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 addresses the opportunities and vulnerabilities embedded within internet protocols for specific, traditionally marginalised 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.
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 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 envisioning 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 sexuality, their access to internet will not be satisfied with connected devices, but with safety and useful digital environments [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 restricted in different levels and qualities in different 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 governments 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 concept 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 developed 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 protocols and standards for the internet infrastructure [RFC7704]. Building and engineering critical internet technology is a component of ‘usage’ [Knodel], one which challenges the cultures of sexism and discrimination.

Harms: Gender and race bias 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.


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


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. The 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 discussed in terms of intersectionality 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 association 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, decentralization.

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. Interoperability, 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, identifying site owners, manipulating indexed content on search engines, Trolling, coordinated attacks (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 punished with online gender based violence. On the other hand, queer people online sexuality is usually labeled 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 intimacy 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 strengthen 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 enumerated, 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 marginalized 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 victimization through extortion, doxxing, and myriad other threats. Lack of privacy leads to risks such as stalking, monitoring and persistent harassment.

While making public otherwise private details about a person can constitute 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 coercion may constitute 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


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


From steel to skin https://fermentos.kefir.red/english/aco-pele

Responsible Data https://responsibledata.io


Design Justice https://docs.google.com/presentation/d/1J3ZWBgxe0QFQ80mUr-QzE6Be8k_sI7XF0Vwu4wfMIVM/edit#slide=id.gcad8d6cb9_0_198

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


6. Security Considerations

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

7. IANA Considerations

This document has no actions for IANA.


8. Informative References


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


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


Authors' Addresses

Juliana Guerra
Derechos Digitales
EMail: juliana@derechosdigitales.org

Mallory Knodel
ARTICLE 19
EMail: mallory@article19.org
Abstract

This document establishes the link between the Internet architecture and the ability of people to exercise their right to freedom of assembly and association online. The Internet increasingly mediates our lives, our relationships and our ability to exercise our human rights. As a forum, it provides a global public space despite being built on predominantly private infrastructure. Since Internet protocols play a central role in the management, development and use of the Internet, the relation between protocols and the aforementioned rights should be analyzed and any adverse impacts should be mitigated.

Status of This Memo

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

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

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

This Internet-Draft will expire on February 23, 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 ................................................. 3
2. Vocabulary used ............................................. 3
3. Research question .......................................... 5
4. Methodology .................................................. 5
5. Literature Review .......................................... 6
6. Cases and examples .......................................... 7
   6.1. Conversing .............................................. 7
      6.1.1. Mailing Lists ...................................... 8
      6.1.2. Multi-party video conferencing .................... 8
      6.1.3. Internet Relay Chat ................................ 9
   6.2. Peer-to-peer networks and systems ...................... 10
      6.2.1. Peer-to-peer system architectures .................. 10
      6.2.2. Version control .................................. 12
   6.3. Grouping together (identities) ......................... 12
      6.3.1. DNS .............................................. 13
      6.3.2. Autonomous Systems ............................... 13
7. Discussion: Establishing the relation ....................... 14
8. Discussion: Protocols and Platforms ........................ 15
9. Conclusions .................................................. 16
10. Acknowledgements ........................................... 17
11. Security Considerations .................................... 17
12. IANA Considerations ........................................ 17
13. Research Group Information ................................ 17
14. References .................................................. 17
   14.1. Informative References ............................... 17
   14.2. URIs ............................................... 24
Authors’ Addresses .............................................. 25
1. Introduction

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

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

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

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

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

2. Vocabulary used

Architecture The design of a structure

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

Within the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet [RFC1930].
The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs [RFC1771].


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

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

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

Infrastructure Underlying basis or structure for a functioning society, organization or community. Because infrastructure is a precondition for other activities it has a procedural, rather than static, nature due to its social and cultural embeddedness [PipekWulf] [Bloketal]. This means that infrastructure is always relational: infrastructure always develops in relation to something or someone [Bowker].

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

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

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

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

3. Research question

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

4. Methodology

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

The methodology was based on process tracing, semi-structured interviews and quantitative and qualitative document analysis which has been further validated through confirmatory research in the form of Human Rights Protocol Reviews. The relationship, proposed as a hypothesis in [RFC8280] says that there is an inherent relation between protocols, the Internet architecture, and human rights. The guidelines in [RFC8280] describe a relationship between the right to freedom of assembly and association and connectivity, security, censorship resistance, anonymity, pseudonymity, accessibility, decentralization, adaptability, and outcome transparency.

