is providing resilient channels of communications, but on the other hand it also exposes information about those who are using the tool which might lead to increased surveillance, identification and the consequences that might be derived from that. This is especially concerning because the usage of a VPN does not protect against the exposure of IP addresses [Crawford].

The risk of surveillance is also exists in an offline space, but this is generally slight easier to analyze for the end-user. Security and privacy expectations of the end-user could be either improved or made explicit. This in turn would result in a more secure and/or private exercise of the right to freedom of assembly or association.

6.3.5. Peer-to-peer networking

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

In his book *The Wealth of Networks*, [Benkler2] significantly expands on his definition of commons-based peer production. In his view, what distinguishes commons-based production is that it doesn't rely upon or propagate proprietary knowledge: "The inputs and outputs of the process are shared, freely or conditionally, in an institutional form that leaves them equally available for all to use as they choose at their individual discretion." [Benkler2]. To ensure that the knowledge generated is available for free use, commons-based projects are often shared under an open license

Peer-to-peer (P2P) is essentially a model of how people interact in real life because "we deal directly with one another whenever we wish to" [Vu]. Usually if we need something we ask our peers, who in turn refer us to other peers. In this sense, the ideal definition of P2P is that "nodes are able to directly exchange resources and services between themselves without the need for centralized servers" where each participating node typically acts both as a server and as a client [Vu]. [RFC5694] has defined it as peers or nodes that should be able to communicate directly between themselves without passing intermediaries, and that the system should be self-organizing and have decentralized control [RFC5694]. With this in mind, the ultimate model of P2P is a completely decentralized system, which is more resistant to speech regulation, immune to single points of failure and has a higher performance and scalability. Nonetheless, in practice some P2P systems are supported by centralized servers and some others have hybrid models where nodes are organized into two layers: the upper tier servers and the lower tier common nodes [Vu].

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

Whether for resource sharing or data sharing, P2P systems are enabling freedom of assembly and association. Not only do they allow for effective dissemination of information, but they leverage

computing resources by diminishing costs allowing for the formation of open collectives at the network level. At the same time, in completely decentralized systems the nodes are autonomous and can join or leave the network as they want -a characteristic that makes the system unpredictable: a resource might be only sometimes available, and some other resources might be missing or incomplete [Vu]. Lack of information might in turn makes association or assembly more difficult.

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

6.4. Universal Access: The Web

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

The W3C has done significant work to ensure that the Web is accessible to people with diverse physical abilities [W3C]. The implementation of these accessibility standards for instance help people who have issues with seeing or rendering images to understand what the image actually contains. Making the web more accessible for people with diverse physical abilities enables them to exercise their right to online assembly and association. While there are accessibility standards implemented for the web, this is less the case for the Internet.

The IETF uses English as its primary working language, both in its documentation and in its communication. This is also the case for reference implementations. It is estimated that roughly 20% of the Earth's population speaks English, whereas only 360 million speak English as their first language. [RFC2277] describes that "Internationalization is for humans. This means that protocols are

not subject to internationalization; text strings are.", this implies that protocol developers, as well as people that work with protocols, are not people, or that protocol developers are all in command of the English language. This means that it is significantly easier for people who have a command of the English language to become a protocol developer - and it might lead to the development of separate protocols that are developed within large language communities that are not using the English language or the Latin script. This makes it harder for people who seek to shape their own space of association and assembly on the Internet to do so. And is thus driving these communities into, often proprietary and non-interoperable services such as Facebook.

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

6.5. Block Together Now: IRC and Refusals

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

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

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

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

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

Communities, collaboration and joint action lie at the heart of the Internet. Even at a linguistic level, the words "networks" and "associations" are closely related. Both are groups and assemblies of people who depend on "links" and "relationships" [Swire]. Taking legal definitions given in international human rights law and related normative documents, we could assert that the rights to freedom of assembly and association protect collective activity online. These rights protect gatherings by persons for a specific purpose and groups with a defined aim over time for a variety of peaceful, expressive and non-expressive, purposes,. It is voluntary and uncoerced.

Given that the Internet itself was originally designed as a medium of communication for machines that share resources with each other as equals [RFC0903], the Internet is now one of the most basic infrastructures for the right to freedom of assembly and association. Since Internet protocols and the Internet architecture play a central role in the management, development and use of the Internet, we established the relation between some protocols and the right to freedom of assembly and association.

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

Lastly, the increasing shift towards closed and non-interoperable platforms in chat and social media networks have a significant impact on the distributed and open nature of the Internet. Often these non-interoperable platforms are built on open-protocols but do not allow for interoperability or data-portability. The use of social-media platforms has enabled groups to associate, but it has also rendered users unable to change platforms, therefore leading to a sort of "forced association" that inhibits people to fully exercise their freedom of assembly and association.

