Workgroup:
Human Rights Protocol Considerations Research
Group
Internet-Draft: draft-irtf-hrpc-association-13
Published: 11 April 2023
Intended Status: Informational
Expires: 13 October 2023
Authors: N. ten Oever
University of Amsterdam
S. Couture
Université de Montréal
M. Knodel
Center for Democracy & Technology

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

Abstract

This document explores whether the relationship between the Internet architecture and the ability of people to exercise their rights to peaceful assembly and association online. It does so by asking the question: what are the protocol development considerations for freedom of assembly and association? The Internet increasingly mediates our lives, our relationships, and our ability to exercise our human rights. As a global assemblage, the Internet provides a public space, yet it is predominantly built on private infrastructure. Since Internet protocols and architecture play a central role in the management, development, and use of the Internet, we analyze the relation between protocols, architecture, and the rights to assemble and associate to mitigate infringements on those rights. This document concludes that the way in which infrastructure is designed and implemented impacts people’s ability to exercise their freedom of assembly and association. It is therefore recommended that the potential impacts of Internet technologies should be assessed, reflecting recommendations of various UN bodies and international norms. Finally, the document considers both the limitations on changing association and impact of "forced association" in the context of online platforms.

Status of This Memo

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

This Internet-Draft will expire on 13 October 2023.

Copyright Notice

Table of Contents

1. Introduction

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

- John Culkin (1967)

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

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

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

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

The current draft continues the work started in “Research into Human Rights Protocol Considerations” [RFC8280] by investigating the impact of Internet protocols on a specific set of human rights, namely the right to peaceful assembly and the right to association. Taking into consideration the international human rights framework, the present document seeks to deepen the relationship between these human rights and Internet architecture, protocols, and standards. In that way, we continue the work of the Human Rights Protocol Consideration Research Group, as laid out in its charter, “to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly” [HRPC-charter].

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

2. Vocabulary used

Architecture The design of a structure

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

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

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

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

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

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

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

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

relational: infrastructure always develops in relation to something or someone [Bowker].

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

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

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

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

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

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

3. Research question

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

4. Methodology

In this document, we deepen our exploration of human rights and protocols by assessing one specific set of human rights: freedom of association and assembly, abbreviated here as FAA. Our methodology for doing so is the following: first, we provide a brief twofold literature review addressing the philosophical and legal definitions of FAA and how this right has already been interpreted or analyzed in the digital context. This literature review is not exhaustive but aims at providing some lines of questioning that could later be used for protocol development. Second, we look at some cases of Internet protocols that are relevant to the sub-questions highlighted in the literature review and analyze how these protocols facilitate or inhibit the right to peaceful assembly and association.

5. Literature Review

5.1. FAA definition and core treaties

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

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

Other treaties are sometimes cited as the source and framework for the rights to freedom of association and assembly. An example of this is Article 5 of the International Convention on the Elimination of All Forms of Racial Discrimination [CERD] which stipulates freedom of peaceful assembly and association should be guaranteed “without discrimination as to race, colour, national or ethnic origin”; Article 15 of the Convention on the Rights of the Child [CRC] which recognises these rights for children with the restrictions cited above; and Article 21 of the Convention on the Rights of Persons with Disabilities [CRPD] which insists on usable and accessible formats and technologies appropriate for persons with different kinds of disabilities. The freedoms of peaceful assembly

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

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

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

The Human Rights Committee considers restrictions of activities of free association online or activities of free association reliant upon digital services, that are also protected under article 21, and stipulates that "States parties must not, for example, block or hinder Internet connectivity in relation to peaceful assemblies. The same applies to geotargeted or technology-specific interference with

connectivity or access to content.” Additionally, “States should ensure that the activities of Internet service providers and intermediaries do not unduly restrict assemblies or the privacy of assembly participants.” [UNGC37].

Interpreting international law, the right to freedom of peaceful assembly and the right to freedom of association protects any collective, gathered either permanently or temporarily for peaceful purposes, online and offline. It is important to underline the property of “freedom” because the right to freedom of association and assembly is voluntary and uncoerced: anyone can join or leave a group of choice, which in turn means one should not be forced to either join, stay or leave. In other words, free association means that only the association of people itself determines who can be a member. An assembly is an "intentional and temporary gathering of a collective in a private or public space for a specific purpose: demonstrations, indoor meetings, strikes, processions, rallies, or even sits-in" [UNGA]. Association has a more formal and established nature and refer to a group of individuals or legal entities brought together in order to collectively act, express, promote, pursue, or defend a field of common interests [UNSRFOAA2012]. Think about civil society organizations, clubs, cooperatives, non-governmental organizations, religious associations, political parties, trade unions, or foundations.

