Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

J. Guerra
Derechos Digitales
M. Knodel
ARTICLE 19

July 08, 2019

Feminism and protocols
draft-guerra-feminism-01

Abstract

This document aims to describe how internet standards, protocols and its implementations may impact diverse groups and communities. The research on how some protocol can be enabler for specific human rights while possibly restricting others has been documented in [RFC8280]. Similar to how RFC 8280 has taken a human rights lens through which to view engineering and design choices by internet standardisation, this document addresgses the opportunities and vulnerabilities embedded within internet protocols for specific, traditionally maginalised groups.

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 January 9, 2020.

Copyright Notice

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

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

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

Table of Contents

1. Introduction 2
1.1. An intersectional perspective 3
1.1.1. Internet as a matrix of domination 4
1.2. Brief history of feminism and the internet 5
2. Methodology 6
3. Feminist Principles 6
3.1. Access 6
3.1.1. Internet access 7
3.1.2. Access to information 7
3.1.3. Usage of technology 8
3.2. Networked 8
3.2.1. Resistance 9
3.2.2. Movement building 9
3.2.3. Internet governance 10
3.3. Economy 10
3.3.1. Business models 10
3.3.2. Open source 11
3.4. Expression 11
3.4.1. Amplify 12
3.4.2. Expression 12
3.4.3. Pornography 12
4. Embodiment 13
4.1. Consent 14
4.1.1. Privacy and data 14
4.1.2. Memory 15
4.1.3. Anonymity 15
4.1.4. Children 16
4.2. Online violence 16
5. References not yet referenced 17
6. Security Considerations 18
7. IANA Considerations 18
8. Informative References 18
Authors' Addresses 21

1. Introduction

This document aims to use a feminist framework to analyse the impacts of internet protocols on society. It is based on a document called The The Feminist Principles of the Internet [FPI], a series of 17 statements with a "gender and sexual rights lens on critical

internet-related rights" for the purpose of enabling women's rights movements to explore issues related to internet technology.

These Principles, as well as most of the experiences and learnings of the feminist movement in the digital age, have focused on invisioning a more just internet as a necessary action in building a more just society, namely one that recognizes differences across a variety of lived experience and identity.

This document must not be understood as a set of rules or recommendations, but as an articulation of key issues with feminist policies and approaches, in order to begin to investigate. That is why this document has two main goals: to identify terminology, both in technical and feminist communities, that can be shared in order to start a dialogue; and to analyze the Feminist Principles based on some of the technical discussions that have been taken into account in the development of protocols.

In what follows, this document first describes the feminist theoretical framework from which it proposes to analyze the impacts of the protocols on marginalized and discriminated communities. In the second part, describes the methodology used to connect the framework mentioned above with the Feminist Principles of the internet. In the third part, characteristics of each principle, as well as the harms on which they are based, the possible points where they connect with IETF work and related rights, are described.

This is still a work in progress so many sections are yet to be done. Coming soon will be added use cases as examples of how protocols and standards can restrict the use of the internet by certain communities and individuals.

1.1. An intersectional perspective

Imagine a highway that connects two big cities, one capable of withstanding heavy traffic at high speeds. Driving there takes experience and expertise, and just a few streets intersect it so as not to hinder traffic. Imagine this highway as a robust body of rights and those who travel along it as people who have traditionally enjoyed these rights.

If someone without enough experience is driving down a road that intersects the highway and wants to get there, that person will be at greater risk of crashing or having an accident. In addition, without a valid license the person will also run the risk of being fined by the traffic authorities. In terms of rights, those intersecting roads are not robust and the risks of accident are forms of

discrimination experienced by those who drive on them. What if many small streets intersect at the same point on the highway?

Arised in black feminist theory, the concept of intersectionality serves to understand how multiple forms of discrimination overlap [Collins]. As first pointed by [Crenshaw] in the United States, "Black women can experience discrimination in ways that are both similar to and different from those experienced by white women and Black men", so an intersectional approach should be able to recognize this type of discrimination by transcending the one-way perspective with which the justice system, as well as feminist and anti-racist movements, had traditionally operated.

From this proposal, the concept has meant a paradigm shift both in feminist thinking [Collins] and movements [Lorde][Davis], and more recently in the design and implementation of public policies [Mason][Hankivsky]. The intersectional approach is not focused on the problem of equality but on difference; discrimination is not analyzed in terms of effective access to rights, but the conditions and capacities that people have to access those rights.

Therefore, an intersectional feminist perspective focuses on social location, the multiple layered identities people live, derived from social relations, history and structures of power through which people can experience both oppression and privilege. These oppressions can be structural and dynamic, determined by gender, race or skin color, class, sexuality, ethnicity, age, language, geographic location, abilities or health conditions, among other factors [Symington].

The concept _matrix of domination_, introduced by [Collins] as complementary to _intersectionality_, refers to the way in which the powers that produce and reproduce intersecting oppression are organized. In summary, the concept _intersectionality_ has served to recognize people’s different experiences and social locations and with this, the need of a bottom up understanding of discrimination and oppression; in addition, the concept _matrix of domination_ turns the gaze on the context of power -institutional, political, economic and symbolic- in which intersecting oppressions operate.

1.1.1. Internet as a matrix of domination

The gender and sexual rights lens on critical internet-related rights contained in the Feminist Principles of the Internet has been built bottom up by the feminist movement [FPI], which treats most prominently people who are negatively discriminated against on the basis of their gender and sexuality, but not exclusively. Because the threats to women and queer people, whose bodies and

manifestations are already under strong, albeit sometimes invisible, social, cultural and political surveillance, an intersectional feminist analysis makes it possible to recognize how multiple oppressions affect the ways people access, use and participate on the internet.

From now on, some of these experiences will be used to identify how the Internet can enable or restrict the possibility of justice and equity among its users. For this purpose, it is useful to understand the internet as a _matrix of domination_ in the sense pointed by [Collins]: as an institutional, political, symbolic and cultural context where different intersecting oppressions are shaped and reinforced.

This document addresses the opportunities and vulnerabilities incorporated into Internet protocols for specific, traditionally discriminated groups, on the assumption that these values are inherent in technological design. Through the proposed intersectional perspective, a multilevel description of the factors, processes and social structures that affect different experiences on the Internet is presented below and, based on specific cases, an analysis will be made of how the different protocols intervene in the shaping and reinforcement of intersecting oppressions faced by users on different social locations.

1.2. Brief history of feminism and the internet

The ways in which feminists have understood, used and mobilised on the internet is significant for a baseline understanding of how internet protocols and feminism intersect. Intersectional feminist action and analysis can be collected into two strategies: addressing the status quo and creating alternatives. Feminists on the early internet embodied both.

It is important to note here that there has always existed a gender gap in access to the internet, which is exacerbated by global wealth inequality.

Since the 1980s, feminist movements have used the internet to challenge power. Globalisation. Development. Cyberfeminism. Internet governance. There is a deeper connection to the internet and social justice struggles in which communication becomes the primary strategy to address inequality. Indeed, in "A History of Feminist Engagement with Development and Digital Technologies" Anita Gurumurthy writes, "the history of the right to communicate reveals the contestation between powerful status quoist forces and those who seek transformative, global change for justice and equality."

At the same time, feminists were using the internet to create feminist space.

Author Feminista Jones argues in "Reclaiming Our Space: How Black Feminists Are Changing the World from the Tweets to the Streets" that the feminist alternative spaces have become mainstream and are leading analysis and critique of the status quo, a merging and strengthening of the two strategies that emerge from this particular historical framing.

Given these myriad expressions of feminism online and feminist movement building online, one thread is perhaps most instructive to this exercise, which we use as the basis for this document: Feminist Principles of the Internet. More about the nature of the complex community that created the Feminist Principles of the Internet can be found at feministinternet.org. The principles, drafted and revised by hundreds of feminists mostly in the global south, highlight historical feminist themes for the digital age in its main categories: access, movements, economy, expression and embodiment.

2. Methodology

- Research: Archive review, HRPC-RG documents, Use cases (bottom-up, participative process within feministinternet community (TODO))

- Presentation: principle, harm identified, related protocols and rights.

TODO

3. Feminist Principles

3.1. Access

Internet access is recognized as a human right [UNGA], but its effective guarantee depends on different and unequal social, cultural, economic and political conditions. In 2018, barely half of the world’s population has access to the internet and in 88% of countries, men have more access than women [ITU]. Geographical location, age, educational and income level, as well as gender, significantly determine how people access to the internet [WebFoundation].