Taking into consideration the international human rights framework regarding freedom of assembly and association, the present document seeks to deepen the relationship between the Internet architecture, protocols, and standards without creating new guidelines. In that way, we continue the work proposed in [RFC8280] and follow the primary aim of the Human Rights Protocol Consideration Research Group, as laid out in its charter where one of the research aims is ‘to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly’. Even though the present work does not seek to create new guidelines, the conclusions could inform the development of new guidelines such as is done in draft-irtf-hrpc-guidelines.

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

5. Literature Review

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

In international law, the right to freedom of assembly and association protects any collective, gathered either permanently or temporarily for "peaceful" purposes. It is important to underline the property of "freedom" because the right to freedom of association and assembly is voluntary and uncoerced: anyone can join or leave a group of choice, which in turn means one should not be forced to either join, stay or leave. What constitutes a definition of "peaceful" is outside the scope of the present document.

The difference between freedom of assembly and freedom of association is merely a gradual one: the former tends to have an informal and ephemeral nature, whereas the latter refers to established and permanent bodies with specific objectives. Nonetheless, both are protected to the same degree.

Where an assembly is an intentional and temporary gathering of a collective in a private or public space for a specific purpose: demonstrations, indoor meetings, strikes, processions, rallies or even sits-in [UNHRC]; association has a more formal and established nature. It refers to a group of individuals or legal entities brought together in order to collectively act, express, pursue or defend a field of common interests [UNGA]. Think about civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions or foundations.

Even if privacy and freedom of expression are the most discussed human rights when it comes to the online world, the right to freedom of assembly and association is quintessential for the Internet. Online association and assembly are the starting point of group to mobilization in modern democracies, and even more so where physical gatherings have been impossible or dangerous [APC]. Throughout the world -from the Arab Spring to Latin American student movements and
the #WomensMarch- the Internet has played a crucial role by providing means for the fast dissemination of information otherwise mediated by the press, or even forbidden by the government [Pensado]. According to Hussain and Howard the Internet helped to "build solidarity networks and identification of collective identities and goals, extend the range of local coverage to international broadcast networks" and as platform for contestation for "the future of civil society and information infrastructure" [HussainHoward].

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

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

6. Cases and examples

As the Internet mediates collective action and collaboration, it impacts on freedom of association and assembly. To answer our research question regarding how internet architecture enable and/or inhibits such human right, we researched several independent and typical cases related to protocols that have been either adopted by the IETF, or are widely used on the Internet. Our goal is to figure out whether they facilitate freedom of assembly and association, or whether they inhibit it through their design or implementation. We also indicate, per case, the interrelation with issues in [RFC8280].

6.1. Conversing

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

6.1.1. Mailing Lists

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

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

Mailing lists’ pervasive use are partly explained because they allow for "free" association: people subscribe (join) and unsubscribe (leave) as they please. Mailing lists also allow for association of specific groups on closed lists. Furthermore, the archival function of mailinglists allows for posterior accountability and analysis. The downsides of mailinglists are similar to the ones generally associated with e-mail, except that end-to-end encryption such as OpenPGP [RFC4880] and S/MIME [RFC5751] are not possible because the final recipients are not known. There have been experimental solutions to address this issue such as Schleuder [Schleuder], but this has not been standardized or widely deployed.

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

6.1.2. Multi-party video conferencing

Multi-party video conferencing protocols like WebRTC [RFC6176] [RFC7118] allow for robust, bandwidth-adaptive, wideband and super-wideband video and audio discussions in groups. The WebRTC protocol was designed to enable responsive real-time communications over the Internet, and is instrumental in allowing streaming video and conferencing applications to run in the browser. In order to easily facilitate direct connections between computers (bypassing the need for a central server to act as a gatekeeper), WebRTC provides
functionality to automatically collect the local and public IP addresses of Internet users (ICE or STUN). These functions do not require consent from the user, and can be instantiated by sites that a user visits without their awareness. The potential privacy implications of this aspect of WebRTC are well documented, and certain browsers have provided options to limit its behavior.’ [AndersonGuarnieri].

Even though some multi-party video conferencing tools facilitate freedom of assembly and association, their own configuration might pose concrete risks for those who use them. On the one hand WebRTC is providing resilient channels of communications, but on the other hand it also exposes information about those who are using the tool which might lead to increased surveillance, identification and the consequences that might be derived from that. This is especially concerning because the usage of a VPN does not protect against the exposure of IP addresses [Crawford].

