Abstract

This document aims to describe how internet standards and 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 September 12, 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.
Feminism and protocols

1.1. Introduction

The experiences and learnings of the feminist movement in the digital age have extrapolated feminist discourse towards building a more just world to envisioning a more just internet, namely one that recognizes differences across a variety of lived experience and identity. The framework that is used to analyse and research internet protocols and standards through a feminist lens is a document called The Feminist Principles of the Internet. In a series of 17 statements, drafted, redrafted and revised by hundreds of activists, the Principles offer...
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. Likewise, this is an attempt to bring a conversation on the intersection of feminism and internet technology into the technical community.

Attempts have been made to highlight where terminology occurs in both technical standards and feminist discourse and distinguish between the two in a meaningful way. A concept like ‘security’, for example, has differing contextual meanings in internet engineering and feminism. Coming to a shared understanding of concepts and terminology is one goal of this document. With a better understanding of concepts and terms, together the technical and feminist communities can attempt to recognize and discuss how the technical decisions with regard to internet infrastructure, standards and protocols, directly or indirectly may affect internet users around the world.

The Principles, like this document, are not designed 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. They express the kind of internet that feminists would like to have, and with whom to collaborate and imagine.

1.2. Intersectional feminism and diversity

Why feminism and not gender? The gender and sexual rights lens on critical internet-related rights has been built bottom up by the feminist movement. Feminism 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, a critical feminist analysis also applies to other marginalised groups. Aiming to use a feminist framework to analyse the impacts of internet protocols on society assumes that values are inherent to technological design. What follows are specifics of how those values can either support or create barriers for gender justice and equity for internet users.

1.3. Brief history of feminism and the internet

It is significant to highlight the ways in which feminists have understood, used and mobilised on the internet. Given myriad expressions of feminism online and feminist movement building online, one thread is perhaps instructive to this exercise. More about the nature of the complex community that created the Feminist Principles of the Internet can be found at feministinternet.org.
1.4. 2. Expression as a framework of understanding

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 will refer to as queer) has been greatly enhanced. 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.

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.

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. In this sense, it is important to recognize that freedom of expression on the internet, and in general its use, is determined by gender, along with other social, economic, political and cultural conditions.

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 violence, 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.

These "use cases" must be known within the IETF, in order to join efforts for the elimination of online gender-based violence, which today seems to be a rule in digital environments. In order to identify ways and strategies to contribute to this purpose, we review below the ways in which both _safety_ and _gender_ have been approached in IETF rfc's and drafts. The following sections consist of a preliminary analysis of the terms used in the IETF drafts and RFCs archive.
By filtering from specific terms, the analysis consists of identifying patterns and regularities in the contexts in which these terms are used. For example, if they are used as an example in "use cases" or if they are part of a technical explanation, and if they are normally accompanied by other terms. The analysis presented is only an initial revision that must be completed and synthesized.

1.4.1.  2.1.  Safety

For the last years, there has been criticism of the way in which digital security accompaniments, advice and training are developed for people who are not directly involved in the development of information technology. It is worth mentioning that digital security, unlike cybersecurity, is more geared towards internet users [Comminos]. Some of these criticisms refer to the fact that the approach to digital security is centred on tools and not on usage practices, and "attacks", "adversaries" or "enemies" in a generic way, without recognizing the specific contexts in which different information protection needs are generated.

Given the common incidents suffered by women and queer people, from a gender perspective it has been preferred to use the term _safety_ to recognize their main need to be able to inhabit digital environments without being the target of attacks such as trolling, harassment, stalking, threats, non-consensual dissemination of intimate images, among others. When speaking of _safety_ rather than _security_, their participation is recognized as users at the most surface level, not as administrators, developers or generators of computer knowledge. In recent years, feminist infrastructure projects have begun to appear while the inclusion of women in developers communities has been promoted. However, today there is still a huge gender gap in the technical and political development of the internet.

In [RFC4949] _safety_ is defined as "the property of a system being free from risk of causing harm (especially physical harm) to its system entities", which is compared to _security_ as the "system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss". But _safety_ has traditionally, especially in the early years of the IETF, been referred to human activities [RFC1244], [RFC2122], [RFC2310] and human rights [RFC1746], [RFC1941], [RFC3694].