The Feminist Principles of the Internet [FPI] explore a broad understanding of the term beyond technicalities. It seeks to connect the technical fact to gendered and socio-economic realities.

3.1.1. Internet access

Access must be to a universal, acceptable, affordable, unconditional, open, meaningful and equal internet, which guarantees rights rather than restricts them [FPI]. As some bodies have always been subject to social and cultural surveillance and violence because of their gender and sexuallity, their access to internet will not be satisfied with connected devices, but with safety and useful digital enviroments [SmKee].

Harms: Restricted connectivity. i.e. Middleboxes (which can be Content Delivery Networks, Firewalls, NATs or other intermediary nodes that provide 'services'besides routing). TODO

Related protocols: The end-to-end principle is important for the robustness of the network and innovation (RFC1958); Content agnosticism: Treating network traffic identically regardless of content.

Related rights: Freedom of expression, freedom of association.

3.1.2. Access to information

Women and queer people have traditionally had restricted their reproductive and sexual rights. Today their rights are resticted in different levels and qualities in differents countries and regions. It is necessary to guarantee access to relevant information related to sexual and reproductive health and rights, pleasure, safe abortion, access to justice, and LGBTIQ+ issues.

Harms: Some goverments and ISPs block pages with this content or monitor online activity by sexual and gender related terminology. Therefore the considerations for anticensorship internet infrastructure technologies also consider, and can possibly alleviate, a gendered component to using the internet.

TODO. Blocked sites, Monitoring by content, identify users by IP or type of traffic.

Related protocols: Information in one's own language is the first condition, as pointed out with the cencept of 'Localization' [RFC8280], referred to the act of tailoring an application for a different language, script, or culture, and involves not only changing the language interaction but also other relevant changes, such as display of numbers, dates, currency, and so on.

TODO. Content agnosticism: Treating network traffic identically regardless of content (but it refers to header content). Censorship resistance.

Related rights: FoE, FoA, Right to political participation, Right to participate in cultural life, arts and science.

3.1.3. Usage of technology

Beyond content, access implies the possibility to use, which means code, design, adapt and critically and sustainably use ICTs. Even though almost 75% of connected individuals are placed in the Global South [WhoseKnowledge], technology is developped mainly in rich countries where student quotas and jobs are filled mainly by men.

However, there is still a long way to go in terms of inclusion of more diverse populations in the spaces of technology development and definition of protocoles and standards for the internet infrastructure [RFC7704]. Building and engineering critical internet technology is a component of 'usage' [Knodel], one which chllenges challenge the cultures of sexism and discrimination.

Harms: Gender and race bian in algorithms, digital gender gap. Necessary to know the charset, gap. The presence of gendered subjects in the IETF RFCs and drafts archive demonstrates stereotyped male and feminine roles.

Related protocols: The concept of 'Internationalization' [RFC6365] refers to the practice of making protocols, standards, and implementations usable in different languages. This is a first step to democratize the development of technology, allowing its implementation in non-English-speaking countries.

TODO. [RFC5646] descentralization, reliability. Adaptability (permissionless innovation).

Related rights: Right to participate in cultural life, arts and science

3.2. Networked

In contexts where women do not have their rights fully guaranteed, or where sexual and gender diversity are socially condemned, the Web has served to meet, organize and resist. With the popularization of the internet, the freedom of expression of both women and other gender identities traditionally marginalized from public life and social acceptance (whom we refer to as queer) has been greatly enhanced.

By adding content in formats like text, audio and video, these groups have been able to connect with each other, as well as open spaces for discussion and visibility of topics that previously seemed vetoed. The web has become a space for activism, reclamation and protest against injustice and gender inequality. It has allowed the construction of international networks of solidarity, support and mobilization, and with this, the strengthening of feminism and other movements that fight for equal rights and for a fair recognition of difference.

3.2.1. Resistance

The internet is a space where social norms are negotiated, performed and imposed. For users it increasingly functions as an extension of offline spaces shaped by patriarchy and heteronormativity. Disident content as well as widely accepted norms and values should have the same possibilities to be added, flow and stay on the net.

Harms: content blocking, content monitoring and identification, traffic monitoring

Related to protocols: Integrity

Related rights: Freedom of expression, Freedom of association.

3.2.2. Movement building

Given the shrinking of civic space offline, the internet provides a global public space, albeit one that relies on private infrastructure [tenOever]. For social causes that push for equality, it is therefore critical that the internet be maintained as a space for alignment, protest, dissent and escape. In the scope of this document, this is a call to maintain and enable the creation of spaces for sustained feminist movement building. Ihe internet provides new and novel ways for communities to come together across borders and without limits of geolocation.

Harms: However this positive aspect of internet communications is threatened by centralised systems of control and cooptation, specifically surveillance and other online repression.

Related protocols: Association of system architectures is a concept that overlaps neatly with the ideals of real-world associations of organisations and communities. "The ultimate model of P2P is a completely decentralized system, which is more resistant to speech regulation, immune to single points of failure and have a higher performance and scalability [tenOever]." It can be descussed in terms of intersectionailty and what we mentioned about ’different

dimensions of freedom'. Maybe the 'solution' is not only P2P because it doesn't take into account different distances from and capacities related to this technology, maybe mixed with another feature?. Integrity.

Related rights: Elements of freedom of assocation as explained in the UDHR include individual and collective rights to privacy and anonymity, as discussed in more detail below.

3.2.3. Internet governance

It is critical for groups who represent civil society interests, social change and the larger public interest to challenge processes and institutions that govern the internet. This requires the inclusion of more feminists and queers at the decision-making table, which can be achieved through democratic policy making. Greater effect will be possible through diffuse ownership of and power in global and local networks.

Harms: Gender gap

Related to protocols: While there is no agreement regarding the ability of the internet to negatively or positively impact on social behaviors, or shape desirable practices [RFC8280], more women and diverse populations' participation in technical development and decision-making spaces will lead to greater possibilities for ICTs to reflect greater inclusiveness and enable less risky and harmful interactions [RFC7704].

Related rights: Right to participate in cultural life, arts and science

3.3. Economy

From a feminist perspective, it is necessary to achieve the promise of an internet that facilitates economic cooperation and collaboration. One internet that can challenge models of economic inequality and transcend into other forms where women and queer people are not relegated or in economic dependence.

3.3.1. Business models

Interrogating the capitalist logic that drives technology towards further privatisation, profit and corporate control implies open discussions on centralisation of services and the logic of vertical integration while holding nuance for the tensions between trust, reliability and diversity.

Alternative forms of economic power can be grounded in principles of cooperation, solidarity, commons, environmental sustainability and openness.

Harms: TODO

Related protocols: Centralisation of services is a current discussion in the IETF that should be informed by feminist critique of capitalist structures [Arkko]. End user centered; W3C, descentralization.

Related rights: TODO

3.3.2. Open source

The digital gender gap has relegated women and other marginalized groups to be internet users, adding content for the benefit of the platforms themselves but without a deep understanding of how these platforms work. This requires shared terminology upon which technology is created to enable experimentation and values exchange. Not only that, but documenting, promoting, disseminating, and sharing knowledge about technology is at the heart of the long-standing free software community’s ethos. This aligns with a feminist approach to technology.

Given the established community of "free software", it is important to note that freedom is not freedom for everyone, always. It is important to identify different dimensions of freedom and how it is expressed in different contexts.

Harms: TODO

Related protocols: Promoting transparency [RFC8280] and simplifying technical terminology is necessary to bridge this gap. Interoperabiliy, Open standards are important as they allow for permissionless innovation. Freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist. Open standards.

Related rights: Right to participate in cultural life, arts and science

3.4. Expression

3.4.1. Amplify

The state, the religious right and other extremist forces who monopolise discourses of morality have traditionally silence women's voices and continue to silence feminist voices and persecute women's human rights defenders.

Harms: Blocking and monitoring content, identifiyng site owners, manipulating indexed content on search engines, Trolling, coordinated attackes (DoS and DDoS).

Related protocols: Content agnosticism: Treating network traffic identically regardless of content, anti censorship.

Related rights: Freedom of expression, Freedom of association, Access to information

3.4.2. Expression

The political expression of gender has not been limited to voices, but has made use of the body and its representation. However, the use of body as a form of political expression on the internet implies a series of risks and vulnerabilities for the people involved in these movements, especially if they do not understand how internet technology works.