8. Acknowledgements

- * Fred Baker, Jefsey, and Andrew Sullivan for work on Internet definitions.
- * Stephane Bortzmeyer, ICNL, and Lisa Vermeer for several concrete text suggestions that found their way in this document.
- * Mark Perkins and Gurshabad for finding a lot of typos.
- * Gurshabad Grover, an anonymous reviewer, ICNL, Lisa Vermeer, and Sandra Braman for full reviews.
- * The hrpc mailinglist at large for a very constructive discussion on a hard topic.

9. Work Space

Current work on this draft is happening at: <https://github.com/IRTF-HRPC/draft-association> Pull requests and issues are welcome.

10. Security Considerations

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

11. IANA Considerations

This document has no actions for IANA.

12. Research Group Information

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

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

13. Informative References

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

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

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

- [APC] Association for Progressive Communications and . Gayathry Venkiteswaran, "Freedom of assembly and association online in India, Malaysia and Pakistan. Trends, challenges and recommendations.", 2016,
<https://www.apc.org/es/system/files/FOAA_online_IndiaMalaysiaPakistan.pdf>.
- [APC3] Association for Progressive Communications, "Closer than ever", 2020, <<https://www.apc.org/en/node/36145/#tools>>.
- [APCtraining] Sauter, D. and Association for Progressive Communications, "Multimedia training kit", 2013,
<http://itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_FOA_Handout.pdf>.
- [Benkler] Benkler, Y., "Peer Production and Cooperation", 2009,
<<http://www.benkler.org/Peer%20production%20and%20cooperation%2009.pdf>>.
- [Benkler2] Benkler, Y., "The wealth of Networks - How social production transforms markets and freedom", New Haven and London - Yale University Press , 2006,
<<http://is.gd/rxUpTQ>>.
- [Bloketal] Blok, A., Nakazora, M., and B.R. Winthereik, "Infrastructuring Environments", Science as Culture 25:1, 1-22. , 2016.
- [Bowker] Bowker, G., "Information mythology and infrastructure", In: L. Bud (Ed.), Information Acumen: The Understanding and use of Knowledge in Modern Business, Routledge, London, 1994, pp.231-247 , 1994.
- [CERD] United Nations, "Convention on the Elimination of all forms of Racial Discrimination", 1966,
<<https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/2F70352A0B65EB67CA256B6E0075FE13>>.
- [CoE] Council of Europe, "Freedom of assembly and association on the Internet", 2015,
<<https://mk0rofifiqa2w3u89nud.kinstacdn.com/wp-content/uploads/COE-report-on-FOAA-rights-on-the-internet-.pdf>>.
- [Crawford] Crawford, D., "The WebRTC VPN Bug and How to Fix", 2015,
<<https://www.bestvpn.com/the-webrtc-vpn-bug-and-how-to-fix-it/>>.

- [CRC] Wikipedia, ., "Lorum", 2000,
<<https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/E123F4F71DCAE3E7CA256B4F007F2905>>.
- [CRPD] United Nations, "Convention on the Rights of Persons with Disabilities", 2007,
<<http://www.austlii.edu.au/au/other/dfat/treaties/2008/12.html>>.
- [FoAdef] Wikipedia, "Freedom of association", 2021,
<https://en.wikipedia.org/wiki/Freedom_of_association>.
- [Glasius] Glasius, M., Schalk, J., and M. De Lange, "Illiberal Norm Diffusion: How Do Governments Learn to Restrict Nongovernmental Organizations?", 2020,
<<https://academic.oup.com/isq/article/64/2/453/5823498>>.
- [HafnerandLyon] Hafnerand, K. and M. Lyon, "Where Wizards Stay Up Late. The Origins of the Internet", First Touchstone Edition (1998): 93. , 1998, <<https://doi.org/10.1111/misr.12020>>.
- [HRPC-charter] Human Rights Protocol Consideration RG, ., "Charter for Research Group", 2015,
<<https://datatracker.ietf.org/doc/charter-irtf-hrpc/>>.
- [HussainHoward] Hussain, M.M. and P.N. Howard, "What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring", Int Stud Rev (2013) 15 (1): 48-66. , 2013, <<https://doi.org/10.1111/misr.12020>>.
- [ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1966,
<<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>>.
- [Kaye] Kaye, D., "The use of encryption and anonymity in digital communications", 2015,
<https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>.
- [LEAP] LEAP, "The Right to Whisper", 2020,
<<https://leap.se/en/about-us/vision>>.

