Human Rights Protocol Considerations Research Group N. ten Oever

Internet-Draft University of Amsterdam & Texas A&M University

Intended status: Informational G. Perez de Acha

Expires: May 6, 2021 Derechos Digitales

 S. Couture

 University de Montreal

 M. Knodel

 Center for Democracy & Technology

 November 02, 2020

 Freedom of Association on the Internet

 draft-irtf-hrpc-association-06

Abstract

 This document discusses the relationships between the Internet

 architecture and the ability of people to exercise their rights 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 global forum, the Internet

 provides a public space, yet it is predominantly built on private

 infrastructure. Since Internet protocols play a central role in the

 management, development, and use of the Internet, we analyze the

 relation between protocols and the rights to assemble and associate

 to mitigate infringements on those rights.

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 May 6, 2021.

ten Oever, et al. Expires May 6, 2021 [Page 1]

Internet-Draft FoA November 2020

Copyright Notice

 Copyright (c) 2020 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 . . . . . . . . . . . . . . . . . . . . . . 5

 5.1. FAA definition and core treaties . . . . . . . . . . . . 5

 5.2. FAA in the digital era . . . . . . . . . . . . . . . . . 8

 5.3. Specific questions raised from the literature review . . 12

 6. Cases and examples . . . . . . . . . . . . . . . . . . . . . 12

 6.1. Got No Peace: Spam and DDoS . . . . . . . . . . . . . . . 13

 6.1.1. Spam . . . . . . . . . . . . . . . . . . . . . . . . 14

 6.1.2. DDoS . . . . . . . . . . . . . . . . . . . . . . . . 14

 6.2. Holistic Agency: Mailing Lists and Spam . . . . . . . . . 15

 6.2.1. Mailing lists . . . . . . . . . . . . . . . . . . . . 15

 6.2.2. Spam . . . . . . . . . . . . . . . . . . . . . . . . 15

 6.3. Civics in Cyberspace: Messaging, Conferencing, and

 Networking . . . . . . . . . . . . . . . . . . . . . . . 16

 6.3.1. Email . . . . . . . . . . . . . . . . . . . . . . . . 16

 6.3.2. Mailing lists . . . . . . . . . . . . . . . . . . . . 16

 6.3.3. IRC . . . . . . . . . . . . . . . . . . . . . . . . . 17

 6.3.4. WebRTC . . . . . . . . . . . . . . . . . . . . . . . 17

 6.3.5. Peer-to-peer networking . . . . . . . . . . . . . . . 18

 6.4. Universal Access: The Web . . . . . . . . . . . . . . . . 19

 6.5. Block Together Now: IRC and Refusals . . . . . . . . . . 20

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

 studies? . . . . . . . . . . . . . . . . . . . . . . . . . . 21

 8. Acknowledgements . . . . . . . . . . . . . . . . . . . . . . 22

 9. Security Considerations . . . . . . . . . . . . . . . . . . . 22

 10. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 23

 11. Research Group Information . . . . . . . . . . . . . . . . . 23

 12. References . . . . . . . . . . . . . . . . . . . . . . . . . 23

ten Oever, et al. Expires May 6, 2021 [Page 2]

Internet-Draft FoA November 2020

 12.1. Informative References . . . . . . . . . . . . . . . . . 23

 12.2. URIs . . . . . . . . . . . . . . . . . . . . . . . . . . 30

 Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 30

1. Introduction

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

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

 "In the digital age, the exercise of the rights of peaceful assembly

 and association has become largely dependent on business enterprises,

 whose legal obligations, policies, technical standards, financial

 models and algorithms can affect these freedoms".

- Annual Report to the UN Human Rights Council by the Special Rapporteur

on the rights to freedom of peaceful assembly and of association (2019).We shape our tools and, thereafter, our tools shape us.&#8202;

 - John Culkin (1967)

 The current draft continues the work started in "Research into Human

 Rights Protocol Considerations" [RFC8280] by investigating the impact

 of Internet protocols on a specific set of human rights, namely the

 right to freedom of assembly and association. Taking into

 consideration the international human rights framework regarding the

 human rights to freedom of assembly and association, the present

 document seeks to deepen the relationship between these human righte

 and Internet architecture, protocols, and standards. In that way, we

 continue the work of the Human Rights Protocol Consideration Research

 Group, as laid out in its charter, where one of the research aims is

 "to expose the relation between protocols and human rights, with a

 focus on the rights to freedom of expression and freedom of assembly"

 [HRPC-charter]. The conclusions may inform the development of new

 guidelines for protocol developers in draft-irtf-hrpc-guidelines.

 The research question of this document is: what are the protocol

 development considerations for freedoms of assembly and association?

2. Vocabulary used

 Architecture The design of a structure

 Autonomous System (AS) Autonomous Systems are the unit of routing

 policy in the modern world of exterior routing [RFC1930].

 Within the Internet, an autonomous system (AS) is a collection of

 connected Internet Protocol (IP) routing prefixes under the

 control of one or more network operators on behalf of a single

 administrative entity or domain that presents a common, clearly

 defined routing policy to the Internet [RFC1930].

ten Oever, et al. Expires May 6, 2021 [Page 3]

Internet-Draft FoA November 2020

 The classic definition of an Autonomous System is a set of routers

 under a single technical administration, using an interior gateway

 protocol and common metrics to route packets within the AS, and

 using an exterior gateway protocol to route packets to other ASs

 [RFC1771].

 Border Gateway Protocol (BGP) An inter-Autonomous System routing

 protocol [RFC4271].

 Connectivity The extent to which a device or network is able to

 reach other devices or networks to exchange data. The Internet is

 the tool for providing global connectivity [RFC1958]. Different

 types of connectivity are further specified in [RFC4084]. The

 combination of the end-to-end principle, interoperability,

 distributed architecture, resilience, reliability and robustness

 are the enabling factors that result in connectivity to and on the

 Internet.

 Decentralization Implementation or deployment of standards,

 protocols or systems without one single point of control.

 Distributed system A system with multiple components that have their

 behavior co-ordinated via message passing. These components are

 usually spatially separated and communicate using a network, and

 may be managed by a single root of trust or authority.

 [Troncosoetal]

 Infrastructure Underlying basis or structure for a functioning

 society, organization or community. Because infrastructure is a

 precondition for other activities it has a procedural, rather than

 static, nature due to its social and cultural embeddedness

 [PipekWulf] [Bloketal]. This means that infrastructure is always

 relational: infrastructure always develops in relation to

 something or someone [Bowker].

 Internet The Network of networks, that consists of Autonomous

 Systems that are connected through the Internet Protocol (IP).

 A persistent socio-technical system over which services are

 delivered [Mainwaringetal],

 A techno-social assemblage of devices, users, sensors, networks,

 routers, governance, administrators, operators and protocols

 An emergent-process-driven thing that is born from the collections

 of the ASes that happen to be gathered together at any given time.

 The fact that they tend to interact at any given time means it is

ten Oever, et al. Expires May 6, 2021 [Page 4]

Internet-Draft FoA November 2020

 an emergent property that happens because they use the protocols

 defined at IETF.

3. Research question

 The research question of this document is: what are the protocol

 development considerations for freedom of assembly and association?

4. Methodology

 The point of departure of the present work [RFC8280] is an initial

 effort to expose the relationship between human rights and the

 Internet architecture, specifically protocols and standards. As

 such, [RFC8280] was inductive and explorative in nature. The

 methodology in this previous work was based on the discourse analysis

 of RFCs, interviews with members of the IETF community, and

 participant observation in IETF working groups, with the goal to

 identify technical concepts that relate to human rights. This work

 resulted in the proposal of guidelines to 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.