Harms: Surveillance, content regulations or restrictions, content blocking.

Related protocols: Confidentiality, keeping data secret from unintended listeners [BCP72]. Data protection [RFC1984]. Encryption

Related rights: Freedom of expression

3.4.3. Pornography

Women's sexual expression online is socially condemned and punushed with online gender based violence. On the other hand, queer people online sexuality is usually labeld as "harmful content". These practices evidence how overcontrolled are gendered bodies and tend to confuse the differences between sexual expression and pornography.

Users build their own public digital identities while using private communications to disseminate information, explore their sexuality in text, image and video, share their initmity with others. Pornography online, on the other hand, has to do with agency, consent, power and labour.

Harms: In internet-connected devices, it has become much easier to mix leisure and work, which implies different risks for users.

Related protocols: [RFC3675]

Related rights: Freedom of expression

4. Embodiment

Most of the threats women and queer people face on line, occur on the user levels of application and content. Most adversaries are other users, but also include institutions, platforms and governments.

For a long time, perhaps since the internet became popular, its use ceased to be a functional matter and became emotional. The access to chat rooms to connect with people at huge distances, the possibility of having personal e-mails, the appearance of social networks to share music, photos and then video, determined not only the social use of a new tool but also the configuration of digital sensitivities, understood by some as sensory extensions of the body.

The internet connections embedded have also meant a radical transformation in the way people access the internet. Much more, considering that today most internet connections, especially in the global south, are mobile connections.

Sharing personal information, and often sensitive data, through platforms that are synchronized with email accounts and other platforms where information considered non-sensitive is published, implies losing control over such information. Much more, considering that each platform hosts the information of its users according to their own terms and conditions in the treatment of data. For women and other groups marginalized by race or gender, these risks are greater.

Just as the internet connection can be considered an extension of the body, social problems such as discrimination and exclusion have been projected into the digital environment- sometimes intensified, sometimes reconfigured. And once again, women, queers, racialized people are the most vulnerable. Most of the threats they face on line, occur in the user level. Most of their "adversaries" are other users, who also act at the user level, with technical or social skills that threaten participation and expressions. Institutions, platforms and governments who are adversarial have great advantage.

At this point, what level of autonomy do these people have as internet users?

4.1. Consent

Some elements of consent online include but are not limited to the following list of issues, which should be elaborated on:

- Data protection * Exposure of personal data

- Culture, design, policies and terms of service of internet platforms

- Agency lies in informed decisions * Real name policies

- Public versus private information * Dissemination of personal or intimate information * Exposure of intimacy * Unauthorized use of photos

Harms: TODO

Related protocols: TODO

Related rights: TODO

4.1.1. Privacy and data

While mentioned at the intersection of previous issues outlined above, this section is particularly critical for women, queers and marginalised populations who are already at greater risk of control and surveillance:

- Right to privacy

- Data protection

- Profit models

- Surveillance and patriarchy by states, individuals, private sector, etc. Those that enable surveillance, eg spouseware.

Harms: TODO

Related protocols: TODO

Related rights: TODO

4.1.2. Memory

One’s consent and control of the information that is available to them and about them online is a key aspect of being a fully empowered individual and community in the digital age. There are several considerations that deserve deeper inspection, such as:

- Right to be forgotten

- Control over personal history and memory on the internet

- Access all our personal data and information online

- Delete forever

Harms: TODO

Related protocols: TODO

Related rights: TODO

4.1.3. Anonymity

While anonymity is never just about technical issues but users protection activities, it becomes more necessary to strenghten the design and functionality of networks, by default. There are several considerations for internet infrastructure related to enabling anonymity for online users. This is particularly important for marginalised groups and can be ennumerated, and expanded upon, thusly:

- Right to anonymity

- Enables other rights like freedom of expression * Censorship * Defamation, descredit * Affectations to expression channels

- Breaking social taboos and heteronormativity * Hate Speech, discriminatory expressions

- Discrimination and safety from discrimination

Harms: TODO

Related protocols: TODO

Related rights: TODO

4.1.4. Children

TODO

Harms: TODO

Related protocols: TODO

Related rights: TODO

4.2. Online violence

Where women and queer people have traditionally been marginalized, their participation in the internet is rejected through different forms of violence by other users, as well as institutions, platforms and governments. But the effects of these violences, which are nothing more than extensions of the traditional violence that these groups and individuals face in social life, increase to the extent that there is not enough technical knowledge to neutralize them, and this is the case of most people who struggle for the recognition of their gender difference.

The security considerations to counter online violence are critical. There is opportunity in a connected world for those who would perpetuate violence against women and other marginalised groups through the use of internet-enabled technologies, from the home to the prison.

Privacy is a critical component of security for populations at risk. The control of information is linked to privacy. Where some would like privacy in order to live privately, others need privacy in order to access information and circumvent censorship and surveillance. The protection of privacy is critical for those at risk to prevent vicimisation through extortion, doxxing, and myriad other threats. Lack of privacy leads to risks such as stalking, monitoring and persistent harrassment.

While making public otherwise private details about a person can consitute a form of abuse, the converse is also a risk: Being erased from society or having one’s online identity controlled by another is a form of control and manipulation. Censorship, misinformation and coersion may consitute violence online. Other forms of non-consensual manipulation of online content includes platform "real name policies", sharing of intimate images and sexual abuse, spreading false accusations, flamming and other tactics.

Key to mitigating these threats is the element of consent.

Harms: TODO

Related protocols: TODO

Related rights: TODO

5. References not yet referenced

In plain sight, on sexuality, rights and the internet in India, Nepal and Sri Lanka https://www.genderit.org/articles/plain-sight-sexuality-rights-and-internet-india-nepal-and-sri-lanka

Human Rights and Internet Protocols: Comparing Processes and Principles https://www.apc.org/sites/default/files/ISSUE_human_rights_2.pdf

Principles of Unity for Infraestructuras Feministas https://pad.kefir.red/p/infraestucturas-feministas Feminist

Principles of the Internet https://feministinternet.org The UX Guide to Getting Consent https://iapp.org/resources/article/the-ux-guide-to-getting-consent

From steel to skin https://fermentos.kefir.red/english/aco-pele Responsible Data https://responsibledata.io

Impact for what and for whom? Digital technologies and feminist movement building internet https://www.genderit.org/feminist-talk/impact-what-and-whom-digital-technologies-and-feminist-movement-building

Design Justice https://docs.google.com/presentation/d/1J3ZWBgxe0QFQ8OmUr-QzE6Be8k_sI7XF0VWu4wfMIVM/edit#slide=id.gcad8d6cb9_0_198

Design Action Collective Points of Unity https://designaction.org/about/points-of-unity

CODING RIGHTS; INTERNETLAB. Violencias de genero na internet: diagnostico, solucoes e desafios. Contribuicao conjunta do Brasil para a relatora especial da ONU sobre violencia contra a mulher. Sao Paulo, 2017. https://www.codingrights.org/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_v061.pdf

Barrera, L. y Rodriguez, C. La violencia en linea contra las mujeres en Mexico. Informe para la Relatora sobre Violencia contra las Mujeres Ms. Dubravka Šimonović. 2017.

https://luchadoras.mx/wp-content/uploads/2017/12/
Informe_ViolenciaEnLineaMexico_InternetEsNuestra.pdf

Sephard, N. Big Data and Sexual Surveillance. APC issue papers. 2016. https://www.apc.org/sites/default/files/
BigDataSexualSurveillance_0_0.pdf

6. Security Considerations

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

7. IANA Considerations

This document has no actions for IANA.

Crenshaw, K. (2018). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics [1989]. In K. T. Bartlett & R. Kennedy (Eds.), Feminist Legal Theory (1st ed., pp. 57-80; By K. Bartlett). https://doi.org/10.4324/9780429500480-5

8. Informative References

[Arkko] Arkko, J., "Considerations on Internet Consolidation and the Internet Architecture.", 2018, <https://datatracker.ietf.org/doc/draft-arkko-iab-internet-consolidation>.

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

[Collins] Collins, P., "Black Feminist Thought: Knowledge, consciousness and the politics of empowerment.", 2000.

[Comninos] Alex Comninos, ., "A cyber security Agenda for civil society: What is at stake?", 2013, <https://www.apc.org/sites/default/files/PRINT_ISSUE_Cyberseguridad_EN.pdf>.