- [Loi] Loi, M. and M. Christen, "Two Concepts of Group Privacy", 2020, <<https://link.springer.com/article/10.1007/s13347-019-00351-0>>.
- [Mainwaringetal] Mainwaring, S.D., Chang, M.F., and K. Anderson, "Infrastructures and Their Discontents: Implications for Ubicomp", DBLP Conference: Conference: UbiComp 2004: Ubiquitous Computing: 6th International Conference, Nottingham, UK, September 7-10, 2004. Proceedings , 2004, <<http://www.dourish.com/classes/readings/Mainwaring-Infrastructure.pdf>>.
- [Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and the first amendment", 1998, <<http://www.cardozoaelj.com/wp-content/uploads/2013/02/Marcus.pdf>>.
- [Nasser] Nasser, R., "قلب", 2013, <<https://nas.sr/%D9%82%D9%84%D8%A8/>>.
- [NelsonHedlun] Minar, N. and M. Hedlun, "A Network of Peers: Models Through the History of the Internet", Peer to Peer: Harnessing the Power of Disruptive Technologies, ed: Andy Oram , 2001, <http://library.uniteddiversity.coop/REconomy_Resource_Pack/More_Inspirational_Videos_and_Useful_Info/Peer_to_Peer-Harnessing_the_Power_of_Disruptive_Technologies.pdf>.
- [Nyokabi] Nyokabi, D.M., Diallo, N., Ntesang, N.W., White, T.K., and T. Ilori, "The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa", 2019, <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1582/3.Global%20article%20HRDA_2_2019.pdf?sequence=4&isAllowed=y>.
- [Pensado] Jaime Pensado, ., "Student Activism. Utopian Dreams.", ReVista. Harvard Review of Latin America (2012). , 2012, <<http://revista.drclas.harvard.edu/book/student-activism>>.
- [PipekWulf] Pipek, V. and W. Wolf, "Infrastructuring: Towards an Integrated Perspective on the Design and Use of Information Technology", Journal of the Association for Information Systems (10) 5, pp. 306-332 , 2009.

- [RFC0001] Crocker, S., "Host Software", RFC 1, DOI 10.17487/RFC0001, April 1969, <<https://www.rfc-editor.org/info/rfc1>>.
- [RFC0155] North, J., "ARPA Network mailing lists", RFC 155, DOI 10.17487/RFC0155, May 1971, <<https://www.rfc-editor.org/info/rfc155>>.
- [RFC0903] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", STD 38, RFC 903, DOI 10.17487/RFC0903, June 1984, <<https://www.rfc-editor.org/info/rfc903>>.
- [RFC1211] Westine, A. and J. Postel, "Problems with the maintenance of large mailing lists", RFC 1211, DOI 10.17487/RFC1211, March 1991, <<https://www.rfc-editor.org/info/rfc1211>>.
- [RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, DOI 10.17487/RFC1771, March 1995, <<https://www.rfc-editor.org/info/rfc1771>>.
- [RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <<https://www.rfc-editor.org/info/rfc1930>>.
- [RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <<https://www.rfc-editor.org/info/rfc1958>>.
- [RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <<https://www.rfc-editor.org/info/rfc2277>>.
- [RFC2810] Kalt, C., "Internet Relay Chat: Architecture", RFC 2810, DOI 10.17487/RFC2810, April 2000, <<https://www.rfc-editor.org/info/rfc2810>>.
- [RFC2812] Kalt, C., "Internet Relay Chat: Client Protocol", RFC 2812, DOI 10.17487/RFC2812, April 2000, <<https://www.rfc-editor.org/info/rfc2812>>.
- [RFC3233] Hoffman, P. and S. Bradner, "Defining the IETF", BCP 58, RFC 3233, DOI 10.17487/RFC3233, February 2002, <<https://www.rfc-editor.org/info/rfc3233>>.
- [RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <<https://www.rfc-editor.org/info/rfc4084>>.

- [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <<https://www.rfc-editor.org/info/rfc4271>>.
- [RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <<https://www.rfc-editor.org/info/rfc4880>>.
- [RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, DOI 10.17487/RFC5694, November 2009, <<https://www.rfc-editor.org/info/rfc5694>>.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <<https://www.rfc-editor.org/info/rfc5751>>.
- [RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March 2011, <<https://www.rfc-editor.org/info/rfc6176>>.
- [RFC7118] Baz Castillo, I., Millan Villegas, J., and V. Pascual, "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)", RFC 7118, DOI 10.17487/RFC7118, January 2014, <<https://www.rfc-editor.org/info/rfc7118>>.
- [RFC7194] Hartmann, R., "Default Port for Internet Relay Chat (IRC) via TLS/SSL", RFC 7194, DOI 10.17487/RFC7194, August 2014, <<https://www.rfc-editor.org/info/rfc7194>>.
- [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <<https://www.rfc-editor.org/info/rfc8280>>.
- [RutzenZenn] Rutzen, D. and J. Zenn, "Association and Assembly in the Digital Age", The International Journal of Not-for-Profit Law, Volume 13, Issue 4 , December 2011.
- [Sauter] Sauter, M., "The Coming Swarm", Bloomsbury , 2014.