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

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

6.1.3. Internet Relay Chat

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

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

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

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

6.2. Peer-to-peer networks and systems

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

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

6.2.1. Peer-to-peer system architectures

Peer-to-peer (P2P) is essentially a model of how people interact in real life because "we deal directly with one another whenever we wish to" [Vu]. Usually if we need something we ask our peers, who in turn refer us to other peers. In this sense, the ideal definition of P2P is that "nodes are able to directly exchange resources and services between themselves without the need for centralized servers" where each participating node typically acts both as a server and as a client [Vu]. RFC 5694 has defined it as peers or nodes that should be able to communicate directly between themselves without passing intermediaries, and that the system should be self-organizing and
have decentralized control [RFC5694]. With this in mind, the ultimate model of P2P is a completely decentralized system, which is more resistant to speech regulation, immune to single points of failure and has a higher performance and scalability. Nonetheless, in practice some P2P systems are supported by centralized servers and some others have hybrid models where nodes are organized into two layers: the upper tier servers and the lower tier common nodes [Vu].

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

Whether for resource sharing or data sharing, P2P systems are enabling freedom of assembly and association. Not only do they allow for effective dissemination of information, but they leverage computing resources by diminishing costs allowing for the formation of open collectives at the network level. At the same time, in completely decentralized systems the nodes are autonomous and can join or leave the network as they want -a characteristic that makes the system unpredictable: a resource might be only sometimes available, and some other resources might be missing or incomplete [Vu]. Lack of information might in turn makes association or assembly more difficult.

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

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

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

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

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

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

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

6.3. Grouping together (identities)

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

6.3.1. DNS

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

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

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

6.3.2. Autonomous Systems

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

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

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

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

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

7. Discussion: Establishing the relation

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

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

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

8. Discussion: Protocols and Platforms

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

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

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

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

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

Given that the Internet itself was originally designed as a medium of communication for machines that share resources with each other as equals [RFC903], the Internet is now one of the most basic infrastructures for the right to freedom of assembly and association. Since Internet protocols and the Internet architecture play a central role in the management, development and use of the Internet, we established the relation between some protocols and the right to freedom of assembly and association.

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

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

   - Fred Baker, Jefsey, and Andrew Sullivan for work on Internet definitions.
   - Stephane Bortzmeyer for several concrete text suggestions that found their way in this document (such as the AS filtering example).
   - Mark Perkins and Gurshabad for finding a lot of typos.
   - Gurshabad Grover and an anonymous reviewer for a full review.
   - The hrpc mailinglist at large for a very constructive discussion on a hard topic.

11. Security Considerations

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

12. IANA Considerations

   This document has no actions for IANA.

13. Research Group Information

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

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

14. References

14.1. Informative References

[AckermannKargerZhang]

[Anderson]

[AndersonGuarnieri]


Couture, et al.  Expires February 23, 2020


14.2. URIs

[1] mailto:hrpc@ietf.org


Authors’ Addresses

Stephane Couture
University of Montreal
EMail: steph@stephcouture.info

Joseph Lorenzo Hall
CDT
EMail: joe@cdt.org

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

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

Abstract

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

Status of This Memo

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

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

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

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

Copyright Notice

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

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

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

This document outlines a set of human rights protocol considerations for protocol developers. It provides questions engineers should ask themselves when developing or improving protocols if they want to understand their potential human rights impact. It should however be noted that the impact of a protocol cannot solely be deduced from its design, but its usage and implementation should also be studied to form a full protocol human rights impact assessment.

The questions are based on the research performed by the hrpc research group which has been documented before these considerations. The research establishes that human rights relate to standards and protocols, and offers a common vocabulary of technical concepts that impact human rights and how these technical concepts can be combined to ensure that the Internet remains an enabling environment for human rights. With this, the contours of a model for developing human rights protocol considerations has taken shape.

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

2. Vocabulary used

3. Guidelines for developing human rights protocol considerations

3.1. Human rights threats

Human rights threats on the Internet come in a myriad of forms. Protocols and standards can harm or enable the right to freedom of expression, right to non-discrimination, right to equal protection, right to participate in cultural life, arts and science, right to freedom of assembly and association, and the right to security. An end-user who is denied access to certain services, data or websites may be unable to disclose vital information about the malpractices of a government or other authority. A person whose communications are monitored may be prevented from exercising their right to freedom of association or participate in political processes [Penney]. In a worst-case scenario, protocols that leak information can lead to physical danger. A realistic example to consider is when individuals perceived as threats to the state are subjected to torture or extra-judicial killing or detention on the basis of information gathered by state agencies through information leakage in protocols.
This document details several 'common' threats to human rights, indicating how each of these can lead to human rights violations/harms and present several examples of how these threats to human rights materialize on the Internet. This threat modeling is inspired by [RFC6973] Privacy Considerations for Internet Protocols, which is based on security threat analysis. This method is a work in progress and by no means a perfect solution for assessing human rights risks in Internet protocols and systems. Certain specific human rights threats are indirectly considered in Internet protocols as part of the security considerations [BCP72], but privacy considerations [RFC6973] or reviews, let alone human rights impact assessments of protocols are not standardized or implemented.