[Crenshaw] Crenshaw, K., "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics.", 1989, <https://doi.org/10.4324/9780429500480-5>.

[Davis] Davis, ., "unknown.", n.d..

[FPI] "The Feminist Principles of the Internet.", 2015, <https://feministinternet.org>.

[Hankivsky] Hankivsky, O., "Intersectionality 101.", 2014, <http://vawforum-cwr.ca/sites/default/files/attachments/intersectionallity_101.pdf>.

[ITU] International Telecommunications Union (ITU), "Statisctics. Global, Regional and Country ICT Data.", 2018, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

[Knodel] Knodel, M. and N. ten Oever, "Terminology, Power and Offensive Language.", 2018, <https://datatracker.ietf.org/doc/draft-knodel-terminology>.

[Lorde] Lorde, ., "unknown.", n.d..

[Mason] Mason, C., "Leading at the Intersections: An Introduction to the Intersectional Approach Model for Policy and Social Change.", 2010.

[RFC1244] Holbrook, J. and J. Reynolds, "Site Security Handbook", RFC 1244, DOI 10.17487/RFC1244, July 1991, <https://www.rfc-editor.org/info/rfc1244>.

[RFC1746] Manning, B. and D. Perkins, "Ways to Define User Expectations", RFC 1746, DOI 10.17487/RFC1746, December 1994, <https://www.rfc-editor.org/info/rfc1746>.

[RFC1941] Sellers, J. and J. Robichaux, "Frequently Asked Questions for Schools", FYI 22, RFC 1941, DOI 10.17487/RFC1941, May 1996, <https://www.rfc-editor.org/info/rfc1941>.

[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>.

[RFC2122] Mavrakis, D., Layec, H., and K. Kartmann, "VEMMI URL Specification", RFC 2122, DOI 10.17487/RFC2122, March 1997, <https://www.rfc-editor.org/info/rfc2122>.

[RFC2310] Holtman, K., "The Safe Response Header Field", RFC 2310, DOI 10.17487/RFC2310, April 1998, <https://www.rfc-editor.org/info/rfc2310>.

[RFC3675] Eastlake 3rd, D., ".sex Considered Dangerous", RFC 3675, DOI 10.17487/RFC3675, February 2004, <https://www.rfc-editor.org/info/rfc3675>.

[RFC3694] Danley, M., Mulligan, D., Morris, J., and J. Peterson, "Threat Analysis of the Geopriv Protocol", RFC 3694, DOI 10.17487/RFC3694, February 2004, <https://www.rfc-editor.org/info/rfc3694>.

[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>.

[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>.

[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>.

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

[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>.

[SmKee] Jac Sm Kee, ., "Imagine a Feminist Internet.", 2018, <http://link.springer.com/10.1057/s41301-017-0137-2>.

[Symington] Symington, A., "Intersectionality: a Tool for Gender and Economic Justice.", 2004, <https://www.awid.org/sites/default/files/atoms/files/intersectionality_a_tool_for_gender_and_economic_justice.pdf>.

[Tao] Internet Engineering Task Force, "The Tao of the IETF.", n.d., <https://www.ietf.org/about/participate/tao>.

[tenOever]
ten Oever, N., "Freedom of Association on the Internet.", 2017, <https://datatracker.ietf.org/doc/html/draft-irtf-hrpc-association>.

[UNGA] United Nations General Assembly, "The promotion, protection and enjoyment of human rights on the Internet.", 2012, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

[WebFoundation]
Web Foundation, "Advancing Women's Rights Online: Gaps and Opportunities in Policy and Research.", 2018, <http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf>.

[WhoseKnowledge]
Whose Knowledge, "Decolonizing the Internet, Summary Report.", 2018, <https://whoseknowledge.org/wp-content/uploads/2018/10/DTI-2018-Summary-Report.pdf>.

Authors' Addresses

Juliana Guerra
Derechos Digitales

EMail: juliana@derechosdigitales.org

Mallory Knodel
ARTICLE 19

EMail: mallory@article19.org

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: 13 October 2023

N. ten Oever
University of Amsterdam
S. Couture
Université de Montréal
M. Knodel
Center for Democracy & Technology

11 April 2023

Internet Protocols and the Human Rights to Freedom of Association and Assembly

draft-irtf-hrpc-association-13

Abstract

This document explores whether the relationship between the Internet architecture and the ability of people to exercise their rights to peaceful assembly and 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 peoples 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 international norms. Finally, the document considers both the limitations on changing association and impact of "forced association" in the context of online platforms.

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 13 October 2023.

Copyright Notice

Copyright (c) 2023 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 14
  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 17
    6.2.1. Mailing lists 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 19
    6.3.4. WebRTC 19
    6.3.5. Peer-to-peer networking 20
  6.4. Universal Access: The Web 22
    6.4.1. Accessibility 22
    6.4.2. Internationalization 22
  6.5. Block Together Now: IRC and Refusals 23

7. Conclusions: What can we learn from these 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 26
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, the present document seeks to deepen the relationship between these human rights 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, 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].

This document has seen extensive discussion and review in the IRTF Human Rights Protocol Considerations (HRPC) research group and represents the consensus of that group. It is not an IETF product and is not a standard.

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. It constitutes an individual right that is exercised collectively. 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 in the digital context. This literature review is not exhaustive but aims at providing some lines of questioning that could later be used for protocol development. Second, we look at some cases of Internet protocols that are relevant to the sub-questions highlighted in the literature review and analyze how these protocols facilitate or 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 [UNGC37]. 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 for the rights 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 these rights for children with the restrictions cited above; and Article 21 of the Convention on the Rights of Persons with Disabilities [CRPD] which insists 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, and articles 10 and 11 of the African Charter on Human and Peoples Rights.

From a more philosophical perspective, Brownlee and Jenkins [Stanford] distinguish between 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. According to Brownlee and Jenkins, "assembly" 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 or commercial businesses, 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), and 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 their 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 considers restrictions of activities of free association online or activities of free association 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. In other words, free association means that only the association of people itself determines who can be a member. 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, non-governmental organizations, 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 privacy, the right to freedom of expression, and the right to 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, the 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 peoples ability to receive the information of the group and impacts 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

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 the right of freedom of association. Various other resolutions and reports have established the online applicability of the freedoms of association and assembly, most recently and authoritatively the Human Rights Committee in General Comment 37 (2020)[UNGC37]. The questions that remain 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,

there have been 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 the 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 communication technologies are not explicitly mentioned in international treaties, these treaties nevertheless apply to the online environment. The report argues that the Internet is the public sphere of the 21st century, 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 associations or assemblies in person, like a protest or demonstration. The report notes, on the other hand, the negative ways in which the Internet can also be used to promote or facilitate terrorism, 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 further our reflection:

* network shutdowns during 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 in China as a violation of freedom of expression

* the telecom company Telus’s blocking of 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 a UN Special Rapporteur noted 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 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 relevant recommendations, 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. The Internet and social media are enablers of protests, as 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. Hacking and DDoS are subject to controversy within the Internet community: some finding them legitimate acts of protest, and others not.

2. Surveillance. While the Internet facilitates association, that association in turn leaves many traces that can be used for law enforcement or for repression of political dissent. Even the threat of surveillance can deter association.

3. Anonymity and pseudonymity. Anonymity and pseudonymity can be useful protection mechanisms for those who'd like to attend online assemblies 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 build solidarity networks and identification of collective identities and goals, extend the range of local coverage to international broadcast networks and served as a platform for contestation of 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] discusses issues of FAA, specifically:

* The expansion of DNS as an enabler of association for minorities. The document argues that 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, 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 it infringes on the freedom of expression of other parties. Furthermore, often devices (such as IoT devices and routers) are enlisted in such DDoS attacks without the owner's or user's consent. Thus they do not have the possibility to exit this assembly. Therefore the document concluded that the 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. Lack of connectivity can significantly impact freedom of assembly and association. In particular, if the user cannot retrieve the reason for their inability to connect, there may not be access to due process to dispute the lack of (secure or private) connectivity, either 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 those rights. Specifically, the report mentions network shutdowns and the use of technology to surveil or crack down on protesters, leading to human rights violations. This includes facial recognition technology, among other ways to violate the privacy of people engaged in an assembly or association. The report makes it explicit that companies play a significant role, by developing, providing or selling the technology, but also by directly causing 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 determine 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. In some cases the line between protocols and applications, implementations, policies and offline realities are 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. In each section, we consider one of the questions identified in the review, and apply the protocol or application (with some overlaps) to that question.