- [Schleuder] Nadir, "Schleuder - A gpg-enabled mailinglist with remailing-capabilities.", 2017, <<https://schleuder.nadir.org/>>.
- [Stanford] Brownlee, K. and D. Jenkins, "Freedom of Association", 2019, <<https://plato.stanford.edu/entries/freedom-association/>>.
- [Swire] Peter Swire, ., "Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection", North Carolina Law Review (2012) 90 (1): 104. , 2012, <<https://ssrn.com/abstract=1989516> or <http://dx.doi.org/10.2139/ssrn.1989516>>.
- [Troncosoetal] Troncoso, C., Isaakdis, M., Danezis, G., and H. Halpin, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments", Proceedings on Privacy Enhancing Technologies ; 2017 (4):307-329 , 2017, <<https://www.petsymposium.org/2017/papers/issue4/paper87-2017-4-source.pdf>>.
- [UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <<http://www.un.org/en/documents/udhr/>>.
- [UNGA] Hina Jilani, ., "Human rights defenders", A/59/401 , 2004, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/401 para. 46>.
- [UNGC37] United Nations Human Rights Committee, "Human Rights Committee General comment No. 37 (2020) on the right of peaceful assembly (article 21), CCPR/C/GC/3", 2020, <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11>.
- [UNGPBHR] United Nations, "Guiding Principles on Business and Human Rights", 2011, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf>.

[UNHRC2018]

United Nations Human Rights Council, "UN Human Rights Council Resolution 'The promotion, protection and enjoyment of human rights on the Internet' (A/HRC/32/L.20)", 2016,
<<https://digitallibrary.un.org/record/1639840?ln=en>>.

[UNHRC2020]

Michelle Bachelet, . and United Nations, "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Report of the United Nations High Commissioner for Human Rights A/HRC/44/24, 2020", 2000,
<https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx>.

[UNSRFAA2012]

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

[UNSRFAA2019]

Clément Voule, . and United Nations, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 2019,
<<https://undocs.org/A/HRC/41/41>>.

[UNSRFOAA2012]

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

[ViennaDeclaration]

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

[Vu]

Vu, Quang Hieu, ., Lupu, Mihai, ., and . Ooi, Beng Chin, "Peer-to-Peer Computing: Principles and Applications", 2010, <<https://www.springer.com/cn/book/9783642035135>>.

[W3C]

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

Authors' Addresses

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

Gisela Perez de Acha
Derechos Digitales
Email: gisela@derechosdigitales.org

Stéphane Couture
Université de Montréal
Email: stephane.couture@umontreal.ca

Mallory Knodel
Center for Democracy & Technology
Email: mknodel@cdt.org

Human Rights Protocol Considerations Research Group	G. Grover
Internet-Draft	Centre for Internet and Society
Updates: 8280 (if approved)	N. ten Oever
Intended status: Informational	University of Amsterdam
Expires: 29 September 2022	28 March 2022

Guidelines for Human Rights Protocol and Architecture Considerations
draft-irtf-hrpc-guidelines-13

Abstract

This document sets guidelines for human rights considerations for developers working on network protocols and architectures, 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].

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

This informational document has consensus for publication from the Internet Research Task Force (IRTF) Human Right Protocol Considerations Research Group. It has been reviewed, tried, and tested by both by the research group as well as by researchers and practitioners from outside the research group. The research group acknowledges that the understanding of the impact of internet protocols and architecture on society is a developing practice and is a body of research that is still in development.

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 29 September 2022.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Human rights threats	4
3. Conducting human rights reviews	5
3.1. Analyzing drafts based on guidelines for human rights considerations model	6
3.2. Analyzing drafts based on their perceived or speculated impact	6
3.3. Expert interviews	6
3.4. Interviews with impacted persons and communities	6
3.5. Tracing impacts of implementations	6
4. Guidelines for human rights considerations	7
4.1. Connectivity	7
4.2. Reliability	8
4.3. Content agnosticism	9
4.4. Localization	10
4.5. Internationalization	11
4.6. Open Standards	12
4.7. Heterogeneity Support	13
4.8. Integrity	14
4.9. Authenticity	15
4.10. Confidentiality	16
4.11. Security	17
4.12. Privacy	18
4.13. Pseudonymity	18
4.14. Anonymity	19
4.15. Censorship resistance	20
4.16. Outcome Transparency	21
4.17. Adaptability	22
4.18. Accessibility	23
4.19. Decentralization	24
4.20. Remedy	25
4.21. Misc. considerations	25

5. Document Status	26
6. Acknowledgements	26
7. Security Considerations	26
8. IANA Considerations	26
9. Research Group Information	27
10. Informative References	27
Authors' Addresses	33

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 how their decisions can potentially influence the exercise of human rights on the Internet. It should be noted that the impact of a protocol cannot solely be deduced from its design, but its usage and implementation should also be studied to form a full protocol human rights impact assessment.

The questions are based on the research performed by the Human Rights Protocol Considerations (hrpc) research group which has been documented before these considerations. The research establishes that human rights relate to standards and protocols, and offers a common vocabulary of technical concepts that influence 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 an 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. The understanding of what human rights are is based on the Universal Declaration of Human Rights [UDHR] and subsequent treaties that jointly form the body of international human rights law [UNHR].