Many threats, enablers and risks are linked to different rights. This is not unsurprising if one takes into account that human rights are interrelated, interdependent and indivisible. Here however we’re not discussing all human rights because not all human rights are relevant to ICTs in general and protocols and standards in particular [Bless]: "The main source of the values of human rights is the International Bill of Human Rights that is composed of the Universal Declaration of Human Rights [UDHR] along with the International Covenant on Civil and Political Rights [ICCPR] and the International Covenant on Economic, Social and Cultural Rights [ICESCR]. In the light of several cases of Internet censorship, the Human Rights Council Resolution 20/8 was adopted in 2012 [UNHRC2016], affirming "... that the same rights that people have offline must also be protected online...". In 2015, the Charter of Human Rights and Principles for the Internet [IRP] was developed and released. According to these documents, some examples of human rights relevant for ICT systems are human dignity (Art. 1 UDHR), non-discrimination (Art. 2), rights to life, liberty and security (Art. 3), freedom of opinion and expression (Art. 19), freedom of assembly and association (Art. 20), rights to equal protection, legal remedy, fair trial, due process, presumed innocent (Art. 7–11), appropriate social and international order (Art. 28), participation in public affairs (Art. 21), participation in cultural life, protection of the moral and material interests resulting from any scientific, literary or artistic production of which [they are] the author (Art. 27), and privacy (Art. 12)." A partial catalog of human rights related to Information and Communications technologies, including economic rights, can be found in [Hill2014].

This is by no means an attempt to exclude specific rights or prioritize some rights over others. If other rights seem relevant, please contact the authors.
3.2. Conducting human rights reviews

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

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

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

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

3.2.2. Analyzing drafts based on their perceived or speculated impact

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

3.2.3. Expert interviews

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

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

3.2.5. Tracing impacts of implementations

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

3.3. Guidelines for human rights considerations

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

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

Note that the guidance provided in this section does not recommend specific practices. The range of protocols developed in the IETF is too broad to make recommendations about particular uses of data or how human rights might be balanced against other design goals. However, by carefully considering the answers to the following questions, document authors should be able to produce a comprehensive analysis that can serve as the basis for discussion on whether the protocol adequately takes specific human rights threats into account. This guidance is meant to help the thought process of a human rights analysis; it does not provide specific directions for how to write a human rights considerations section (following the example set in [RFC6973]).
In considering these questions, authors will need to be aware of the potential of technical advances or the passage of time to undermine protections. In general, considerations of rights are likely to be more effective if they are considered given a purpose and specific use cases, rather than as abstract absolute goals.

3.3.1. Connectivity

Question(s): Does your protocol add application-specific functions to intermediary nodes? Could this functionality be added to end nodes instead of intermediary nodes? Is your protocol optimized for low bandwidth and high latency connections? Could your protocol also be developed in a stateless manner?

Explanation: The end-to-end principle [Saltzer] holds that ‘the intelligence is end to end rather than hidden in the network’ [RFC1958]. The end-to-end principle is important for the robustness of the network and innovation. Such robustness of the network is crucial to enabling human rights like freedom of expression.

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

Impacts:

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

3.3.2. Privacy

Question(s): Did you have a look at the Guidelines in the Privacy Considerations for Internet Protocols [RFC6973] section 7? Does your protocol maintain the confidentiality of metadata? Could your protocol counter traffic analysis? Does your protocol adhere to data minimization principles? Does your document identify potentially sensitive data logged by your protocol and/or for how long that needs to be retained for technical reasons?

Explanation: Privacy refers to the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. [RFC4949]. If a protocol provides insufficient privacy protection it
may have a negative impact on freedom of expression as users self-censor for fear of surveillance, or find themselves unable to express themselves freely.

Example: See [RFC6973]

Impacts:
- Right to freedom of expression
- Right to non-discrimination

3.3.3. Content agnosticism

Question(s): If your protocol impacts packet handling, does it use user data (packet data that is not included in the header)? Is it making decisions based on the payload of the packet? Does your protocol prioritize certain content or services over others in the routing process? Is the protocol transparent about the prioritization that is made (if any)?

Explanation: Content agnosticism refers to the notion that network traffic is treated identically regardless of payload, with some exception where it comes to effective traffic handling, for instance where it comes to delay tolerant or delay sensitive packets, based on the header.

Example: Content agnosticism prevents payload-based discrimination against packets. This is important because changes to this principle can lead to a two-tiered Internet, where certain packets are prioritized over others on the basis of their content. Effectively this would mean that although all users are entitled to receive their packets at a certain speed, some users become more equal than others.