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 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 advises to:

(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 states have an obligation to protect human rights, there has been an increasing call for non-state actors, such as companies, also 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: not only that the companys own processes should not negatively impact human rights, but also that the company 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, where technology could be used for legitimate purposes, but could also be used to limit freedom of association or assembly, this obligation 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 questions of consent, but also harm, are crucial. In the 2000s a significant part of the technical and policy debate on spam revolved around the fact that certain corporations 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. Many countries are 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 impact of their efforts would be much smaller. Conversely, 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 sifting through many messages,

other expressions would be drowned out and would be severely hampered. Allowing unlimited sending of unsolicited messages would be a blow against freedom of speech: when everyone talks, nobody can hear.

Whereas one could perhaps consider singular instances in which spam could be proportional, legitimate uses of online campaigning, or online protesting, would be drowned out by other spam. Furthermore, the individual receiving the spam never consented to receiving it. Finally, the widespread usage of spam constitutes an attack on the internet infrastructure in terms of mailservers, bandwidth, and inboxes. This in turn thus hamper the freedom of association and assembly that is happening in and is facilitated through the internet infrastructure. Finally, spam leads to spam filtering by users and mail providers on behalf of the user, this in turn might lead to the blocking of messages that a user would consent to, but that get caught in the filter.

6.1.2. DDoS

Distributed Denial of Service attacks are leveled against a server or service by a controller of multiple hosts by overloading the server or services bandwidth or resources (volume-based floods) or exploiting protocol behaviours (protocol attacks). DDoS attacks can thus stifle the right to assemble online for organisations whose websites are targeted. 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. Their commonalities are their volume, and the unrequested nature of participation in DDoS and the receiving of spam. One could say that the ’receivers’ of demonstrations did not ask for it either, but in the case of spam the receivers are generally a larger group than one particular target, else the spam could be described as a DDoS attack against one target. 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 Internets 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 later, 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 and low-cost association: people subscribe (join) and unsubscribe (leave) as they please. Another contributor to their widespread use is that email functions on low bandwith connections and across platforms. Mailing lists also allow for association of specific groups on closed lists. This enables agency of membership, a key component of freedom of association and assembly.

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 wish to be in contact with.

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 other 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 with positive effects on freedom of expression [Kaye]. Here we look at messaging, including 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

Email was one of the first applications of the early Internet that showed what the architecture was really capable of, allowing people to exchange messages much faster and more cheaply than communication networks could do before. This enabled many collaborations among academics and other users of the early network, showcasing the importance of email in the forming of assemblies and associations. Whereas many messaging solutions have been invented since email, it is still widely used because of its distributed architecture, reliability, and ability to function on a wide range of devices and platforms.

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, we can see how particular features of mailing lists enable or inhibit 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 mailing 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. One downside of mailing lists are the privacy and security concerns generally associated with email. End-to-end encryption with OpenPGP [RFC4880] and S/MIME [RFC5751] can keep email communications authenticated and confidential if properly configured, deployed and used, but users often do not have those protections. And with mailing lists, this protection is not typically possible, because with many lists the final recipients are not known to the sender. There have been experimental solutions to address this issue [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]: 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.

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 and barring an ISP or government from knowing which user I am on IRC, 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.

For the purposes of civic participation and freedom of association and assembly in particular, it is critical that IRCs federated design allows many interoperable, yet customisable, instances and basic assurance of confidentiality through transport encryption. IRC differs from email in the sense that it allows for real-time interaction, stimulating the sense of conversation. This allows people to organize, develop ideas as well as joint identities. This is strengthened through the federated nature of IRC, which gives users the ability to use and connect through different servers, contributing to freedom of association. 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. This facilitates exchanges over the Internet in a similar manner to IRC, but including the usage of audio and video. WebRTC can be configured as direct peer-to-peer videochat without sending data through a central server. This ability to function without a central server is a strong

facilitator of freedom of association and assembly.

However, WebRTC 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 also exists in offline spaces, but may generally be easier to analyze for the user. Security and privacy expectations of the user could be either improved or made explicit. This in turn would result in a more secure and private exercise of the right to freedom of assembly or association.

6.3.5. Peer-to-peer networking

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]. However, the foundational networking protocol of the modern Internet, the Border Gateway Protocol [RFC1163] [RFC1164] [RFC4271], still functions like original peer to peer network, with an extensive practice of peering and transit [MeierHahn2015]. For an example higher up the stack one could look at the peer-to-peer architecture of BitTorrent [RFC5694].

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."

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 doesnt 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. 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 the architecture 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. 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].

Whether for resource sharing or data sharing, P2P systems enable freedom of assembly and association. Not only do they allow for effective dissemination of information, but they also leverage computing resources and diminish the costs 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. This makes the system unpredictable: a resource might be only sometimes available, and some other resources might be missing or incomplete [Vu]. Lack of information might in turn make association or assembly more difficult.

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?

6.4.1. Accessibility

The W3C has done significant work to ensure that the Web is accessible to people with diverse physical abilities [W3C]. For example, the implementation of accessibility standards helps people who have issues with seeing or rendering images to understand what the image depicts. 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.

6.4.2. Internationalization

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 Earths population speaks English, whereas only 360 million speak English as their first language. [RFC2277] states 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 all speak English. As a result, it may be significantly easier for people who have a command of the English language to become a protocol developer. It could also lead to a divergence, with the development of separate protocols that are developed within large language communities that don’t use English language or 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. Communities may therefore be driven to rely on proprietary and non-interoperable services, such as Facebook and Weibo, where use of their own script and language is supported.

When Ramsey Nasser developed the Arabic programming language (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 historically programming tools used the ASCII character set, which encodes Latin characters and was based on the English language. Though modern tools use Unicode, there persist cultural biases in computer science and engineering down to the level of code. Despite long significant efforts, it is still largely impossible to register an email address

in a language such as Devanagari, Arabic, or Chinese. Even where possible, it is to be expected that there will be a significant failure rate in sending and receiving emails to and from other services. This makes it harder for people who do not speak English and/or dont use the 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 powers 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].

Moderation and de-federation can be a tool to uphold freedom of association and assembly, because it allows groups to have control over their own make up. 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. However, these controls can also seriously hamper the ability of a group to get together. Some argue that the low cost of creating a new group is a protection against this, however, this could lead to a repetition of crises of moderation of membership and speech.

7. Conclusions: What can we learn from these 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 can easily conclude 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, if and when participation 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 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 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 people’s 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 potential impacts of Internet technologies should be assessed, reflecting recommendations of various UN bodies and international norms.

Lastly, the increasing shift away from federated and interoperable messaging exchange towards closed platforms with non-interoperable chat and media-sharing functionality have a significant impact on the distributed and open nature of the use of the Internet. Often these platforms are built on open protocols but do not allow for interoperability or data portability. Future research could further investigate how the use of social media platforms has enabled individuals to associate in groups, but at the same time rendered those groups unable to change or transcend platforms, therefore leading to sorts of "bounded association" and "forced association" both of which inhibit people from fully exercising their freedom of assembly and association.

8. Acknowledgements

* Gisela Perez de Acha for co-authoring the first versions of this document

* Fred Baker and Jefsey 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.

* Nick Doty, 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.

* Efforts put in this document by Niels ten Oever were made possible through funding from the Ford Foundation, the Open Technology Fund, and the Dutch Research Council (NWO) through grant MVI.19.032 as part of the program 'Maatschappelijk Verantwoord Innoveren (MVI)'.

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/mailinglists.pdf>.

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

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

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

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

[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>.

[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>.

[MeierHahn2015]
Uta Meier-Hahn, "Creating connectivity: trust, distrust and social microstructures at the core of the internet", 2015, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587843>.

[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/rfc/rfc1>.

[RFC0155] North, J., "ARPA Network mailing lists", RFC 155, DOI 10.17487/RFC0155, May 1971, <https://www.rfc-editor.org/rfc/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/rfc/rfc903>.

[RFC1163] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1163, DOI 10.17487/RFC1163, June 1990, <https://www.rfc-editor.org/rfc/rfc1163>.