 In this document, we deepen our exploration of human rights and

 protocols by assessing one specific set of human rights: freedom of

 association and assembly, abbreviated here as FAA. Our methodology

 for doing so is the following: first, we provide a brief twofold

 literature review addressing the philosophical and legal definitions

 of FAA and how this right has already been interpreted or analyzed

 concerning the digital. This literature review is not exhaustive nor

 systematic but aims at providing some lines of questioning that could

 later be used for protocol development. The second part of our

 methodology looks at some cases of Internet protocols that are

 relevant to the sub-questions highlighted in the literature review,

 and analyze how these protocols facilitate and inhibit the right to

 assembly and association.

5. Literature Review

5.1. FAA definition and core treaties

 The rights to freedom of association and assembly are defined and

 guaranteed in national law and international treaties. Article 20 of

 the Universal Declaration of Human Rights [UDHR] states for instance

 that "Everyone has the right to freedom of peaceful assembly and

 association" and that "No one may be compelled to belong to an

 association". Article 23 further guarantees that "Everyone has the

ten Oever, et al. Expires May 6, 2021 [Page 5]

Internet-Draft FoA November 2020

 right to form and to join trade unions for the protection of his

 interests". In the International Covenant on Civil and Political

 Rights [ICCPR], article 21 stipulates that "The right of peaceful assembly

 shall be recognized" and that "No restrictions may be placed on the

 exercise of this right other than those imposed in conformity with

 the law and which are necessary in a democratic society in the

 interests of national security or public safety, public order (ordre

 public), the protection of public health or morals or the protection

 of the rights and freedoms of others" while article 22 states that

 "Everyone shall have the right to freedom of association with others,

 including the right to form and join trade unions".

General Comment No. 37 on the right of peaceful assembly by the United Nations Human Rights Committee affirms that the right of peaceful assembly protects non-violent online gatherings: “associated activities that happen online or otherwise rely upon digital services […] are also protected” [UNGC37]. Interference with emerging communications technologies that offer the opportunity to assemble either wholly or partly online or play an integral role in organizing, participating in and monitoring physical gatherings are assumed to impede assemblies which are protected by this right. Moreover, any restriction on the ‘operation of information dissemination systems’ must conform with the tests for restrictions on freedom of expression (see below).

Other treaties

 are sometimes cited as the source and framework to the right to

 freedom of association and assembly. Such as Article 5 of the International Convention on the

 Elimination of All Forms of Racial Discrimination [CERD] which

 stipulates freedom of peaceful assembly and association should be

 guaranteed "without discrimination as to race, colour, national or

 ethnic origin"; Article 15 of the Convention on the Rights of the

 Child [CRC] which recognises to child pending the restrictions cited

 above; and Article 21 of the Convention on the Rights of Persons with

 Disabilities [CRPD] which insist on usable and accessible formats and

 technologies appropriate for persons with different kinds of

 disabilities. The freedoms of peaceful assembly and association are also protected under regional human rights treaties: article 11 of the European Convention on Human Rights, articles 15 and 16 of the American Convention on Human Rights, article 10 and 11 of the African Charter on Human and Peoples’ Rights.

 From a more philosophical perspective, Brownlee and Jenkins

 [Stanford] make some interesting distinctions in particular regarding

 the concepts of association, assembly and interaction, deviating somewhat from what is established in interpretations of international human rights law.

 "Interaction" refers to any kind of interpersonal and often

 incidental engagements in daily life, like encountering strangers on

 a bus. Interaction is seen as a "prerequisite" for association.

 Assembly, according to Brownlee and Jenkins has a more political connotation and is

 often used to refer to activists, protesters, or members of a group

 in a deliberating event. . The authors refer to association as

 more "persistent connections" and distinguish between intimate associations,

 like friendship, love, or family, and collective association like

 trade unions, commercial business, or "expressive associations" like

 civil rights organizations or LGBTQIA associations. For Brownlee and

 Jenkins [Stanford], the right to association is linked to different

 relative freedoms: permission (to associate or dissociate), claim-

 right (to oppose others interfering with our conduct), power (to

 alter the status of our association), immunity (from other people

 interfering in our right). Freedom of association thus

 refers both to the individual right to join or leave a group and to

 the collective right to form or dissolve a group.

Freedoms of association and peaceful assembly, however, are relative and not absolute.

Excluding someone from an association

ten Oever, et al. Expires May 6, 2021 [Page 6]

Internet-Draft FoA November 2020

 based on its sex, race or other individual characteristic is also

 often contentious if not illegal. As mentioned above, international human rights law provides the framework for legitimate restrictions on these rights, as well as the right to privacy and the right to freedom of expression and opinion. Restrictions can be imposed by states, but only if this is lawful and

 proportionate. States must document how these limitations are

 necessary in the interests of national security or public safety,

 public order, the protection of public health or morals, or the

 protection of the rights and freedoms of others. Finally, states

 must also protect participants against possible abuses by non-State

 actors.

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

 Interpreting international law, the right to freedom of peaceful assembly and the right to freedom of

 association protect any collective, gathered either permanently or

 temporarily for "peaceful" purposes, online and offline. It is important to underline

 the property of "freedom" because the right to freedom of association

 and assembly is voluntary and uncoerced: anyone can join or leave a

 group of choice, which in turn means one should not be forced to

 either join, stay or leave. .

 An assembly is an “intentional and temporary gathering of a

 collective in a private or public space for a specific purpose:

 demonstrations, indoor meetings, strikes, processions, rallies, or

 even sits-in”; Association has a more formal and established

 nature and refers to a group of individuals or legal entities

 brought together in order to collectively act, express, promote, pursue, or

 defend a field of common interests [UNSRFOAA2012]. Think about civil society

 organizations, clubs, cooperatives, NGOs, religious associations,

 political parties, trade unions, or foundations.

 When talking about the human rights of freedom of association and

 assembly, one should always take into account that 'all human rights

 are indivisible, interrelated, unalienable, universal, and mutually

 reinforcing' [ViennaDeclaration]. This means that in the analysis of

 the impact of a certain variable on freedom of association and

 assembly one should take other human rights into account too. When

 devising an approach to mitigate a possible negative influence on

 this right, one should also always take into account the possible

 impact this might have on other rights. For example, the following

 rights are often impacted in conjunction with freedom of association

 and assembly: the right to political participation, the right to

 (group) privacy, the right to freedom of expression, and access to

 information. For instance, when the right to political participation

 is hampered, this often happens in conjunction with a limitation of

 the freedom of association and assembly because political

 participation is often done collectively. When the right to privacy

 is hampered, this privacy of particular groups is also impacted (so-

ten Oever, et al. Expires May 6, 2021 [Page 7]

Internet-Draft FoA November 2020

 called 'group privacy' [Loi], which potentially has consequences for

 the right to association and assembly. Where the freedom of

 expression of a group is hampered, such as in protests or through

 Internet shutdowns, this both hampers other people's ability to

 receive the information of the group, and impact the right to

 assembly of the people who seek to express themselves as a group

 [Nyokabi].

 Finally, if the right to association and assembly is limited by

 national law, this does not mean it is consistent with international

 human rights law. In such a case, the national law would therefore

 not be legitimate [Glasius].