Impacts:
- Right to freedom of expression
- Right to non-discrimination
- Right to equal protection

3.3.4. Security

Question(s): Did you have a look at Guidelines for Writing RFC Text on Security Considerations [BCP72]? Have you found any attacks that are somewhat related to your protocol yet considered out of scope of your document? Would these attacks be pertinent to the human rights
enabling features of the Internet (as described throughout this document)?

Explanation: Security is not a single monolithic property of a protocol or system, but rather a series of related but somewhat independent properties. Not all of these properties are required for every application. Since communications are carried out by systems and access to systems is through communications channels, security goals obviously interlock, but they can also be independently provided. [BCP72].

Example: See [BCP72].

Impacts:
- Right to freedom of expression
- Right to freedom of assembly and association
- Right to non-discrimination
- Right to security

3.3.5. Internationalization

Question(s): Does your protocol have text strings that have to be understood or entered by humans? Does your protocol allow Unicode? If so, do you accept texts in one charset (which must be UTF-8), or several (which is dangerous for interoperability)? If character sets or encodings other than UTF-8 are allowed, does your protocol mandate a proper tagging of the charset? Did you have a look at [RFC6365]?

Explanation: Internationalization refers to the practice of making protocols, standards, and implementations usable in different languages and scripts (see Localization). In the IETF, internationalization means to add or improve the handling of non-ASCII text in a protocol. [RFC6365] A different perspective, more appropriate to protocols that are designed for global use from the beginning, is the definition used by W3C:

"Internationalization is the design and development of a product, application or document content that enables easy localization for target audiences that vary in culture, region, or language." {{W3C118nDef}}

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

In the current IETF policy [RFC2277], internationalization is aimed at user-facing strings, not protocol elements, such as the verbs used by some text-based protocols. (Do note that some strings are both content and protocol elements, such as the identifiers.) If IETF wants the Internet to be a global network of networks, the protocols should work with languages apart from English and character sets apart from Latin characters. It is therefore crucial that at least the content carried by the protocol can be in any script, and that all scripts are treated equally.

Example: See localization

Impacts:

- Right to freedom of expression
- Right to political participation
- Right to participate in cultural life, arts and science

3.3.6. Censorship resistance

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

Explanation: Censorship resistance refers to the methods and measures to prevent Internet censorship.

Example: In the development of the IPv6 protocol, it was discussed to embed a Media Access Control (MAC) address into unique IP addresses. This would make it possible for ‘eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node. This is why Privacy Extensions for Stateless Address Autoconfiguration in IPv6 have been introduced. [RFC4941]
Identifiers of content exposed within a protocol might be used to facilitate censorship, as in the case of Application Layer based censorship, which affects protocols like HTTP. In HTTP, denial or restriction of access can be made apparent by the use of status code 451, which allows server operators to operate with greater transparency in circumstances where issues of law or public policy affect their operation [RFC7725].

Impacts:
- Right to freedom of expression
- Right to political participation
- Right to participate in cultural life, arts and science
- Right to freedom of assembly and association

3.3.7. Open Standards

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

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

Open standards are important as they allow for permissionless innovation, which is important to maintain the freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist. It is at the heart of the Internet as we know it, and to maintain its fundamentally open nature, we need to be mindful of the need for developing open standards.

All standards that need to be normatively implemented should be freely available and with reasonable protection for patent infringement claims, so it can also be implemented in open source or free software. Patents have often held back open standardization or been used against those deploying open standards, particularly in the domain of cryptography [newegg]. An exemption of this is sometimes made when a protocol is standardized that normatively relies on specifications produced by others SDOs that are not freely available. Patents in open standards or in normative references to other standards should have a patent disclosure [notewell], royalty-free licensing [patentpolicy], or some other form of fair, reasonable and non-discriminatory terms.

Example: [RFC6108] describes a system for providing critical end-user notifications to web browsers, which has been deployed by Comcast, an Internet Service Provider (ISP). Such a notification system is being used to provide near-immediate notifications to customers, such as to warn them that their traffic exhibits patterns that are indicative of malware or virus infection. There are other proprietary systems that can perform such notifications, but those systems utilize Deep Packet Inspection (DPI) technology. In contrast, that document describes a system that does not rely upon DPI, and is instead based on open IETF standards and open source applications.

Impacts:
- Right to freedom of expression
- Right to participate in cultural life, arts and science

3.3.8. Heterogeneity Support

Question(s): Does your protocol support heterogeneity by design? Does your protocol allow for multiple types of hardware? Does your protocol allow for multiple types of application protocols? Is your protocol liberal in what it receives and handles? Will it remain usable and open if the context changes? Does your protocol allow
there to be well-defined extension points? Do these extension points allow for open innovation?