[RFC1164] Honig, J., Katz, D., Mathis, M., Rekhter, Y., and J. Yu, "Application of the Border Gateway Protocol in the Internet", RFC 1164, DOI 10.17487/RFC1164, June 1990, <https://www.rfc-editor.org/rfc/rfc1164>.

[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/rfc/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/rfc/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/rfc/rfc1930>.

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

[RFC2810] Kalt, C., "Internet Relay Chat: Architecture", RFC 2810, DOI 10.17487/RFC2810, April 2000, <https://www.rfc-editor.org/rfc/rfc2810>.

[RFC2812] Kalt, C., "Internet Relay Chat: Client Protocol", RFC 2812, DOI 10.17487/RFC2812, April 2000, <https://www.rfc-editor.org/rfc/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/rfc/rfc3233>.

[RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/guidingprinciplesbusinesshr_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>.

[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

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
Internet-Draft
Updates: 8280 (if approved)
Intended status: Informational
Expires: 15 August 2024

G. Grover
N. ten Oever
University of Amsterdam

12 February 2024

Guidelines for Human Rights Protocol and Architecture Considerations
draft-irtf-hrpc-guidelines-21

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 (HRPC) 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 15 August 2024.

Copyright Notice

Copyright (c) 2024 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 7
3.5. Tracing impacts of implementations 7
4. Guidelines for human rights considerations 7
4.1. Intermediaries 8
4.2. Connectivity 9
4.3. Reliability 9
4.4. Content signals 10
4.5. Internationalization 11
4.6. Localization 12
4.7. Open Standards 13
4.8. Heterogeneity Support 15
4.9. Adaptability 16
4.10. Integrity 17
4.11. Authenticity 17
4.12. Confidentiality 18
4.13. Security 20
4.14. Privacy 20
4.15. Anonymity and Pseudonymity 21
4.15.1. Pseudonymity 22
4.15.2. Unlinkability 23
4.16. Censorship resistance 23
4.17. Outcome Transparency 24
4.18. Accessibility 25
4.19. Decentralization 26

4.20. Remedy 26
4.21. Misc. considerations 27
5. Document Status 28
6. Acknowledgements 28
7. Security Considerations 28
8. IANA Considerations 28
9. Research Group Information 29
10. Informative References 29
Authors' Addresses 36

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. [HR-RT] 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 HRPC 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 neither standardized nor 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, were not discussing all human rights because not all human rights are relevant to information and communication technologies (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 UN 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. 711), 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 be done by any participant, and 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.

Human rights review can be done by document authors, document shepherds, members of review teams, advocates, or impacted communities to influence the standard development process. IETF documents can benefit from people with different knowledges, perspectives, and backgrounds, especially since their implementation can impact many different communities as well.

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 4. 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 Request For Comments (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. Intermediaries

Question(s): Does your protocol depend on or allow for protocol-specific functions at intermediary nodes?

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. When a protocol exchange includes both endpoints and an intermediary, there are new opportunities for failure, especially when the intermediary is not under control of either endpoint, or even largely invisible to it, as, for instance, in intercepting HTTPS proxies [https-interception]. This pattern also contributes to ossification, because the intermediaries may impose protocol restrictions sometimes in violation of the specification that prevent the endpoints from using more modern protocols, as described in Section 9.3 of [RFC8446].

Note that intermediaries are distinct from services: in the former case the third party element is part of the protocol exchange, whereas in the latter the endpoints communicate explicitly with the service. The client/server pattern provides clearer separation of responsibilities between elements than having an intermediary. However, even in client/server systems, it is often good practice to provide for end-to-end encryption between endpoints for protocol elements which are outside of the scope of the service, as in the design of MLS [I-D.ietf-mls-protocol].

Example: Encryption between the endpoints can be used to protect the protocol from interference by intermediaries. The encryption of transport layer information in QUIC [RFC9000] and of the TLS Server Name Indication field [I-D.ietf-tls-esni] are examples of this

practice. One consequence of this is to limit the extent to which network operators can inspect traffic, requiring them to have control of the endpoints in order to monitor their behavior.

Impacts:

* Right to freedom of expression

* Right to freedom of assembly and association

4.2. Connectivity

Questions(s): Is your protocol optimized for low bandwidth and high latency connections? Could your protocol also be developed in a stateless manner?

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.

Impacts:

* Right to freedom of expression

* Right to freedom of assembly and association

4.3. 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 will also have mechanisms to recover from failure gracefully, and if applicable, will allow for partial healing.

It is important here to draw a distinction between random degradation and malicious degradation. Some attacks against previous versions of TLS, for example, exploited TLS ability to gracefully downgrade to non-secure cipher suites [FREAK][Logjam] from a functional perspective, this is useful; from a security perspective, this can be disastrous.

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 TCPs ACK message [RFC0793]. 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

4.4. Content signals

Question(s): Does your protocol include explicit or implicit plaintext elements, either in the payload or headers, that can be used for differential treatment? Is there a way minimise leaking of such data to network intermediaries? If not, is there a way for deployments of the protocol to make the differential treatment (including prioritisation of certain traffic), if any, auditable for negative impacts on net neutrality?

Example: When network intermediaries are able to determine the type of content that a packet is carrying then they can use that information to discriminate in favor of one type of content and against another. This impacts users ability to send and receive the content of their choice.

As recommended in [RFC8558] protocol designers should avoid the construction of implicit signals of their content. In general, protocol designers should avoid adding explicit signals for intermediaries. In certain cases, it may be necessary to add such explicit signals, but designers should only do so when they provide clear benefit to end users (see [RFC8890] for more on the priority of constituencies). In these cases, the implications of those signal for human rights should be documented.

Note that many protocols provide signals that are intended for endpoints that can be used as implicit signals by intermediaries for traffic discrimination, either based on content (e.g., TCP port numbers) or sender/receiver (IP addresses). Where possible, these should be protected from intermediaries by encryption. In many cases e.g., IP address these signals are difficult to remove, but in other cases, such as TLS Application Layer Protocol Negotiation [RFC7301], there are active efforts to protect this data [I-D.ietf-tls-esni].

* Right to freedom of expression

* Right to non-discrimination

* Right to equal protection

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 the World Wide Web Consortium (W3C):

> "Internationalization is the design and development of a product, application or document content that enables easy localization for target audiences that vary in culture, region, or language." {{W3Ci18nDef}}

Many protocols that handle text only handle one charset (US-ASCII), or leave the question of what coded character set and encoding are used up to local guesswork (which leads, of course, to interoperability problems). If multiple charsets are permitted, they must be explicitly identified [RFC2277]. Adding non-ASCII text to a protocol allows the protocol to handle more scripts, hopefully representing users across the world. In todays world, that is normally best accomplished by allowing Unicode encoded in UTF-8 only.

In current IETF practice [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.) Although this is reasonable practice for non-user visible elements, given the IETFs mission to make the Internet a global network of networks, [RFC3935] developers should provide full and equal support for all scripts and character sets in the user-facing features of protocols and for any content they carry.

Example: See localization

Impacts:

* Right to freedom of expression

* Right to political participation

* Right to participate in cultural life, arts and science

4.6. Localization

Question(s): Does your protocol uphold the standards of internationalization? Have you made any concrete steps towards localizing your protocol for relevant audiences?

Explanation: Localization refers to the adaptation of a product, application or document content to meet the language, cultural and other requirements of a specific target market (a locale) [W3Ci18nDef]. 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). Internationalization is related to localization, but they are not the same. Internationalization is a necessary precondition for localization.

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 American Standard Code for Information Interchange (ASCII) and knowing English. This limits the ability of a large part of the worlds online population from using the Internet in a way that is culturally and linguistically accessible. An example of a standard that has taken into account the view that individuals like to have access to data in their native language can be found in [RFC5646]. The document describes a way to label information with an identifier for the language in which it is written. And this allows information to be presented and accessed in more than one language.

Impacts:

* Right to non-discrimination

* Right to participate in cultural life, arts and science

* Right to freedom of expression

4.7. Open Standards

Question(s): Is your protocol fully documented in a way that it could be easily implemented, improved, built upon and/or further developed? Do you depend on proprietary code for the implementation, running or further development of your protocol? Does your protocol favor a particular proprietary specification over technically-equivalent competing specification(s), for instance by making any incorporated vendor specification required or recommended [RFC2026]? Do you normatively reference another standard that is not available without cost (and could you do without it)? Are you aware of any patents that would prevent your standard from being fully implemented [RFC8179] [RFC6701]?