This document does not provide a detailed taxonomy of the nature of (potential) human rights violations, whether direct or indirect, long-term or short-term, certain protocol choices might present. In part because this is highly context-dependent, and in part, because this document aims to provide a practical set of guidelines. However, further research in this field would definitely benefit developers and implementers.

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

This informational document has consensus for publication from the Internet Research Task Force (IRTF) Human Right Protocol Considerations Research Group. It has been reviewed, tried, and tested by both by the research group as well as by researchers and practitioners from outside the research group. The research group acknowledges that the understanding of the impact of internet protocols and architecture on society is a developing practice and is a body of research that is still in development.

2. Human rights threats

Threats to the exercise of human rights on the Internet come in many forms. Protocols and standards may harm or enable the right to freedom of expression, right to freedom of information, right to non-discrimination, right to equal protection, right to participate in cultural life, arts and science, right to freedom of assembly and association, right to privacy, and the right to security. An end-user who is denied access to certain services or content 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 or dissuaded 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, extra-judicial killing or detention on the basis of information gathered by state agencies through the monitoring of network traffic.

This document presents several examples of how 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 surprising 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, affirming that "the same rights that people have offline must also be protected online." [UNHRC2016] 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.

3. Conducting human rights reviews

Ideally, protocol developers and collaborators should incorporate human rights considerations into the design process itself (see Guidelines for human rights considerations). This section provides guidance on how to conduct a human rights review, i.e. gauge the impact or potential impact of a protocol or standard on human rights.

Human rights reviews can take place at different stages of the development process of an Internet-Draft. 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:

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

This analysis of Internet-Drafts uses the model as described in section 3.3. The outlined categories and questions can be used to review an Internet-Draft. 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. Analyzing drafts based on their perceived or speculated impact

When reviewing an Internet-Draft, specific human rights impacts can 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 may lead to new speculative understandings of links between human rights and protocols.

3.3. 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 its 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, which can help the review gain traction when it is published.

3.4. Interviews with impacted persons and communities

Protocols impact users of the Internet. Interviews can help the reviewer understand how protocols affect the people that use the protocols. Since human rights are best understood from the perspective of the rights-holder, this approach will improve the understanding of the real world effects of the technology. At the same time, it can be hard to attribute specific changes to a particular protocol, this is of course even harder when a protocol has not been (widely) deployed.

3.5. Tracing impacts of implementations

The reality of deployed protocols can be at odds with the expectations during the protocol design and development phase [RFC8980]. When a specification already has associated running code, the code can be analyzed either in an experimental setting or on the Internet where its impact can be observed. In contrast to reviewing the draft text, this approach can allow the reviewer to understand

how the specifications works in practice, and potentially what unknown or unexpected effects the technology has.

4. Guidelines for human rights considerations

This section provides guidance for document authors in the form of a questionnaire about protocols and how technical decisions can shape the exercise of human rights. The questionnaire may be useful at any point in the design process, particularly after the document authors have developed a high-level protocol model as described in [RFC4101]. These guidelines do not seek to replace any existing referenced specifications, but rather contribute to them and look at the design process from a human rights perspective.

Protocols and Internet Standards might benefit from a documented discussion of potential human rights risks arising from potential misapplications of the protocol or technology described in the RFC. This might be coupled with an Applicability Statement for that RFC.

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

In considering these questions, authors will need to be aware of the potential of technical advances or the passage of time to undermine protections. In general, considerations of rights are likely to be more effective if they are considered given a purpose and specific use cases, rather than as abstract absolute goals.

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

4.1. 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 certain functions can and should be performed at 'ends' of the network. [RFC1958] states "that in very general terms, the community believes that the goal is connectivity [...] and the intelligence is end to end rather than hidden in the network." Generally speaking, it is easier to attain reliability of data transmissions with computation at endpoints rather than at intermediary nodes.

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

Example: Encrypting connections, like done with HTTPS, can add a significant network overhead and consequently make web resources less accessible to those with low bandwidth and/or high latency connections. [HTTPS-REL] Encrypting traffic is a net positive for privacy and security, and thus protocol designers can acknowledge the tradeoffs of connectivity made by such decisions.

Impacts:

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

4.2. Reliability

Question(s): Is your protocol fault tolerant? Does it downgrade gracefully, i.e. with mechanisms for fallback and/or notice? 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 and resiliency ensures that a protocol will execute its function consistently and error resistant as described, and function without unexpected result. Measures for reliability in protocols assure users that their intended communication was successfully executed.

A system that is reliable degrades 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 non-secure cipher suites - from a functional perspective, this is useful; from a security perspective, this can be disastrous. 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

4.3. 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 exceptions where it comes to effective traffic handling, for instance where it comes to delay-tolerant or delay-sensitive packets, based on the header. If there is any prioritization based on the content or metadata of the protocol, the protocol should be transparent about such information and reasons thereof.