Explanation: The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and Internet service providers, each with their own separate policy concerns, there is a large heterogeneity of administrative domains and pricing structures. As a result, the heterogeneity principle proposed in [RFC1958] needs to be supported by design [FIArch].

Example: Heterogeneity is inevitable and needs be supported by design. Multiple types of hardware must be allowed for, e.g. transmission speeds differing by at least 7 orders of magnitude, various computer word lengths, and hosts ranging from memory-starved microprocessors up to massively parallel supercomputers. Multiple types of application protocols must be allowed for, ranging from the simplest such as remote login up to the most complex such as commit protocols for distributed databases. [RFC1958].

Impacts:
- Right to freedom of expression
- Right to political participation

3.3.9. Pseudonymity

Question(s): Have you considered the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.2? Does the protocol collect personally derived data? Does the protocol generate or process anything that can be, or be tightly correlated with, personally identifiable information? Does the protocol utilize data that is personally-derived, i.e. derived from the interaction of a single person, or their device or address? Does this protocol generate personally derived data, and if so how will that data be handled?

Explanation: Pseudonymity - the ability to use a persistent identifier not linked to one’s offline identity - is an important feature for many end-users, as it allows them different degrees of disguised identity and privacy online.
Example: While designing a standard that exposes personal data, it is important to consider ways to mitigate the obvious impacts. While pseudonyms cannot be simply reverse engineered - some early approaches simply took approaches such as simple hashing of IP addresses, these could then be simply reversed by generating a hash for each potential IP address and comparing it to the pseudonym - limiting the exposure of personal data remains important.

Pseudonymity means using a pseudonym instead of one’s "real" name. There are many reasons for users to use pseudonyms, for instance to: hide their gender, protect themselves against harassment, protect their families’ privacy, frankly discuss sexuality, or develop a artistic or journalistic persona without repercussions from an employer, (potential) customers, or social surrounding.

[geekfeminism] The difference between anonymity and pseudonymity is that a pseudonym often is persistent. "Pseudonymity is strengthened when less personal data can be linked to the pseudonym; when the same pseudonym is used less often and across fewer contexts; and when independently chosen pseudonyms are more frequently used for new actions (making them, from an observer’s or attacker’s perspective, unlinkable)." [RFC6973]

Impacts:
- Right to non-discrimination
- Right to freedom of assembly and association

3.3.10. Accessibility

Question(s): Is your protocol designed to provide an enabling environment for people who are not able-bodied? Have you looked at the W3C Web Accessibility Initiative for examples and guidance?

Explanation: Sometimes in the design of protocols, websites, web technologies, or web tools, barriers are created that exclude people from using the Web. The Internet should be designed to work for all people, whatever their hardware, software, language, culture, location, or physical or mental ability. When the Internet technologies meet this goal, it will be accessible to people with a diverse range of hearing, movement, sight, and cognitive ability.

[W3CAccessibility]

Example: The HTML protocol as defined in [HTML5] specifically requires that every image must have an alt attribute (with a few exceptions) to ensure images are accessible for people that cannot themselves decipher non-text content in web pages.
3.3.11. Localization

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

Explanation: Localization refers to the adaptation of a product, application or document content to meet the language, cultural and other requirements of a specific target market (a locale) [W3CIntDef]. It is also described as the practice of translating an implementation to make it functional in a specific language or for users in a specific locale (see Internationalization).

Example: The Internet is a global medium, but many of its protocols and products are developed with a certain audience in mind, that often share particular characteristics like knowing how to read and write in ASCII and knowing English. This limits the ability of a large part of the world’s online population from using the Internet in a way that is culturally and linguistically accessible. An example of a protocol that has taken into account the view that individuals like to have access to data in their native language can be found in [RFC5646]. This protocol labels the information content with an identifier for the language in which it is written. And this allows information to be presented in more than one language.

Impacts:

- Right to non-discrimination
- Right to participate in cultural life, arts and science
- Right to freedom of expression

3.3.12. Decentralization

Question(s): Can your protocol be implemented without a single point of control? If applicable, can your protocol be deployed in a federated manner? What is the potential for discrimination against
users of your protocol? How can your protocol be used to implicate users? Does your protocol create additional centralized points of control?

Explanation: Decentralization is one of the central technical concepts of the architecture of the networks, and embraced as such by the IETF [RFC3935]. It refers to the absence or minimization of centralized points of control, a feature that is assumed to make it easy for new users to join and new uses to unfold [Brown]. It also reduces issues surrounding single points of failure, and distributes the network such that it continues to function even if one or several nodes are disabled. With the commercialization of the Internet in the early 1990s, there has been a slow move away from decentralization, to the detriment of the technical benefits of having a decentralized Internet.