5.2. FAA in the digital era

 Before discussing freedom of association and assembly as it pertains

 to digital environments, we must first recognize that the United

 Nations Human Rights Council adopted resolutions on the promotion, protection and enjoyment of human rights on the Internet in 2012, 2014, 2016 and 2018, affirming and reaffirming "... that the same rights that people have offline must

 also be protected online ..." [Resolution]. Therefore the digital environment is

 no exception to application of this right by any means. Various other resolutions and report have established the online applicability of the freedoms of association and assembly, most recently and authoritatively by the Human Rights Committee in General Comment 37 (2020)[UNGC37]. The

 questions that remain, however, are how these rights should be

 conceptualized and implemented in different parts and levels of

 digital environments.

 The right to freedom of assembly and association online is the subject of

 increasing discussions and analysis. Especially since social media played an important role in several revolutions in 2011, which has led to increasing and ever more sophisticated attacks by autocratic governments on online communities and other associational activities occurring on the Internet [RutzenZenn].In 2016, the Council of Europe

 published a report, "Report by the Committee of experts on cross-

 border flow of Internet traffic and Internet freedom on Freedom of

 assembly and association on the Internet" [CoE] which noted that

 while the Internet and technologies are not explicitly mentioned in

 international treaties, these treaties nevertheless apply to "the

 online environment". The report argue the "Internet is the public

 sphere of the 21st century", something demonstrated by the fact that

 informal associations can be gathered at scale in a matter of hours

 on the Internet, and that digital communication tools often serve to

 facilitate, publicize or otherwise enable presential associations or

 assemblies, like a protest or demonstration. They note, on the other

 hand, the negative ways in which the Internet can also be used to

 promote or facilitate terrorism, urban violence and hate speech, thus

 insisting on the "extremely important and urgent" need to fight

 online terrorist activities such as recruitment or mobilization,

 while at the same time respecting the right to peaceful assembly and

 association of other users. The report mentions the following use

 cases that could be help further our reflection:

ten Oever, et al. Expires May 6, 2021 [Page 8]

Internet-Draft FoA November 2020

 - Instances of network shutdowns in the Arab Spring, to prevent

 people from organising themselves or assembling

 - California's Bay Area Rapid Transit (BART) shutdown of mobile

 phone service, to avoid protester violence and disruption of

 service

 - The wholesale blocking of Google as a violation of freedom of

 expression

 - Telus, a telecom company which blocked customers' access to

 websites critical of Telus during a Telecommunications Workers

 Union strike against it

 - The targeting of social media users who call for or organise

 protests though the Internet in Turkey's Gezi Park protests

 - Mass surveillance or other interferences with privacy in the

 context of law enforcement and national security

 - Use of VPNs (Virtual Private Networks) to the TOR network to

 ensure anonymity

 - Distributed Denial of Service attacks (DDoS) as civil

 disobedience.

 In 2019, the UN Special Rapporteur on the rights to freedom of

 peaceful assembly and of association, notes the opportunities

 and challenges posed by digital networks to the rights to freedom of

 peaceful assembly and of association [UNSRFAA2019]. The report recommends that

 international human rights norms and principles should also be used

 as a framework "that guides digital technology companies' design,

 control and governance of digital technologies". The report states

 that "technical standards" in particular can affect the freedom of

 association and assembly, and makes some recommendations on which the

 following could be relevant to our discussion here:

 - "[Undertake] human rights impact assessments which incorporate the

 rights to freedom of peaceful assembly and of association when

 developing or modifying their products and services,"

 - "increase the quality of participation in and implementation of

 existing multi-stakeholder initiatives,"

 - "collaborate with governments and civil society to develop

 technology that promotes and strengthens human rights,"

ten Oever, et al. Expires May 6, 2021 [Page 9]

Internet-Draft FoA November 2020

 - "support the research and development of appropriate technological

 solutions to online harassment, disinformation and propaganda,

 including tools to detect and identify State-linked accounts and

 bots," and

 - "adopt monitoring indicators that include specific concerns

 related to freedom of peaceful assembly and association."

 In one of their "training kits" [APCtraining], the Association of

 Progressive Communications addressed different impacts of the

 internet on association and assembly and raised three particular

 issues worthy to note here:

 1. Organization of protests. Internet and social media are enablers

 of protests, such as it was seen in the "Arab Spring". Some of

 these protests - like online petitions or campaigns - are similar

 to offline association and assembly, but other protest forms are

 inherent to the Internet capacity like hacking, DDOS and are

 subject to controversy within the Internet community, some people

 finding it legitimate, and others not.

 2. Surveillance. While the Internet facilitates association, the

 association in turn leaves a lot of traces that can be used in

 turn for law enforcement but also for repressing political

 dissents. As they note, even the threat of surveillance can have

 deter facilitation.

 3. Anonymity and pseudonymity can be useful protection mechanism for

 those who'd like to attend legitimate association without facing

 retribution. On the other hand, anonymity can be used to harm

 society, such as in online fraud or sexual predation.

 Online association and assembly are the starting point of 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 an 'open global community' of network designers,

 operators, vendors, and researchers [RFC3233] is also protected by

 freedom of assembly and association . Discussions, comments and

 consensus around RFCs are possible because of the collective

ten Oever, et al. Expires May 6, 2021 [Page 10]

Internet-Draft FoA November 2020

 expression that freedom of association and assembly allow. The very

 word "protocol" found its way into the language of computer

 networking based on the need for collective agreement among a group

 of assembled network users [HafnerandLyon].

 [RFC8280] is a paper by the Human Rights Protocol Consideration

 Resarch Group in the Internet Research Taskforce on internet

 protocols and human rights that discusses issues of FAA,

 specifically:

 - The expansion of DNS for generic namespace as an enabler of

 association for minorities. The paper argues that specifically

 the expansion of the DNS to allow for new generic Top Level

 Domains (gTLDs) can have negative impacts on freedom of

 association because of restrictive policies by some registries and

 registrars, on the other hand could gTLDs also enable communities

 to build clearly identifiable spaces for association (such as

 .gay).

 - The impact of Distributed Denial of Service attacks on freedom of

 association. Whereas DDoS has been used as a tool for protest, in

 many cases this is infringing on other parties freedom of

 expression. Furthermore, often devices (such as IoT devices and

 routers) are inscribed in such DDoS attacks whereas the owner or

 user did not consent to this. Thus they do not have the

 possibility to exit this assembly. Therefore the draft concluded

 that that IETF "should try to ensure that their protocols cannot

 be used for DDoS attacks"

 - The impact of middleboxes on the ability of users to connect to

 the Internet and therefore their ability to exercise their right

 to freedom of association and assembly. The lack of connectivity

 can significantly impact freedom of assembly and association of a

 user. Especially if this is done in a way that is not knowable

 for the user and if there is no possibility to for the user to

 have access to due process to dispute the lack of (secure or

 private) connectivity in general or to a specific service.

 In June 2020, the United Nations High Commissioner for Human

 Rights it is concluded that technologies can be enablers of the exercise of

 FAA, but technology is also significantly used to interfere with the

 ability of people to exercise their right to freedom of association and

 assembly. Specifically, the report mentions network shutdowns, the

 usage of technology to surveil or crack down on protesters, leading to human rights violations. This includes

 facial recognition technology, and the uses of other ways to violate the (group)

 privacy of people engaged in an assembly or association. The report

 makes it explicit that companies play a significant role enabling,

ten Oever, et al. Expires May 6, 2021 [Page 11]

Internet-Draft FoA November 2020

 for instance by developing, providing or selling the technology, but

 also by directly exercising these violations [UNHCHR2020].