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

4.4. 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) [W3Cil18nDef]. For our purposes, it can be 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

4.5. Internationalization

Question(s): Does your protocol or specification define text string elements, in the payload or headers, that have to be understood or entered by humans? Does your specification 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 specification 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." {{W3Cil18nDef}}

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 identifiers.) Given the IETF's mission to make the Internet a global network of networks, [RFC3935] developers should ensure that protocols work with languages apart from English and character sets apart from Latin characters. It is therefore crucial that at the very 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

4.6. 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 (and open source software) allow users to glean information about how the tools they are using work, including the tools' security and privacy properties. They additionally 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

4.7. 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?

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].

Heterogeneity support in protocols can thus enable a wide range of devices and (by extension) users to participate on the network.

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

4.8. 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

4.9. 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

4.10. Confidentiality

Question(s): Does this protocol expose the transmitted data over the wire? Does the 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]. The possibility of pervasive monitoring and surveillance undermines users' trust, and can be mitigated by ensuring confidentiality, i.e. passive attackers should gain little or no information from observation or inference of protocol activity. [RFC7258][RFC7624].

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

4.11. 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/specification, 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].

Typically, any protocol operating on the internet can be the target of passive attacks (when the attacker can access and read packets on the network); active attacks (when an attacker is capable of writing information to the network packets). [BCP72]

Example: See [BCP72].

Impacts:

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

- * Right to non-discrimination
- * Right to security

4.12. 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 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]. 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

4.13. Pseudonymity

Question(s): 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? If yes, can the protocol be implemented in a way that does not rely on personally identifiable information? If not, does the specification describe how any such data be handled? Have you considered the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.2?

Explanation: 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]

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. This can allow an enabling environment for users to exercise other rights, including freedom of expression and political participation, without fear or direct identification or discrimination.

Example: Generally, pseudonymous identifiers cannot be simply reverse engineered. Some early approaches took approaches such as simple hashing of IP addresses, but these could then be simply reversed by generating a hash for each potential IP address and comparing it to the pseudonym.

Example: There are also efforts for application layer protocols, like Oblivious DNS Over HTTPS, [draft-pauly-dprive-oblivious-doh] that can separate identifiers from requests.

Impacts:

- * Right to non-discrimination
- * Right to freedom of expression
- * Right to political participation
- * Right to freedom of assembly and association

4.14. 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 seeks to distribute it to more entities than the originally-intended recipients (see [RFC6235] as an example), you should anonymize the data, but keep in mind that "anonymizing" data is notoriously hard. For example, just dropping the last byte of an IP address does not "anonymize" 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.

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

4.15. Censorship resistance

Question(s): Can your protocol contribute to filtering? Could be implemented to censor data or services? Could it be designed to ensure this doesn't happen? Does your protocol make it apparent or transparent when access to a resource is restricted and reasons therefor? Does your protocol introduce new identifiers or reuse existing identifiers (e.g. MAC addresses) that might be associated

with persons or content?

Explanation: Governments and service providers block or filter content or traffic, often without the knowledge of end-users. [RFC7754] See [draft-irtf-pearg-censorship] for a survey of censorship techniques employed across the world, which lays out protocol properties that have been exploited to censor access to information. Censorship resistance refers to the methods and measures to prevent Internet censorship.

Example: Identifiers of content exposed within a protocol might be used to facilitate censorship, as in the case of 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].

If a protocol potentially enables censorship, protocol designers should strive towards creating error codes that capture different scenarios (blocked due to administrative policy, unavailable because of legal requirements, etc.) to minimize ambiguity for end-users.

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 standardisation efforts like Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941] and MAC address randomization [draft-zuniga-mac-address-randomization] have been pursued.

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

4.16. 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:

- * Right to freedom of expression
- * Right to privacy
- * Right to freedom of assembly and association
- * Right to access to information

4.17. Adaptability

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

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.

Adaptability and permissionless innovation can be used to shape information networks as preferenced by groups of users. Furthermore, a precondition of adaptability is the ability of the people who can adapt the network to be able to know and understand the network. This is why adaptability and permissionless innovation are inherently connected to the right to education and the right to science as well as the right to freedom of assembly and association as well as the right to freedom of expression. Since it allows the users of the network to determine how the assemble, collaborate, and express themselves.

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

4.18. Accessibility

Question(s): Is your protocol designed to provide an enabling environment for all? 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.

Another example is the works that is done in the AVT and AVTCORE working groups in the IETF that enable text conversation in multimedia, text telephony, wireless multimedia and video communications for sign language and lip-reading (ie. [RFC9071]).

Impacts:

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

4.19. 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? Does your protocol create additional centralized points of control?

Explanation: Decentralization is one of the central technical concepts of the architecture of the Internet, and is 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. For a more detailed discussion of this topic, please see [arkkoetal].

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 into. 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

4.20. Remedy

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

Explanation: Providing access to remedy by states and corporations is a part of the UN Guiding Principles on Business and Human Rights [UNGP]. Access to remedy may help victims of human rights violations in seeking justice, or allow law enforcement agencies to identify a possible violator. However, mechanisms in protocols that try to enable 'attribution' to individuals will impede the exercise of the right to privacy. The former Special Rapporteur for Freedom of Expression has also argued that anonymity is an inherent part of freedom of expression [Kaye]. Considering the potential adverse impact of attribution on the right to privacy and freedom of expression, enabling attribution on an individual level is most likely not consistent with human rights.