Explanation: The Internet was able to be developed into the global network of networks because of the existence of open, non-proprietary standards [Zittrain]. They are crucial for enabling interoperability. Yet, open standards are not explicitly defined within the IETF. On the subject, [RFC2026] states: Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined at the IETF. National and international groups also publish implementors agreements that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be open external standards for the purposes of the Internet Standards Process. Similarly, [RFC3935] does not define open standards but does emphasize the importance of an open process, i.e., any interested person can participate in the work, know what is being decided, and make [their] 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 standards development organizations (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

4.8. Heterogeneity Support

Question(s): Does your protocol support heterogeneity by design? Does your protocol allow for multiple types of hardware? Does your protocol allow for multiple types of application protocols? Is your protocol liberal in what it receives and handles? Will it remain usable and open if the context changes?

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 ISPs, 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 significantly contributed to the success of the internet architecture [Zittrain]. Niels Bohr famously said: Prediction is very difficult, especially if its about the future, this also holds true for future uses of the internet architecture and infrastructure. Therefore, as a rule of thumb it is important to - as far as possible - design your protocol for different devices and uses, especially at lower layers of the stack. However, if you choose not to do this, it could be relevant to document the reasoning for that.

Impacts:

* Right to freedom of expression

* Right to political participation

4.9. Adaptability

Question(s): Question: Is your protocol written in a modular fashion and does it facilitate or hamper extensibility? In this sense, 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 to assemble, collaborate, and express themselves.

Example: WebRTC generates audio and/or video data. WebRTC can be used in different locations by different parties; WebRTCs standard application programming interfaces (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

4.10. 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. Alice sends a message to Bob, which Corinne intercepts and modifies. Bob cannot see that 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

4.11. 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, DNS Security (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 that the data did not come from Alice but from Corinne.

With 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 is unable to verify whether that the data came from Alice.

Impacts:

* Right to privacy

* Right to freedom of expression

* Right to security

4.12. Confidentiality

Question(s): Does the protocol expose the transmitted data over the wire? Does the protocol expose information related to identifiers or data? If so, what does it reveal to each 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

4.13. 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

4.14. 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 privacy

* Right to non-discrimination

4.15. Anonymity and Pseudonymity

Question(s): Does your protocol make use of identifiers? Are these identifiers persistent? Are they used across multiple contexts? Is it possible for the user to reset or rotate them without negatively impacting the operation fo the protocol? Are they visible to others besides the protocol endpoints? Are they tied to real-world identities? Have you considered the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.2?

Explanation: Most protocols depend on the use of some kind of identifier in order to correlate activity over time and space. For instance:

* IP addresses are used as an identity for the source and destination for IP datagrams.

* QUIC connection identifiers are used to correlate packets belonging to the same connection.

* HTTP uses cookies to correlate multiple HTTP requests from the same client.

* Email uses email addresses of the form example@example.com (mailto:example@example.com) to identify senders and receivers.

In general, these identifiers serve a necessary function for protocol operations, by allowing them to maintain continuity. However, they can also create privacy risks. There are two major ways in which those risks manifest:

* The identifier may itself reveal the users identity in some way or be tied to an identifier which does, as is the case when E.164 (telephone) numbers are used as identifiers for instant messaging systems.

* While the identifier may not reveal the users identity, it may make it possible to link enough of a users behavior to threaten their privacy, as is the case with HTTP cookies.

Because identifiers are necessary for protocol operation, true anonymity is very difficult to achieve, but there are practices which promote user privacy even when identifiers are used.

Impacts:

* Right to non-discrimination

* Right to freedom of expression

* Right to political participation

* Right to freedom of assembly and association

4.15.1. Pseudonymity

In general, user privacy is better preserved when identifiers are pseudonymous (not tied to a users real-world identity).

Example: In the development of the IPv6 protocol, it was discussed to embed a Media Access Control (MAC) address into unique IP addresses. This would make it possible for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node. This is why standardization efforts like Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941] and MAC address randomization [draft-zuniga-mac-address-randomization] have been pursued.

Note that it is often attractive to try to create a pseudonym from a persistent identifier. This can be very difficult to do correctly in a way that does not allow for recovering the persistent identifiers.

Example: A common practice in Web tracking is to encrypt email addresses by hashing them, thus allegedly making them non-personally identifying. However, because hash functions are public operations, it is possible to dictionary search candidate email addresses and recover the original address [email-hashing].

4.15.2. Unlinkability

Even true pseudonymous identifiers can present a privacy risk if they are used across a wide enough scope. User privacy is better preserved if identifiers have limited scope both in time and space.

Example: An example is Dynamic Host Configuration Protocol (DHCP) where sending a persistent identifier as the client name was not mandatory but, in practice, done by many implementations, before [RFC7844].

Example: Third party cookies in HTTP allow trackers to correlate HTTP traffic across sites. This is the foundation of a whole ecosystem of Web tracking. Increasingly, Web browsers are restricting the use of third party cookies in order to protect user privacy.

4.16. Censorship resistance

Question(s): Does your protocol architecture facilitate censorship? Does it include choke points which are easy to use for censorship? Does it expose identifiers which can be used to selectively block certain kinds of trafic? Could it be designed to be more censorship resistant? Does your protocol make it apparent or transparent when access to a resource is restricted and the reasons why it is restricted?

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: The current design of the Web has a number of architectural choke points where it is possible for censors to intervene. These include obtaining the control of the domain name itself, DNS blocking at either the protocol layer or at the resolver, IP address blocking, and blocking at the Web server. There has been extensive work on content distribution systems which are intended to be more censorship resistant, and some, such as BitTorrent, are in wide use, but these systems may have inferior reliability and performance compared to the Web (e.g., they do not support active content on the server).

Example: Identifiers of content exposed within a protocol might be used to facilitate censorship by allowing the censor to determine which traffic to block. DNS queries, the host request header in an HTTP request, the Server Name Indication (SNI) in a Transport Layer

Security (TLS) ClientHello are all examples of protocol elements that can travel in plaintext and be used by censors to identify what content a user is trying to access. [draft-irtf-pearg-censorship]. Protocol mechanisms such as Encrypted Client Hello [I-D.ietf-tls-esni] or DNS over HTTPS [RFC8484] that encrypt metadata provide some level of resistance to this type of protocol inspection. Full traffic encryption systems such as Tor [https://torproject.org] can also be used by people access otherwise censored resources.

Example: As noted above, one way to censor Web traffic is to require the server to block it or require internet service providers to block requests to the server. In HTTP, denial or restriction of access can be made apparent by the use of status code 451, which allows server operators and intermediaries 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.

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

4.17. Outcome Transparency

Question(s): Are the intended and forseen effects of your protocol documented and easily comprehensible?

Explanation: Certain technical choices may have unintended consequences. Have you described the central use case(s) for your protocol with a clear description of expected behavior and how it may, or may not, impact other protocols, implementations, user expectations, or behavior? Have you reviewed other protocols that solve similar problems, or make use of similar mechanisms, to see if there are lessons that can be learnt from their use and misuse?

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. Unexpected outcomes might not be technical, but rather architectural, social or economic. Therefore it is of importance to document the intended outcomes and other possible outcomes that have been considered.

Impacts:

* Right to freedom of expression

* Right to privacy

* Right to freedom of assembly and association

* Right to access to information

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 work done in the AVT and AVTCORE working groups in the IETF that enables text conversation in multimedia, text telephony, wireless multimedia and video communications for sign language and lip-reading (i.e., [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 ISPs, 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 partys 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, current mechanisms in protocols that try to enable attribution to individuals impede the exercise of the right to privacy. The former UN 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 personally identifiable information to data streams as a means to enable the human right to remedy might help in identifying a violator of human rights and provide access to remedy, but this would disproportionally affect all users right to privacy, anonymous expression, and association. Furthermore, there are some recent advances in enabling abuse detection in end-to-end encrypted messaging systems, which also carry some risk to users privacy [messenger-franking][hecate].

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 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 lays out 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].

* Reese Enghardt, Joe Hall, Avri Doria, Joey Salazar, Corinne Cath-Speth, Farzaneh Badii, Sandra Braman, Colin Perkins, John Curran, Eliot Lear, Mallory Knodel, Brian Trammell, Jane Coffin, Eric Rescorla, Sofía Celi and the hrpc list for reviews and suggestions.