5.3. Specific questions raised from the literature review

 Here are some questions raised from the literature review that can

 have implications for protocol design:

 1. Should protocols be designed to enable legitimate limitations on

 association in the interests of "national security or public

 safety, public order (ordre public), the protection of public

 health or morals or the protection of the rights and freedoms of

 others", as stated in the ICCPR article 21 [ICCPR]? Where in the

 stack do we care for FAA?

 2. Can protocols facilitate agency of membership in associations,

 assemblies and interactions?

 3. What are the features of protocols that enable freedom of

 association and assembly?

 4. Does protocol development sufficiently consider usable and

 accessible formats and technologies appropriate for all persons,

 including those with different kinds of disabilities?

 5. Can a protocol be designed to legitimately exclude someone from

 an association?

 In the following sections we attempt to answer these questions with

 specific examples of standardized protocols in the IETF.

6. 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 are aware that some of the following examples go beyond the use of

 Internet protocols and flow over into the application layer or

 examples in the offline world whereas the purpose of the current

 document is to break down the relationship between Internet protocols

 and the right to freedom of assembly and association. Nonetheless,

 we do recognize that in some cases the line between them and

ten Oever, et al. Expires May 6, 2021 [Page 12]

Internet-Draft FoA November 2020

 applications, implementations, policies and offline realities are

 often blurred and hard -if not impossible- to differentiate.

 We use the literature review to guide our process of inquiry for each

 case, and to dive deeper in what can be found interesting about each

 case as it relates to freedom of association.

6.1. Got No Peace: Spam and DDoS

 Should protocols be designed to enable legitimate limitations on

 association in the interests of "national security or public safety,

 public order (ordre public), the protection of public health or morals

 or the protection of the rights and freedoms of others", as stated in

 the ICCPR article 21 [ICCPR]? Where in the stack do we care for FAA?

The 2020 report by the United Nations High Commissioner for Human

 Rights [UNHCHR2020] described how technology is often used to limit

 freedom of assembly and association, such as for instance through

 network shutdowns and the surveillance of groups. Because access to

 the Internet is crucial not only for freedom of association and

 assembly, but also for the right to development, and the right to

 freedom of expression and information [Nyokabi], the United Nation

 Special Rapporteur argues that:

 (b) Avoid resorting to disruptions and shutdowns of Internet or

 telecommunications networks at all times and particularly during

 assemblies, including those taking place in electoral contexts

 and during times of unrest;

 Whereas the states have the obligation to protect human rights, there

 has been an increasing call for non-state actors, such as companies,

 to respect human rights. The UN adopted guiding principles on business and human rights [UNGPBHR] and talks within the HRC are ongoing about an international legally binding instrument to regulate the activities of transnational corporations and other business enterprises]. This includes a chain-responsibility

 of actors, which means that not just the company's own processes

 should not negatively impact human rights, but they should also

 engage in due diligence processes, such as human rights impact

 assessments. This includes an assessment of whether the products

 that are sold, or the services that are provided, can be used to

 engage in human rights violations, or whether human rights violations

 occur in any stage of the supply chain of the company. If this is

 the case, measures should be taken to mitigate this.

 In the case of dual-use technologies, this means that technology

 could be used for legitimate purposes, but could also be used to

 limit freedom of association or assembly, it might mean that

 producers or sellers should limit the parties they sell to, or even

 better, ensure that the illegitimate use of the technology is not

 technically possible anymore, or made more difficult.

ten Oever, et al. Expires May 6, 2021 [Page 13]

Internet-Draft FoA November 2020

6.1.1. Spam

 In the 1990s as the internet became more and more commercial, spam

 came to be defined as irrelevant or unsolicited messages that were

 posted many times to multiple news groups or mailing lists [Marcus]}.

 Here the question of consent, but also harm, are crucial. In the

 2000s a large part of the discussion revolved around the fact that

 certain corporations, protected by the right to freedom of

 association, considered spam to be a form of "commercial speech",

 thus encompassed by free expression rights [Marcus]. Yet spam can be

 not only a nuisance, but a threat to systems and users.

 This leaves us with an interesting case around spam mitigation: spam is currently handled

 mostly by mail providers on behalf of the user, next to that

 countries are increasingly adopting opt-in regimes for mailing lists

 and commercial e-mail, with a possibility of serious fines in case of

 violation. Yet many ask: is spam not the equivalent of the fliers and

 handbills ever present in our offline world? The big difference

 between the proliferation of such messages offline and online is the

 scale. It is not hard for a single person to message a lot of

 people online, whereas if that person needed to go house by house the scale

 and impact of their actions would be much smaller. Inversely if it

 were a common practice to expose people to unlimited unwanted messages online,

 users would be drowned in such messages, and no expression would be

 possible anymore. Allowing illimited sending of unsolicited messages

 would be a blow against freedom of speech: when everyone talks,

 nobody listens.

 Here the argument is very similar to DDoS attacks, considered next:

 Legitimate uses of online campaigning, or online protesting, are

 drowned out by a malicious use which constitutes an attack on the

 internet infrastructure and thus the assembly or association itself.

6.1.2. DDoS

 Distributed Denial of Service attacks are leveled against a server or

 service by a controller of a host or multiple hosts by overloading

 the server or service's bandwidth or resources (volume-based floods)

 or exploit protocol behaviours (protocol attacks). DDoS attacks can

 thus stifle and complicate the rights to assemble online for media

 and human rights organisations whose websites are the target of DDoS.

 At the same time there are comparisons made between DDoS attacks and

 sit-in protests [Sauter]. However the main distinction is

 significant: only a small fragment of "participants" (from

 controllers to compromised device owners) in DDoS attacks are aware

 or willing [RFC8280]. Notably DDoS attacks are increasingly used to

 commit crimes such as extortion, which infringe on others' human

 rights.

ten Oever, et al. Expires May 6, 2021 [Page 14]

Internet-Draft FoA November 2020

 Because of the interrelation of technologies, it cannot be said that

 there is one point in the technical stack that there are

 characteristics of "peaceful" or "non-peaceful" association visible

 to protocol developers. As we can see from the cases of spam

 blocking and DDoS mitigation that "peaceful or non-peaceful" is not a

 meaningful heuristic, or even characteristic, of problematic content.

 If anything, their commonality is scale and volume.

6.2. Holistic Agency: Mailing Lists and Spam

 Can protocols facilitate agency of membership in associations,

 assemblies and interactions?

6.2.1. Mailing lists

 Since the beginning of the Internet mailing lists have been a key

 site of assembly and association [RFC0155] [RFC1211]. In fact,

 mailing lists were one of the Internet's first functionalities

 [HafnerandLyon].

 In 1971 four years after the invention of email, the first mailing

 list was created to talk about the idea of using Arpanet for

 discussion. What had initially propelled the Arpanet project forward

 as a resource sharing platform was gradually replaced by the idea of

 a network as a means of bringing people together [Abbate]. More than

 45 years after, mailing lists are pervasive and help communities to

 engage, have discussions, share information, ask questions, and build

 ties. Even as social media and discussion forums grow, mailing lists

 continue to be widely used [AckermannKargerZhang] and are still a

 crucial tool to organise groups and individuals around themes and

 causes [APC3].

 Mailing lists' pervasive use are partly explained because they allow

 for "free" association: people subscribe (join) and unsubscribe

 (leave) as they please. Mailing lists also allow for association of

 specific groups on closed lists. This free association online

 enables agency of membership, a key component of freedom of

 association and assembly.