1.4.2.  2.2.  Gender

As IETF is centered on "identifying, and proposing solutions to, pressing operational and technical problems in the Internet" and as according to the Tao of the IETF, "we believe in rough consensus and
running code", it is not supposed to concentrate on the particular characteristics of internet users, but on the proper functioning of the systems [Tao]. In addition, due to the characteristics of the type of technologies that are designed in the IETF, many times the "use cases" or implementations refer to the way in which companies arrange the infrastructure for their clients, not necessarily to the way internet users interact with that infrastructure.

In this sense, it seems not within the mandate of the IETF to imagine the particular needs of users’ gender, race or ethnicity. However, in the drafts and RFCs archive there appear subjects with gender as well as supposedly universal entities that sometimes represent concrete functions of the systems, and other times the voluntary actions of the operators. As a first step in imagining possible gender considerations when designing internet protocols, below is a very brief description of how gender appears in IETF documents. This is also a very preliminary analysis, which could later be complimented and added to the search for entities with cultural and phenotypic characteristics that could make them vulnerable on the internet.

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

In this sense, access must be considered in several dimensions, in addition to internet access as a possibility of being connected:
1.5.1. 3.1. Access to information

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.

But it is also necessary to be able to access relevant information, related for example to sexual and reproductive health and rights, pleasure, safe abortion, access to justice, and LGBTIQ issues. 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.

1.5.2. 3.2. Usage of technology

Beyond content, access implies the possibility to use, which means code, design, adapt and critically and sustainably use ICTs. As 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.

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.

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]. The presence of gendered subjects in the IETF RFCs and drafts archive demonstrates stereotyped male and feminine roles. On the other hand, the generalized mention of agents - as universal subjects - in those documents, ignores the existence of other corporealities, which includes non binary identities or with a marked physical difference.

Building and engineering critical internet technology is a component of ‘usage’. There are challenge the cultures of sexism and discrimination in all spaces, some of which can be found in existing RFCs.
1.6. 4. Economy

1.6.1. 4.1. Free and open source

The digital gender gap has relegated women and other marginalized groups to be internet users, adding content for the benefit of the platform itself but without a deep understanding of how these platforms work. Promoting transparency [RFC8280] and simplifying technical terminology is necessary to bridge this gap. 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.

1.6.2. 4.2. Power and centralisation

A feminist approach to technology requires a strong critique of capitalist power, centralisation of services and the logic of vertical integration while holding nuance for the tensions between trust, reliability and diversity. Centralisation of services is a current discussion in the IETF that should be informed by feminist critique of capitalist structures [Arkko].

1.7. 5. Networked

1.7.1. 5.1. Freedom of association

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. 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. At the same time, the internet provides new and novel ways for communities to come together across borders and without limits of geolocation. However this positive aspect of internet communications is threatened by centralised systems of control and cooptation, specifically surveillance and other online repression.
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]."

1.7.2. 5.2. Internet governance

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].

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.

1.8. 6. Embodiment

Most of the threats women and non binary 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 connected 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. People build their own public digital identities, use private communications to disseminate information, explore their sexuality in text, image and video, share their intmitiy with others. In internet-connected devices, it has
become much easier for leisure and work to mix, which implies different risks for users.

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 online, 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?

1.8.1. 6.1. Online violence

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

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

While making public otherwise private details about a person can 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.

1.8.2. 6.2. 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

1.8.3. 6.3. 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

1.8.4. 6.4. 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.

1.8.5. 6.5. 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

2. References not yet referenced


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


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

Design Justice https://docs.google.com/presentation/d/1J3ZWBgxeQFQ8OmUr-QzE6Be8k_s17XF0VWu4wIMIVM/edit#slide=id.gcad8d6cb9_0_198

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


3. Security Considerations

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

4. IANA Considerations

This document has no actions for IANA.

5. Informative References


Authors' Addresses

Juliana Guerra
Derechos Digitales
EMail: juliana@derechosdigitales.org

Mallory Knodel
ARTICLE 19
EMail: mallory@article19.org