Example: The bits traveling the Internet are increasingly susceptible to monitoring and censorship, from both governments and Internet service providers, as well as third (malicious) parties. The ability to monitor and censor is further enabled by the increased centralization of the network that creates central infrastructure points that can be tapped 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

3.3.13. Reliability

Question(s): Is your protocol fault tolerant? Does it downgrade gracefully? Can your protocol resist malicious degradation attempts? Do you have a documented way to announce degradation? Do you have measures in place for recovery or partial healing from failure? Can your protocol maintain dependability and performance in the face of unanticipated changes or circumstances?

Explanation: Reliability ensures that a protocol will execute its function consistently and error resistant as described, and function without unexpected result. A system that is reliable degenerates gracefully and will have a documented way to announce degradation. It also has mechanisms to recover from failure gracefully, and if applicable, allow for partial healing. It is important here to draw
a distinction between random degradation and malicious degradation. Many current attacks against TLS, for example, exploit TLS’ ability to gracefully downgrade to older cipher suites - from a functional perspective, this is good; from a security perspective, this can be very bad. As with confidentiality, the growth of the Internet and fostering innovation in services depends on users having confidence and trust [RFC3724] in the network. For reliability, it is necessary that services notify the users if a delivery fails. In the case of real-time systems in addition to the reliable delivery the protocol needs to safeguard timeliness.

Example: In the modern IP stack structure, a reliable transport layer requires an indication that transport processing has successfully completed, such as given by TCP’s ACK message [RFC0793], and not simply an indication from the IP layer that the packet arrived. Similarly, an application layer protocol may require an application-specific acknowledgment that contains, among other things, a status code indicating the disposition of the request (See [RFC3724]).

Impacts:
- Right to freedom of expression
- Right to security

3.3.14. Confidentiality

Question(s): Does this protocol expose information related to identifiers or data? If so, does it do so to each other protocol entity (i.e., recipients, intermediaries, and enablers) [RFC6973]? What options exist for protocol implementers to choose to limit the information shared with each entity? What operational controls are available to limit the information shared with each entity?

What controls or consent mechanisms does the protocol define or require before personal data or identifiers are shared or exposed via the protocol? If no such mechanisms or controls are specified, is it expected that control and consent will be handled outside of the protocol?

Does the protocol provide ways for initiators to share different pieces of information with different recipients? If not, are there mechanisms that exist outside of the protocol to provide initiators with such control?

Does the protocol provide ways for initiators to limit the sharing or express individuals’ preferences to recipients or intermediaries with regard to the collection, use, or disclosure of their personal data?
If not, are there mechanisms that exist outside of the protocol to provide users with such control? Is it expected that users will have relationships that govern the use of the information (contractual or otherwise) with those who operate these intermediaries? Does the protocol prefer encryption over clear text operation?

Explanation: Confidentiality refers to keeping your data secret from unintended listeners [BCP72]. The growth of the Internet depends on users having confidence that the network protects their personal data [RFC1984].

Example: Protocols that do not encrypt their payload make the entire content of the communication available to the idealized attacker along their path. Following the advice in [RFC3365], most such protocols have a secure variant that encrypts the payload for confidentiality, and these secure variants are seeing ever-wider deployment. A noteworthy exception is DNS [RFC1035], as DNSSEC [RFC4033] does not have confidentiality as a requirement. This implies that, in the absence of the use of more recent standards like DNS over TLS [RFC7858] or DNS over HTTPS [RFC8484], all DNS queries and answers generated by the activities of any protocol are available to the attacker. When store-and-forward protocols are used (e.g., SMTP [RFC5321]), intermediaries leave this data subject to observation by an attacker that has compromised these intermediaries, unless the data is encrypted end-to-end by the application-layer protocol or the implementation uses an encrypted store for this data [RFC7624].

Impacts:
- Right to privacy
- Right to security

3.3.15. Integrity

Question(s): Does your protocol maintain, assure and/or verify the accuracy of payload data? Does your protocol maintain and assure the consistency of data? Does your protocol in any way allow for the data to be (intentionally or unintentionally) altered?

Explanation: Integrity refers to the maintenance and assurance of the accuracy and consistency of data to ensure it has not been (intentionally or unintentionally) altered.

Example: Integrity verification of data is important to prevent vulnerabilities and attacks from on-path attackers. These attacks happen when a third party (often for malicious reasons) intercepts a
communication between two parties, inserting themselves in the middle changing the content of the data. In practice this looks as follows:

Alice wants to communicate with Bob.
Corinne forges and sends a message to Bob, impersonating Alice.
Bob cannot see the data from Alice was altered by Corinne.
Corinne intercepts and alters the communication as it is sent between Alice and Bob.
Corinne is able to control the communication content.