6.2.2. Spam

 As we mentioned before, there are interesting implications for

 freedom of association and assembly when looking at spam mitigation.

 Here we want to specifically note that if we consider that the rights

 to assembly and association also mean that "no one may be compelled

 to belong to an association" [UDHR], spam infringes both rights if an

 op-out mechanism is not provided and people are obliged to receive

 unwanted information, or be reached by people they do not know.

ten Oever, et al. Expires May 6, 2021 [Page 15]

Internet-Draft FoA November 2020

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

 What are the features of protocols that enable freedom of

 association and assembly?

 Civic participation is often expressed as the freedom to associate

 and assemble, along with a whole other set of enabling rights such as

 freedom of expression and the right to privacy. Former UN Special

 Rapporteur David Kaye established a strong relationship between

 technology that allows anonymity and uses encryption have positive

 effects on freedom of expression [Kaye]. Here we look at messaging,

 such as email, mailing lists and internet relay chat; video

 conferencing and peer-to-peer networking protocols to investigate the

 common features that enable freedom of association and assembly

 online.

6.3.1. Email

 Similarly to freedom of expression's enabling and universal right to

 impart one's ideas openly, "the right to whisper", or

 confidentiality, is the ability to limit to whom one imparts one's

 ideas. An encrypted email project, the LEAP Encryption Access

 Project, says, "like free speech, the right to whisper is a necessary

 precondition for a free society. Without it, civil society

 languishes and political freedoms are curtailed. As the importance

 of digital communication for civic participation increases, so too

 does the importance of the ability to digitally whisper." [LEAP]

6.3.2. Mailing lists

 Not only are mailing lists a good example of how protocols can

 facilitate the necessary ingredient of agency in freedom of

 association, mailing lists are an example of messaging technology

 that has other features that enable freedom of association and

 assembly.

 The archival function of mailing lists allows for posterior

 accountability and analysis. The ubiquity and interoperability of

 email, and by extension email lists, provides a low barrier to entry

 to an inclusive medium.

 Association and assembly online can be undermined when right to

 privacy is at risk. And one of the downsides of mailing lists are

 similar to the privacy and security concerns generally associated

 with email. At least with email, end-to-end encryption such as

 OpenPGP [RFC4880] and S/MIME [RFC5751] can keep user communications

 authenticated and confidential. With mailing lists, this protection

 is not as possible because with many lists the final recipients are

ten Oever, et al. Expires May 6, 2021 [Page 16]

Internet-Draft FoA November 2020

 typically too many for . There have been experimental solutions to

 address this issue such as Schleuder [Schleuder], but this has not

 been standardized or widely deployed.

6.3.3. IRC

 Internet Relay Chat (IRC) is an application layer protocol that

 enables communication in the form of text through a client/server

 networking model [RFC2810]. In other words, a chat service. IRC

 clients are computer programs that a user can install on their

 system. These clients communicate with chat servers to transfer

 messages to other clients. Features of IRC include: federated

 design, transport encryption, one-to-many routing, creation of topic-

 based "channels", and spam or abuse moderation.

 For the purposes of civic participation and freedom of association

 and assembly in particular it is critical that IRC's federated design

 allows many interoperable, yet customisable, instances and basic

 assurance of confidentiality through transport encryption. We

 investigate the particular aspect of agency in membership through

 moderation in the section 'Block Together Now: IRC and Refusals'

 below.

6.3.4. WebRTC

 Multi-party video conferencing protocols like WebRTC [RFC6176]

 [RFC7118] allow for robust, bandwidth-adaptive, wideband and super-

 wideband video and audio discussions in groups. '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

 might pose concrete risks for those who use them. One the one hand

 WebRTC is providing resilient channels of communications, but on the

 other hand it also exposes information about those who are using the

 tool which might lead to increased surveillance, identification and

 the consequences that might be derived from that. This is especially

ten Oever, et al. Expires May 6, 2021 [Page 17]

Internet-Draft FoA November 2020

 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.

6.3.5. Peer-to-peer networking

 At the organizational level, peer production is one of the most

 relevant innovations from Internet mediated social practices.

 According to [Benkler] these networks imply 'open collaborative

 innovation and creation, performed by diverse, decentralized groups

 organized principally by neither price signals nor organizational

 hierarchy, harnessing heterogeneous motivations, and governed and

 managed based on principles other than the residual authority of

 ownership implemented through contract.' [Benkler].

 In his book The Wealth of Networks, [Benkler2] significantly expands

 on his definition of commons-based peer production. In his view,

 what distinguishes commons-based production is that it doesn't rely

 upon or propagate proprietary knowledge: "The inputs and outputs of

 the process are shared, freely or conditionally, in an institutional

 form that leaves them equally available for all to use as they choose

 at their individual discretion." [Benkler2]. To ensure that the

 knowledge generated is available for free use, commons-based projects

 are often shared under an open license

 Peer-to-peer (P2P) is essentially a model of how people interact in

 real life because "we deal directly with one another whenever we wish

 to" [Vu]. Usually if we need something we ask our peers, who in turn

 refer us to other peers. In this sense, the ideal definition of P2P

 is that "nodes are able to directly exchange resources and services

 between themselves without the need for centralized servers" where

 each participating node typically acts both as a server and as a

 client [Vu]. [RFC5694] has defined it as peers or nodes that should

 be able to communicate directly between themselves without passing

 intermediaries, and that the system should be self-organizing and

 have decentralized control [RFC5694]. With this in mind, the

 ultimate model of P2P is a completely decentralized system, which is

 more resistant to speech regulation, immune to single points of

 failure and has a higher performance and scalability. Nonetheless,

 in practice some P2P systems are supported by centralized servers and

 some others have hybrid models where nodes are organized into two

 layers: the upper tier servers and the lower tier common nodes [Vu].

ten Oever, et al. Expires May 6, 2021 [Page 18]

Internet-Draft FoA November 2020

 Since the ARPANET project, the original idea behind the Internet was

 conceived as what we would now call a peer-to-peer system [RFC0001].

 Over time it has increasingly shifted towards a client/server model

 with "millions of consumer clients communicating with a relatively

 privileged set of servers" [NelsonHedlun].

 Whether for resource sharing or data sharing, P2P systems are

 enabling freedom of assembly and association. Not only do they allow

 for effective dissemination of information, but they leverage

 computing resources by diminishing costs allowing for the formation

 of open collectives at the network level. At the same time, in

 completely decentralized systems the nodes are autonomous and can

 join or leave the network as they want -a characteristic that makes

 the system unpredictable: a resource might be only sometimes

 available, and some other resources might be missing or incomplete

 [Vu]. Lack of information might in turn makes association or

 assembly more difficult.

 Additionally, when architecturally assessing the role of P2P systems

 we could say that: "the main advantage of centralized P2P systems is

 that they are able to provide a quick and reliable resource locating.

 Their limitation, however, is that the scalability of the systems is

 affected by the use of servers. While decentralized P2P systems are

 better than centralized P2P systems in this aspect, they require a

 longer time in resource locating. As a result, hybrid P2P systems

 have been introduced to take advantage of both centralized and

 decentralized architectures. Basically, to maintain the scalability,

 similar to decentralized P2P systems, there are no servers in hybrid

 P2P systems. However, peer nodes that are more powerful than others

 can be selected to act as servers to serve others. These nodes are

 often called super peers. In this way, resource locating can be done

 by both decentralized search techniques and centralized search

 techniques (asking super peers), and hence the systems benefit from

 the search techniques of centralized P2P systems." [Vu].