Example: Adding personal identifiable information to data streams might help in identifying a violator of human rights and provide access to remedy, but this would disproportionately affect all users right to privacy, anonymous expression, and association.

Impacts:

- * Right to remedy
- * Right to security
- * Right to privacy

4.21. Misc. considerations

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

Explanation: Publication of a particular RFC under a certain status has consequences. Publication as an Internet Standard as part of the Standards Track may signal to implementers that the specification has a certain level of maturity, operational experience, and consensus. Similarly, publication of a specification as an experimental document as part of the non-standards track would signal to the community that the document "may be intended for eventual standardization but [may]

not yet [be] ready" for wide deployment. The extent of the deployment, and consequently its overall impact on end-users, may depend on the document status presented in the RFC. See [BCP9] and updates to it for a fuller explanation.

5. Document Status

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

6. Acknowledgements

Thanks to:

- * Corinne Cath-Speth for work on [RFC8280].
- * Theresa Engelhard, Joe Hall, Avri Doria, Joey Salazar, Corinne Cath-Speth, Farzaneh Badii, Sandra Braman, Colin Perkins, John Curran, Eliot Lear, Mallory Knodel, and the hrpc list for reviews and suggestions.
- * Individuals who conducted human rights reviews for their work and feedback: Amelia Andersdotter, Beatrice Martini, Karan Saini and Shivan Kaul Sahib.

7. Security Considerations

Article three of the Universal Declaration of Human Rights reads: "Everyone has the right to life, liberty and security of person.". This article underlines the importance of security and its interrelation with human life and liberty, but since human rights are indivisible, interrelated and interdependent, security is also closely linked to other human rights and freedoms. This document seeks to strengthen human rights, freedoms, and security by relating and translating these concepts to concepts and practices as they are used in Internet protocol and architecture development. The aim of this is to secure human right and thereby improve the sustainability, usability, and effectiveness of the network. The document seeks to achieve this by providing guidelines as done in section three of this document.

8. IANA Considerations

This document has no actions for IANA.

9. 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 (<mailto:hrpc@ietf.org>). Information on the group and information on how to subscribe to the list is at <https://www.irtf.org/mailman/listinfo/hrpc> (<https://www.irtf.org/mailman/listinfo/hrpc>)

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

10. Informative References

[arkkoetal]

Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsure, J., and N. ten Oever, "Considerations on Internet Consolidation and the Internet Architecture", 2019, <https://datatracker.ietf.org/doc/html/draft-arkko-iab-internet-consolidation-02>.

[BCP72]

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

[BCP9]

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

[Bless]

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

[Brown]

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

[draft-irtf-pearg-censorship]

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

[draft-pauly-dprive-oblivious-doh]

Kinnear, E., McManus, P., Pauly, T., Verma, T., and C.A. Wood, "Oblivious DNS Over HTTPS", 2022, <https://tools.ietf.org/html/draft-pauly-dprive-oblivious-doh>.

- [draft-zuniga-mac-address-randomization]
Zuniga, JC., Bernardos, CJ., and A. Andersdotter, "MAC address randomization", 2020,
<<https://tools.ietf.org/html/draft-irtf-pearg-censorship>>.
- [FIArch] "Future Internet Design Principles", January 2012,
<http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf>.
- [geekfeminism]
Geek Feminism Wiki, "Pseudonymity", 2015,
<<http://geekfeminism.wikia.com/wiki/Pseudonymity>>.
- [Hill2014] Hill, R., "Partial Catalog of Human Rights Related to ICT Activities", 2014,
<<http://www.apig.ch/UNIGE%20Catalog.pdf>>.
- [HTML5] W3C, "HTML5", 2014, <<https://www.w3.org/TR/html5/>>.
- [HTTPS-REL]
Meyer, E., "Securing Web Sites Made Them Less Accessible", 2018, <<https://meyerweb.com/eric/thoughts/2018/08/07/securing-sites-made-them-less-accessible/>>.
- [ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976,
<<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>>.
- [ICESCR] United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights", 1966,
<<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>>.
- [IRP] Internet Rights and Principles Dynamic Coalition, "10 Internet Rights & Principles", 2014,
<http://internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_10RightsandPrinciples_28May2014-11.pdf>.
- [Kaye] Kaye, D., "The use of encryption and anonymity in digital communications", 2015,
<https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>.