Impacts:
- Right to freedom of expression
- Right to security

3.3.16. Authenticity

Question(s): Do you have sufficient measures to confirm the truth of an attribute of a single piece of data or entity? Can the attributes get garbled along the way (see security)? If relevant, have you implemented IPsec, DNSsec, HTTPS and other Standard Security Best Practices?

Explanation: Authenticity ensures that data does indeed come from the source it claims to come from. This is important to prevent certain attacks or unauthorized access and use of data.

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

Example: Authentication of data is important to prevent vulnerabilities, and attacks from on-path attackers. These attacks happen when a third party (often for malicious reasons) intercepts a communication between two parties, inserting themselves in the middle and posing as both parties. In practice this looks as follows:

Alice wants to communicate with Bob.
Alice sends data to Bob.
Corinne intercepts the data sent to Bob.
Corinne reads (and potentially alters) the message to Bob.
Bob cannot see the data did not come from Alice but from Corinne.

When there is proper authentication the scenario would be as follows:

Alice wants to communicate with Bob.
Alice sends data to Bob.
Corinne intercepts the data sent to Bob. Corinne reads and alters the message to Bob. Bob can see the data did not come from Alice.

Impacts:
- Right to privacy
- Right to freedom of expression
- Right to security

3.3.17. Adaptability

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

Explanation: Adaptability is closely interrelated with permissionless innovation: both maintain the freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist. It is at the heart of the Internet as we know it, and to maintain its fundamentally open nature, we need to be mindful of the impact of protocols on maintaining or reducing permissionless innovation to ensure the Internet can continue to develop.

Example: WebRTC generates audio and/or video data. In order to ensure that WebRTC can be used in different locations by different parties, it is important that standard Javascript APIs are developed to support applications from different voice service providers. Multiple parties will have similar capabilities, in order to ensure that all parties can build upon existing standards these need to be adaptable, and allow for permissionless innovation.

Impacts:
- Right to education
- Freedom of expression
- Freedom of assembly and association

3.3.18. Outcome Transparency

Question(s): Are the effects of your protocol fully and easily comprehensible, including with respect to unintended consequences of protocol choices?
Explanation: Certain technical choices may have unintended consequences.

Example: Lack of authenticity may lead to lack of integrity and negative externalities, of which spam is an example. Lack of data that could be used for billing and accounting can lead to so-called "free" arrangements which obscure the actual costs and distribution of the costs, for example the barter arrangements that are commonly used for Internet interconnection; and the commercial exploitation of personal data for targeted advertising which is the most common funding model for the so-called "free" services such as search engines and social networks. Other unexpected outcomes might not be technical, but rather architectural, social or economical.

Impacts:
- Freedom of expression
- Privacy
- Freedom of assembly and association
- Access to information

3.3.19. Anonymity

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

Explanation: Anonymity refers to the condition of an identity being unknown or concealed [RFC4949]. Even though full anonymity is hard to achieve, it is a non-binary concept. Making pervasive monitoring and tracking harder is important for many users as well as for the IETF [RFC7258]. Achieving a higher level of anonymity is an important feature for many end-users, as it allows them different degrees of privacy online. Anonymity is an inherent part of the right to freedom of opinion and expression and the right to privacy. Avoid adding identifiers, options or configurations that create or might lead to patterns or regularities that are not explicitly required by the protocol.

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

Often protocols expose personal data, it is important to consider ways to mitigate the obvious privacy impacts. A protocol that uses data that could help identify a sender (items of interest) should be protected from third parties. For instance, if one wants to hide the source/destination IP addresses of a packet, the use of IPsec in tunneling mode (e.g., inside a virtual private network) can be helpful to protect from third parties likely to eavesdrop packets exchanged between the tunnel endpoints.

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

Impacts:
- Right to non-discrimination
- Right to political participation
- Right to freedom of assembly and association
- Right to security

4. Document Status

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

5. Acknowledgements

Thanks to:
- Corinne Cath for work on [RFC8280].
- Theresa Engelhard, Joe Hall, Avri Doria and the hrpc list for reviews and suggestions.
- The Human Rights Review Team for implementing and improving the guidelines.
6. Security Considerations

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

7. IANA Considerations

This document has no actions for IANA.

8. Research Group Information

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

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

9. References

9.1. Informative References


9.2. URIs

[1] mailto:hrpc@ietf.org

Authors’ Addresses

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

Gurshabad Grover
Centre for Internet and Society
EMail: gurshabad@cis-india.org
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.
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 is 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 document 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 absolutely 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 document 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 the 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 position 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 Philosophy 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


11.2. URIs

[1] mailto:hrpc@ietf.org

Author’s Address

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net