6.4. Universal Access: The Web

 Does protocol development sufficiently consider usable and accessible

 formats and technologies appropriate for persons with different kinds

 of disabilities?

 The W3C has done significant work to ensure that the Web is

 accessible to people with diverse physical abilities [W3C]. The

 implementation of these accessibility standards for instance help

 people who have issues with seeing or rendering images to

 understand what the image actually contains.

ten Oever, et al. Expires May 6, 2021 [Page 19]

Internet-Draft FoA November 2020

 The IETF uses English as its primary working language, both in its

 documentation and in its communication. This is also the case for

 reference implementations. Whereas it is estimated that roughly 20%

 of the Earth's population speaks English, whereas only 360 million

 speak English as their first language. [RFC2277] describes that

 '"Internationalization is for humans. This means that protocols are

 not subject to internationalization; text strings are.", this implies

 that protocol developers, as well as people that work with protocols,

 are not people, or that protocol developers are all in command of the

 English language. This means that it is significantly easier for

 people who have a command of the English language to become a

 protocol developer - and it might lead to the development of separate

 protocols that are developed within large language communities that

 are not using the English language or the Latin script. This makes

 it harder for people who seek to shape their own space of association

 and assembly on the Internet to do so. And is thus driving these

 communities into, often proprietary and non-interoperable services

 such as Facebook.

 When Ramsey Nasser developed the Arabic programming language

 &#1602;&#1604;&#1576; (transliterated Qalb, Qlb and Alb) [Nasser] he

 called it 'engineering performance art' instead of engineering,

 because he knew that his language would not work. In part this is

 because all modern programming tools are based on the ASCII character

 set, which encodes Latin Characters and was originally based on the

 English Language. This highlights cultural biases of computer

 science and engineering. Despite long significant efforts, it is

 still largely impossible to register an email address in a language

 such as Devanagari, Arabic, or Chinese. Even if it is possible - it

 is to be expected that there will be a significant failure rate in

 sending and receiving emails with other services. This makes it

 harder for people who do not speak English and/or don't use the

 written Latin script to exercise their freedom of association and

 assembly.

6.5. Block Together Now: IRC and Refusals

 Can a protocol be designed to legitimately exclude someone

 from an association?

 Previously we spoke about the privacy protecting features of IRC that

 enable freedom of association and assembly, including transport

 security. But now we turn to the ability to block users and

 effectively moderate discussions on IRC as a key feature of the

 technology that enables agency in membership, a key aspect of freedom

 of association and assembly.

ten Oever, et al. Expires May 6, 2021 [Page 20]

Internet-Draft FoA November 2020

 For order to be kept within the IRC network, special classes of users

 become "operators" and are allowed to perform general maintenance

 functions on the network: basic network tasks such as disconnecting

 (temporary or permanently) and reconnecting servers as needed

 [RFC2812]. One of the most controversial power of operators is the

 ability to remove a user from the connected network by 'force', i.e.,

 operators are able to close the connection between any client and

 server [RFC2812].

 IRC servers may deploy different policies for the ability of users to

 create their own channels or 'rooms', and for the delegation of

 'operator'-rights in such spaces. Some IRC servers support SSL/TLS

 connections for security purposes [RFC7194] which helps stop the use

 of packet sniffer programs to obtain the passwords of IRC users, but

 has little use beyond this scope due to the public nature of IRC

 channels. TLS connections require both client and server support

 (that may require the user to install TLS binaries and IRC client

 specific patches or modules on their computers). Some networks also

 use TLS for server to server connections, and provide a special

 channel flag (such as +S) to only allow TLS-connected users on the

 channel, while disallowing operator identification in clear text, to

 better utilize the advantages that TLS provides.

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

 Communities, collaboration and joint action lie at the heart of the

 Internet. Even at a linguistic level, the words "networks" and

 "associations" are closely related. Both are groups and assemblies

 of people who depend on "links" and "relationships" [Swire]. Taking

 legal definitions given in international human rights law and related normative documents

 , we could assert that the rights to freedom of assembly

 and association protect collective activity online. These rights protect gatherings by persons for a specific purpose and groups with a defined aim over time for a variety of peaceful, expressive and non-expressive, purposes,. voluntary and uncoerced.

 Given that the Internet itself was originally designed as a medium of

 communication for machines that share resources with each other as

 equals [RFC0903], the Internet is now one of the most basic

 infrastructures for the rights to freedom of assembly and association.

 Since Internet protocols and the Internet architecture play a central

 role in the management, development and use of the Internet, we

 established the relation between some protocols and the right to

 freedom of assembly and association.

 After reviewing several cases representative of FAA considerations

 inherent in protocols standardized at the IETF, we can conclude that

 the way in which infrastructure is designed and implemented impacts

 people's ability to exercise their freedom of assembly and

ten Oever, et al. Expires May 6, 2021 [Page 21]

Internet-Draft FoA November 2020

 association. This is because different technical designs come with

 different properties and characteristics. These properties and

 characteristics on the one hand enable people to assemble and

 associate, but on the other hand also add limiting, or even

 potentially endangering, characteristics. More often than not, this

 depends on the context. A clearly identified group for open

 communications, where messages are sent in cleartext and where

 peoples persistent identities are visible, can help to facilitate an

 assembly and build trust, but in other contexts the same

 configuration could pose a significant danger. Endangering

 characteristics should be mitigated, or at least clearly communicated

 to the users of these technologies.

 Lastly, the increasing shift towards closed and non-interoperable

 platforms in chat and social media networks have a significant impact

 on the distributed and open nature of the Internet. Often these non-

 interoperable platforms are built on open-protocols but do not allow

 for interoperability or data-portability. The use of social-media

 platforms has enabled groups to associate, but it has also rendered

 users unable to change platforms, therefore leading to a sort of

 "forced association" that inhibits people to fully exercise their

 freedom of assembly and association.

8. Acknowledgements

 - Fred Baker, Jefsey, and Andrew Sullivan for work on Internet

 definitions.

 - Stephane Bortzmeyer 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.

9. Security Considerations

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

 considerations.

ten Oever, et al. Expires May 6, 2021 [Page 22]

Internet-Draft FoA November 2020

10. IANA Considerations

 This document has no actions for IANA.

11. 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]

12. References

12.1. Informative References

 [Abbate] Janet Abbate, ., "Inventing the Internet", Cambridge: MIT

 Press (2013): 11. , 2013,

 <https://mitpress.mit.edu/books/inventing-internet>.

 [AckermannKargerZhang]

 Ackerman, M., Karger, D., and A. Zhang, "Mailing Lists:

 Why Are They Still Here, What's Wrong With Them, and How

 Can We Fix Them?", Mit. edu (2017): 1. , 2017,

 <https://people.csail.mit.edu/axz/papers/

 mailinglists.pdf>.

 [AndersonGuarnieri]

 Anderson, C. and C. Guarnieri, "Fictitious Profiles and

 WebRTC's Privacy Leaks Used to Identify Iranian

 Activists", 2016,

 <https://iranthreats.github.io/resources/webrtc-

 deanonymization/>.

 [APC] Association for Progressive Communications and . Gayathry

 Venkiteswaran, "Freedom of assembly and association online

 in India, Malaysia and Pakistan. Trends, challenges and

 recommendations.", 2016,

 <https://www.apc.org/es/system/files/

 FOAA\_online\_IndiaMalaysiaPakistan.pdf>.