* Individuals who conducted human rights reviews for their work and feedback: Amelia Andersdotter, Shane Kerr, 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 rights 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., Notthingham, 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-ietf-ohai-ohttp]
Thomson, M. and C.A. Wood, "Oblivious DNS Over HTTPS", 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp>.

[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-zuniga-mac-address-randomization]
Zuniga, J.C., Bernardos, C.J., and A. Andersdotter, "MAC address randomization", 2020, <https://tools.ietf.org/html/draft-ietf-madinas-mac-address-randomization>.

[email-hashing]
Acar, G., Englehardt, S., and A. Narayanan, "Four cents to deanonymize: Companies reverse hashed email addresses", n.d., <https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/>.

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

[FREAK] "Tracking the FREAK Attack", 2015, <https://web.archive.org/web/20150304002021/https://freakattack.com/>.

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

[hecate] Issa, R., Alhaddad, N., and M. Varia, "Hecate, Abuse Reporting in Secure Messengers with Sealed Sender", 2022, <https://eprint.iacr.org/2021/1686>.

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

[HR-RT] "Human Rights Reviews", 2022, <https://github.com/IRTF-HRPC/reviews>.

[HTML5] W3C, "HTML5", 2014, <https://www.w3.org/TR/html5/>.

[https-interception]
Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J., and V. Paxson, "The Security Impact of HTTPS Interception", 2017.

[I-D.ietf-mls-protocol]
Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", 2023, <https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/>.

[I-D.ietf-tls-esni]
Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-17, 9 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-17>.

[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>.

[Logjam] Adrian, D., Bhargavan, K., and . et al, "Imperfect Forward Secrecy, How Diffie-Hellman Fails in Practice", 2015, <https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf>.

[messenger-franking]
Grubbs, P., Lu, J., and T. Ristenpart, "Message Franking via Committing Authenticated Encryption", 2017, <https://eprint.iacr.org/2017/664>.

[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", 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>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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>.

[RFC8558] Hardie, T., Ed., "Transport Protocol Path Signals", RFC 8558, DOI 10.17487/RFC8558, April 2019, <https://www.rfc-editor.org/info/rfc8558>.

[RFC8890] Nottingham, M., "The Internet is for End Users", RFC 8890, DOI 10.17487/RFC8890, August 2020, <https://www.rfc-editor.org/info/rfc8890>.

[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>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[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/guidingprinciplesbusinesshr_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-i18n.en>.

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

Authors' Addresses

Gurshabad Grover
Email: gurshabad@cis-india.org

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

Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: March 31, 2020

N. ten Oever
University of Amsterdam

September 28, 2019

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

Abstract

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

Status of This Memo

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 March 31, 2020.

Copyright Notice

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

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

Table of Contents

1. Introduction 2
2. Vocabulary Used 4
3. Research Question 4
4. Technology and Politics: a review of literature and community positions 5
4.1. Technology is value neutral 5
4.2. Some protocols are political sometimes 6
4.3. All protocols are political sometimes 6
4.4. The network of networks has its own logic and values . . 6
4.5. Protocols are inherently political 7
5. Discussion 8
6. Conclusion 9
7. Security Considerations 10
8. IANA Considerations 10
9. Acknowledgments 10
10. Research Group Information 10
11. References 10
11.1. Informative References 10
11.2. URIs 14
Author's Address 14

1. Introduction

"Standards are recipes for reality."

- Lawrence Busch

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

- Andrew L. Russell

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

-{{RFC3935}}

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

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

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

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

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

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

- the military [RFC0164] [RFC0316];

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

- and non-governmental entities [RFC0196].

Sandra Braman has foregrounded these political consideration in historical RFC in her extensively analysis of these documents [BramanII]. This document seeks to understand how this is relevant for current day Internet standardization and protocol design. The coordinating of transnational stakeholders in a process of negotiation and agreement through the development of common rules is a form of global governance [Nadvi]. Standards are among the mechanisms by which this governance is achieved, although this process is not exclusively undertaken by transnational corporations. Conformance to certain standards is often a basic condition of

participation so there are strong economic and political incentives to conform, even in the absence of legal requirements [Russell].

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

2. Vocabulary Used

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

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

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

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

Internet Standards 'An Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.' [RFC2026]

3. Research Question

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

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

In 1993 the Computer Professionals for Social Responsibility stated that 'the Internet should meet public interest objectives'. Similarly, [RFC3935] states that 'The Internet isn't value-neutral, and neither is the IETF.'. Ethics and the Internet was already a topic of an RFC by the IAB in 1989 [RFC1087], when the Internet was still looking entirely different. Nonetheless there has been a recent uptick in discussions within the IETF and IRTF about the impact of Internet protocols on human rights [RFC8280], and more generally in public debate about the impact of technology on society.

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

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

4.1. Technology is value neutral

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

4.2. Some protocols are political sometimes

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

4.3. All protocols are political sometimes

While not an absolutist standpoint it recognizes that all design decisions are subject to the law of unintended consequences, especially in a context where the interrelation between protocols is hard to predict. The system consisting of the Internet and its users is vastly complex; it is chaotic in nature; standards are voluntary; and therefore its emergent properties cannot be predicted. This concept strongly hinges on the general purpose aspect of information technology and its malleability. Whereas not all (potential) behaviours, affordances and impacts of protocols can possibly be predicted, one could, as a point of departure, consider the impact of proposed implementations.

4.4. The network of networks has its own logic and values

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

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

In the same way - in another and more recent example - the very existence of automobiles imposes physical forms on the world different from those that come from the electric tram or the horse-cart. The logic of the automobile means speed and the rapid covering of distance, which encourages suburban development and a tendency toward conurbation. But even if that did not happen, widespread

automobile use requires paved roads, and parking lots and structures. These are pressures that come from the automotive technology itself, and would not arise without that technology.

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

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

4.5. Protocols are inherently political

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

(1) because of the symbolic forms in which information is encoded;

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

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

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

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

Recent scholars of Internet infrastructure and governance have also pointed out that Internet processes and standards have become part and parcel of political processes and public policies. Several concrete examples are found within this approach, for instance, the IANA transition or global innovation policy [DeNardis]. The Raven

process in which the IETF refused to standardize wiretapping - which resulted in [RFC2804] - was an instance where an international governance body took a position that was perceived by many as political, although driven by a technical argument. The process that led to [RFC7258] is similar: the Snowden disclosures, which occurred in the political space, engendered the IETF to act. While [RFC2804] was a statement about how a protocol for wiretapping would _not_ be developed, [RFC7258] was a statement that contributed to the development of protocols such as [RFC7858], [RFC8226], and [RFC8404]. The impact of political tensions on protocol development is summarized in [Abbate] who says: "protocols are politics by other means," emphasizing the interests that are at play in the process of designing standards.

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

5. Discussion

Economics, competition, collaboration, openness, and political impact have been an inherent part of the work of the IETF since its early beginnings [Russell] [BramanII] [Abbate]. The IETF cannot ordain which standards are to be used on the networks, and it specifically does not determine the laws of regions or countries where networks are being used, but it does set open standards for interoperability on the Internet, and has done so for many of the Internet’s formative years. Because a standard is the blue-print for how to accomplish a particular task, the adopted standards have a normative effect. The standardization work at the IETF has direct implications on what is perceived as technologically possible and useful where networking technologies are being deployed, and thus its standards reflect what is considered by the technical community as feasible and good practice.

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

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

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

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

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

6. Conclusion

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

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

7. Security Considerations

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

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgments

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

10. Research Group Information

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

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

11. References

11.1. Informative References

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

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

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

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

[BramanI] Braman, S., "Internationalization of the Internet by design: The first decade", Global Media and Communication, Vol 8, Issue 1, pp. 27 - 45 , 2012, <http://people.tamu.edu/~Braman/bramanpdfs/43_internationalization.pdf>.

[BramanII] Braman, S., "The Framing Years: Policy Fundamentals in the Internet Design Process, 1969-1979", The Information Society Vol. 27, Issue 5, 2011 , 2010, <http://people.tamu.edu/~Braman/bramanpdfs/50_theframingyears.pdf>.

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

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

[DeNardis] Denardis, L., "The Internet Design Tension between Surveillance and Security", IEEE Annals of the History of Computing (volume 37-2) , 2015, <http://is.gd/7GAnFy>.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

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

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

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

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

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

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

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

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

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

11.2. URIs

[1] mailto:hrpc@ietf.org

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

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

Author's Address

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net