- [newegg] Mullin, J., "Newegg on trial: Mystery company TQP rewrites the history of encryption", 2013, <<http://arstechnica.com/tech-policy/2013/11/newegg-on-trial-mystery-company-tqp-re-writes-the-history-of-encryption/>>.
- [notewell] IETF, "Note Well", 2015, <<https://www.ietf.org/about/note-well.html>>.
- [patentpolicy] W3C, "W3C Patent Policy", 2004, <<https://www.w3.org/Consortium/Patent-Policy-20040205/>>.
- [Penney] Penney, J., "Chilling Effects: Online Surveillance and Wikipedia Use", 2016, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645>.
- [Pouwelse] Pouwelse, Ed, J., "Media without censorship", 2012, <<https://tools.ietf.org/html/draft-pouwelse-censorfree-scenarios>>.
- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <<https://www.rfc-editor.org/info/rfc793>>.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.
- [RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <<https://www.rfc-editor.org/info/rfc1958>>.
- [RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <<https://www.rfc-editor.org/info/rfc1984>>.
- [RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <<https://www.rfc-editor.org/info/rfc2026>>.
- [RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <<https://www.rfc-editor.org/info/rfc2277>>.

- [RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <<https://www.rfc-editor.org/info/rfc3365>>.
- [RFC3724] Kempf, J., Ed., Austein, R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <<https://www.rfc-editor.org/info/rfc3724>>.
- [RFC3935] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <<https://www.rfc-editor.org/info/rfc3935>>.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <<https://www.rfc-editor.org/info/rfc4033>>.
- [RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <<https://www.rfc-editor.org/info/rfc4101>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <<https://www.rfc-editor.org/info/rfc4941>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <<https://www.rfc-editor.org/info/rfc5321>>.
- [RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <<https://www.rfc-editor.org/info/rfc5646>>.
- [RFC6108] Chung, C., Kasyanov, A., Livingood, J., Mody, N., and B. Van Lieu, "Comcast's Web Notification System Design", RFC 6108, DOI 10.17487/RFC6108, February 2011, <<https://www.rfc-editor.org/info/rfc6108>>.

- [RFC6235] Boschi, E. and B. Trammell, "IP Flow Anonymization Support", RFC 6235, DOI 10.17487/RFC6235, May 2011, <<https://www.rfc-editor.org/info/rfc6235>>.
- [RFC6365] Hoffman, P. and J. Klensin, "Terminology Used in Internationalization in the IETF", BCP 166, RFC 6365, DOI 10.17487/RFC6365, September 2011, <<https://www.rfc-editor.org/info/rfc6365>>.
- [RFC6701] Farrel, A. and P. Resnick, "Sanctions Available for Application to Violators of IETF IPR Policy", RFC 6701, DOI 10.17487/RFC6701, August 2012, <<https://www.rfc-editor.org/info/rfc6701>>.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <<https://www.rfc-editor.org/info/rfc6973>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.
- [RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <<https://www.rfc-editor.org/info/rfc7624>>.
- [RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles", RFC 7725, DOI 10.17487/RFC7725, February 2016, <<https://www.rfc-editor.org/info/rfc7725>>.
- [RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <<https://www.rfc-editor.org/info/rfc7754>>.
- [RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <<https://www.rfc-editor.org/info/rfc7844>>.

- [RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <<https://www.rfc-editor.org/info/rfc7858>>.
- [RFC8179] Bradner, S. and J. Contreras, "Intellectual Property Rights in IETF Technology", BCP 79, RFC 8179, DOI 10.17487/RFC8179, May 2017, <<https://www.rfc-editor.org/info/rfc8179>>.
- [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <<https://www.rfc-editor.org/info/rfc8280>>.
- [RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/info/rfc8484>>.
- [RFC8980] Arkko, J. and T. Hardie, "Report from the IAB Workshop on Design Expectations vs. Deployment Reality in Protocol Development", RFC 8980, DOI 10.17487/RFC8980, February 2021, <<https://www.rfc-editor.org/info/rfc8980>>.
- [RFC9071] Hellström, G., "RTP-Mixer Formatting of Multiparty Real-Time Text", RFC 9071, DOI 10.17487/RFC9071, July 2021, <<https://www.rfc-editor.org/info/rfc9071>>.
- [Saltzer] Saltzer, J.H., Reed, D.P., and D.D. Clark, "End-to-End Arguments in System Design", ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288. , 1984.
- [UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <<http://www.un.org/en/documents/udhr/>>.
- [UNGP] United Nations, "United Nations Guiding Principles on Business and Human Rights", 2011, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf>.
- [UNHR] United Nations, "The Core International Human Rights Instruments and their monitoring bodies", 2011, <<https://www.ohchr.org/en/professionalinterest/pages/coreinstruments.aspx>>.
- [UNHRC2016] United Nations Human Rights Council, "UN Human Rights Council Resolution "The promotion, protection and

enjoyment of human rights on the Internet" (A/HRC/32/L.20)", 2016, <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement>>.

[W3CAccessibility]

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

[W3Ci18nDef]

W3C, "Localization vs. Internationalization", 2010,
<<http://www.w3.org/International/questions/qa-il8n.en>>.

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

Authors' Addresses

Gurshabad Grover
Centre for Internet and Society
Email: gurshabad@cis-india.org

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