 [APC3] Association for Progressive Communications, "Closer than

 ever", 2020, <https://www.apc.org/en/node/36145/#tools>.

ten Oever, et al. Expires May 6, 2021 [Page 23]

Internet-Draft FoA November 2020

 [APCtraining]

 Sauter, D. and Association for Progressive Communications,

 "Multimedia training kit", 2013,

 <http://itrainonline.org/itrainonline/mmtk/

 APC\_IRHRCurriculum\_FOA\_Handout.pdf>.

 [Australia]

 Australian Government, Attorney-General's Department,

 "Right to freedom of assembly and association", 2020,

 <https://www.ag.gov.au/rights-and-protections/human-

 rights-and-anti-discrimination/human-rights-scrutiny/

 public-sector-guidance-sheets/right-freedom-assembly-and-

 association#topofpage>.

 [Benkler] Benkler, Y., "Peer Production and Cooperation", 2009,

 <http://www.benkler.org/

 Peer%20production%20and%20cooperation%2009.pdf>.

 [Benkler2]

 Benkler, Y., "The wealth of Networks - How social

 production transforms markets and freedom", New Haven and

 London - Yale University Press , 2006,

 <http://is.gd/rxUpTQ>.

 [Bloketal]

 Blok, A., Nakazora, M., and B. Winthereik,

 "Infrastructuring Environments", Science as Culture 25:1,

 1-22. , 2016.

 [Bowker] Bowker, G., "Information mythology and infrastructure",

 In: L. Bud (Ed.), Information Acumen: The Understanding

 and use of Knowledge in Modern

 Business,Routledge,London,1994,pp.231-247 , 1994.

[UNGC37] Human Rights Committee “General comment No. 37 (2020) on the right of peaceful assembly (article 21)”, CCPR/C/GC/3, 2020

< https://tbinternet.ohchr.org/\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11>

 [CERD] United Nations, "Convention on the Elimination of all

 forms of Racial Discrimination", 1966,

 <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/

 AllDocIDs/2F70352A0B65EB67CA256B6E0075FE13>.

 [CoE] Council of Europe, "Freedom of assembly and association on

 the Internet", 2015,

 <https://mk0rofifiqa2w3u89nud.kinstacdn.com/wp-

 content/uploads/COE-report-on-FOAA-rights-on-the-

 internet-.pdf>.

ten Oever, et al. Expires May 6, 2021 [Page 24]

Internet-Draft FoA November 2020

 [Crawford]

 Crawford, D., "The WebRTC VPN "Bug" and How to Fix", 2015,

 <https://www.bestvpn.com/the-webrtc-vpn-bug-and-how-to-

 fix-it/>.

 [CRC] Wikipedia, ., "Lorum", 2000,

 <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/

 AllDocIDs/E123F4F71DCAE3E7CA256B4F007F2905>.

 [CRPD] United Nations, "Convention on the Rights of Persons with

 Disabilities", 2007,

 <http://www.austlii.edu.au/au/other/dfat/

 treaties/2008/12.html>.

 [Glasius] Glasius, M., Schalk, J., and M. De Lange, "Illiberal Norm

 Diffusion: How Do Governments Learn to Restrict

 Nongovernmental Organizations?", 2020,

 <https://academic.oup.com/isq/article/64/2/453/5823498>.

 [HafnerandLyon]

 Hafnerand, K. and M. Lyon, "Where Wizards Stay Up Late.

 The Origins of the Internet", First Touchstone Edition

 (1998): 93. , 1998, <https://doi.org/10.1111/misr.12020>.

 [HRPC-charter]

 Human Rights Protocol Consideration RG, ., "Charter for

 Research Group", 2015,

 <https://datatracker.ietf.org/doc/charter-irtf-hrpc/>.

 [HussainHoward]

 Hussain, M. and P. Howard, "What Best Explains Successful

 Protest Cascades? ICTs and the Fuzzy Causes of the Arab

 Spring", Int Stud Rev (2013) 15 (1): 48-66. , 2013,

 <https://doi.org/10.1111/misr.12020>.

 [ICCPR] United Nations General Assembly, "International Covenant

 on Civil and Political Rights", 1966,

 <http://www.ohchr.org/EN/ProfessionalInterest/Pages/

 CCPR.aspx>.

 [Kaye] Kaye, D., "The use of encryption and anonymity in digital

 communications", 2015,

 <https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/

 Session29/Documents/A.HRC.29.32\_AEV.doc>.

 [LEAP] LEAP, "The Right to Whisper", 2020,

 <https://leap.se/en/about-us/vision>.

ten Oever, et al. Expires May 6, 2021 [Page 25]

Internet-Draft FoA November 2020

 [Loi] Loi, M. and M. Christen, "Two Concepts of Group Privacy",

 2020, <https://link.springer.com/article/10.1007/

 s13347-019-00351-0>.

 [Mainwaringetal]

 Mainwaring, S., Chang, M., and K. Anderson,

 "Infrastructures and Their Discontents: Implications for

 Ubicomp", DBLP Conference: Conference: UbiComp 2004:

 Ubiquitous Computing: 6th International Conference,

 Nottingham, UK, September 7-10, 2004. Proceedings , 2004,

 <http://www.dourish.com/classes/readings/Mainwaring-

 Infrastructure.pdf>.

 [Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and

 the first amendment", 1998, <http://www.cardozoaelj.com/

 wp-content/uploads/2013/02/Marcus.pdf>.

 [Nasser] Nasser, R., "&#1602;&#1604;&#1576;", 2013,

 <https://nas.sr/%D9%82%D9%84%D8%A8/>.

 [NelsonHedlun]

 Minar, N. and M. Hedlun, "A Network of Peers: Models

 Through the History of the Internet", Peer to Peer:

 Harnessing the Power of Disruptive Technologies, ed: Andy

 Oram , 2001, <http://library.uniteddiversity.coop/

 REconomy\_Resource\_Pack/

 More\_Inspirational\_Videos\_and\_Useful\_Info/Peer\_to\_Peer-

 Harnessing\_the\_Power\_of\_Disruptive\_Technologies.pdf>.

 [Nyokabi] Nyokabi, D., Diallo, N., Ntesang, N., White, T., and T.

 Ilori, "The right to development and internet shutdowns:

 Assessing the role of information and communications

 technology in democratic development in Africa", 2019,

 <https://repository.gchumanrights.org/bitstream/handle/20.

 500.11825/1582/3.Global%20article%20HRDA\_2\_2019.pdf?sequen

 ce=4&isAllowed=y>.

 [Pensado] Jaime Pensado, ., "Student Activism. Utopian Dreams.",

 ReVista. Harvard Review of Latin America (2012). , 2012,

 <http://revista.drclas.harvard.edu/book/student-activism>.

 [PipekWulf]

 Pipek, V. and W. Wolf, "Infrastructuring: Towards an

 Integrated Perspective on the Design and Use of

 Information Technology", Journal of the Association for

 Information Systems (10) 5, pp. 306-332 , 2009.

ten Oever, et al. Expires May 6, 2021 [Page 26]

Internet-Draft FoA November 2020

 [RFC0001] Crocker, S., "Host Software", RFC 1, DOI 10.17487/RFC0001,

 April 1969, <https://www.rfc-editor.org/info/rfc1>.

 [RFC0155] North, J., "ARPA Network mailing lists", RFC 155,

 DOI 10.17487/RFC0155, May 1971,

 <https://www.rfc-editor.org/info/rfc155>.

 [RFC0903] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A

 Reverse Address Resolution Protocol", STD 38, RFC 903,

 DOI 10.17487/RFC0903, June 1984,

 <https://www.rfc-editor.org/info/rfc903>.

 [RFC1211] Westine, A. and J. Postel, "Problems with the maintenance

 of large mailing lists", RFC 1211, DOI 10.17487/RFC1211,

 March 1991, <https://www.rfc-editor.org/info/rfc1211>.

 [RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-

 4)", RFC 1771, DOI 10.17487/RFC1771, March 1995,

 <https://www.rfc-editor.org/info/rfc1771>.

 [RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation,

 selection, and registration of an Autonomous System (AS)",

 BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996,

 <https://www.rfc-editor.org/info/rfc1930>.

 [RFC1958] Carpenter, B., Ed., "Architectural Principles of the

 Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996,

 <https://www.rfc-editor.org/info/rfc1958>.

 [RFC2277] Alvestrand, H., "IETF Policy on Character Sets and

 Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277,

 January 1998, <https://www.rfc-editor.org/info/rfc2277>.

 [RFC2810] Kalt, C., "Internet Relay Chat: Architecture", RFC 2810,

 DOI 10.17487/RFC2810, April 2000,

 <https://www.rfc-editor.org/info/rfc2810>.

 [RFC2812] Kalt, C., "Internet Relay Chat: Client Protocol",

 RFC 2812, DOI 10.17487/RFC2812, April 2000,

 <https://www.rfc-editor.org/info/rfc2812>.

 [RFC3233] Hoffman, P. and S. Bradner, "Defining the IETF", BCP 58,

 RFC 3233, DOI 10.17487/RFC3233, February 2002,

 <https://www.rfc-editor.org/info/rfc3233>.

 [RFC4084] Klensin, J., "Terminology for Describing Internet

 Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084,

 May 2005, <https://www.rfc-editor.org/info/rfc4084>.

ten Oever, et al. Expires May 6, 2021 [Page 27]

Internet-Draft FoA November 2020

 [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A

 Border Gateway Protocol 4 (BGP-4)", RFC 4271,

 DOI 10.17487/RFC4271, January 2006,

 <https://www.rfc-editor.org/info/rfc4271>.

 [RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R.

 Thayer, "OpenPGP Message Format", RFC 4880,

 DOI 10.17487/RFC4880, November 2007,

 <https://www.rfc-editor.org/info/rfc4880>.

 [RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P)

 Architecture: Definition, Taxonomies, Examples, and

 Applicability", RFC 5694, DOI 10.17487/RFC5694, November

 2009, <https://www.rfc-editor.org/info/rfc5694>.

 [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet

 Mail Extensions (S/MIME) Version 3.2 Message

 Specification", RFC 5751, DOI 10.17487/RFC5751, January

 2010, <https://www.rfc-editor.org/info/rfc5751>.

 [RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer

 (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March

 2011, <https://www.rfc-editor.org/info/rfc6176>.

 [RFC7118] Baz Castillo, I., Millan Villegas, J., and V. Pascual,

 "The WebSocket Protocol as a Transport for the Session

 Initiation Protocol (SIP)", RFC 7118,

 DOI 10.17487/RFC7118, January 2014,

 <https://www.rfc-editor.org/info/rfc7118>.

 [RFC7194] Hartmann, R., "Default Port for Internet Relay Chat (IRC)

 via TLS/SSL", RFC 7194, DOI 10.17487/RFC7194, August 2014,

 <https://www.rfc-editor.org/info/rfc7194>.

 [RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights

 Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280,

 October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[RutzenZenn] Rutzen, D. and J. Zenn, “ Association and Assembly in the Digital Age”, The International Journal of Not-for-Profit Law, Volume 13, Issue 4, December 2011 <https://www.icnl.org/resources/research/ijnl/association-and-assembly-in-the-digital-age-2>

[Sauter] Sauter, M., "The Coming Swarm", Bloomsbury , 2014.

 [Schleuder]

 Nadir, "Schleuder - A gpg-enabled mailinglist with

 remailing-capabilities.", 2017,

 <https://schleuder.nadir.org/>.

ten Oever, et al. Expires May 6, 2021 [Page 28]

Internet-Draft FoA November 2020

 [Stanford]

 Brownlee, K. and D. Jenkins, "Freedom of Association",

 2019,

 <https://plato.stanford.edu/entries/freedom-association/>.

 [Swire] Peter Swire, ., "Social Networks, Privacy, and Freedom of

 Association: Data Empowerment vs. Data Protection", North

 Carolina Law Review (2012) 90 (1): 104. , 2012,

 <https://ssrn.com/abstract=1989516 or

 http://dx.doi.org/10.2139/ssrn.1989516>.

 [Troncosoetal]

 Troncoso, C., Isaakdis, M., Danezis, G., and H. Halpin,

 "Systematizing Decentralization and Privacy: Lessons from

 15 Years of Research and Deployments", Proceedings on

 Privacy Enhancing Technologies ; 2017 (4):307-329 , 2017,

 <https://www.petsymposium.org/2017/papers/issue4/

 paper87-2017-4-source.pdf>.

 [UDHR] United Nations General Assembly, "The Universal

 Declaration of Human Rights", 1948,

 <http://www.un.org/en/documents/udhr/>.

 [UNHCHR2020] Michelle Bachelet, “Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Report of the United Nations High Commissioner for Human Rights” A/HRC/44/24, 2020

<https://undocs.org/en/A/HRC/44/24>.

 [UNGPBHR] United Nations, "Guiding Principles on Business and Human

 Rights", 2011,

 <https://www.ohchr.org/documents/publications/

 guidingprinciplesbusinesshr\_en.pdf>.

 [UNSRFAA2012] Maina Kiai, "Report of the Special Rapporteur on the

 rights to freedom of peaceful assembly and of

 association", A/HRC/20/27 , 2012,

 <http://freeassembly.net/wp-content/uploads/2013/10/A-HRC-

 20-27\_en-annual-report-May-2012.pdf>.

[UNSRFAA2019] Clément Voule, “Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association”, A/HRC/41/41, 2019

<https://undocs.org/A/HRC/41/41>

ten Oever, et al. Expires May 6, 2021 [Page 29]

Internet-Draft FoA November 2020

 [UNHRC2018]

 United Nations Human Rights Council, "UN Human Rights

 Council Resolution 'The promotion, protection and

 enjoyment of human rights on the Internet'2018 <https://digitallibrary.un.org/record/1639840?ln=en> .

 [ViennaDeclaration]

 United Nations, "Vienna Declaration and Programme of

 Action", 1993,

 <https://www.ohchr.org/en/professionalinterest/pages/

 vienna.aspx>.

 [Vu] Vu, Quang Hieu, ., Lupu, Mihai, ., and . Ooi, Beng Chin,

 "Peer-to-Peer Computing: Principles and Applications",

 2010, <https://www.springer.com/cn/book/9783642035135>.

 [W3C] W3C, "Accessibility", 2015,

 <https://www.w3.org/standards/webdesign/accessibility>.

12.2. URIs

 [1] mailto:hrpc@ietf.org

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

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

Authors' Addresses

 Niels ten Oever

 University of Amsterdam & Texas A&M University

 EMail: mail@nielstenoever.net

 Gisela Perez de Acha

 Derechos Digitales

 EMail: gisela@derechosdigitales.org

 Stephane Couture

 University de Montreal

 EMail: stephane.couture@umontreal.ca

ten Oever, et al. Expires May 6, 2021 [Page 30]

Internet-Draft FoA November 2020

 Mallory Knodel

 Center for Democracy & Technology

 EMail: mknodel@cdt.org