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

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

5.2. FAA in the digital era

The United Nations Human Rights Council adopted resolutions on the promotion, protection and enjoyment of human rights on the Internet in 2012, 2014, 2016 and 2018, affirming and reaffirming "that the same rights that people have offline must also be protected online" [UNHRC2018]. Therefore the digital environment is no exception to application of the right of freedom of association. Various other resolutions and reports have established the online applicability of the freedoms of association and assembly, most recently and authoritatively the Human Rights Committee in General Comment 37 (2020)[UNGC37]. The questions that remain are how these rights should be conceptualized and implemented in different parts and levels of digital environments.

The right to freedom of assembly and association online is the subject of increasing discussions and analysis. Especially since social media played an important role in several revolutions in 2011, there have been increasing and ever more sophisticated attacks by autocratic governments on online communities and other associational activities occurring on the Internet [RutzenZenn]. In 2016, the Council of Europe published the “Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet” [CoE] which noted that while the Internet and communication technologies are not explicitly mentioned in international treaties, these treaties nevertheless apply to “the online environment”. The report argues that the “Internet is the public sphere of the 21st century”, demonstrated by the fact that informal associations can be gathered at scale in a matter of hours on the Internet, and that digital communication tools often serve to facilitate, publicize or otherwise enable associations or assemblies in person, like a protest or demonstration. The report notes, on the other hand, the negative ways in which the Internet can also be used to promote or facilitate terrorism, violence and hate speech, thus insisting on the “extremely important and urgent” need to fight online terrorist activities such as recruitment or mobilization, while at the same time respecting the right to peaceful assembly and association of other users. The report mentions the following examples that could further our reflection:

* network shutdowns during the Arab Spring, to prevent people from organising themselves or assembling

*California's Bay Area Rapid Transit (BART) shutdown of mobile phone service, to prevent potential property destruction by protesters and disruption of service

*the wholesale blocking of Google in China as a violation of freedom of expression

*the telecom company Telus's blocking of customers' access to websites critical of Telus during a Telecommunications Workers Union strike against it

*the targeting of social media users who call for or organise protests though the Internet in Turkey's Gezi Park protests

*mass surveillance or other interferences with privacy in the context of law enforcement and national security

*use of VPNs (Virtual Private Networks) and the Tor network to ensure anonymity

*Distributed Denial of Service attacks (DDoS) as civil disobedience.

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

*"[Undertake] human rights impact assessments which incorporate the rights to freedom of peaceful assembly and of association when developing or modifying their products and services,"

*"increase the quality of participation in and implementation of existing multi-stakeholder initiatives,"

*"collaborate with governments and civil society to develop technology that promotes and strengthens human rights,"

*"support the research and development of appropriate technological solutions to online harassment, disinformation and propaganda, including tools to detect and identify State-linked accounts and bots," and

*"adopt monitoring indicators that include specific concerns related to freedom of peaceful assembly and association."

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

1. Organization of protests. The Internet and social media are enablers of protests, as was seen in the Arab Spring. Some of these protests - like online petitions or campaigns - are similar to offline association and assembly, but other protest forms are inherent to the Internet. Hacking and DDoS are subject to controversy within the Internet community: some finding them legitimate acts of protest, and others not.

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

3. Anonymity and pseudonymity. Anonymity and pseudonymity can be useful protection mechanisms for those who'd like to attend online assemblies without facing retribution. On the other hand, anonymity can be used to harm society, such as in online fraud or sexual predation.

Online association and assembly are the starting point of civic mass mobilization in modern democracies, and even more so where physical gatherings have been impossible or dangerous [APC]. Throughout the world - from the Arab Spring to Latin American student movements and the #WomensMarch - the Internet has played a crucial role by providing means for the fast dissemination of information otherwise mediated by the press, or even forbidden by the government [Pensado]. According to Hussain and Howard the Internet helped “build solidarity networks and identification of collective identities and goals, extend the range of local coverage to international broadcast networks” and served as a platform for contestation of “the future of civil society and information infrastructure” [HussainHoward]. The IETF itself, defined as an "open global community" of network designers, operators, vendors, and researchers [RFC3233] is also protected by freedom of assembly and association. Discussions, comments and consensus around RFCs are possible because of the collective expression that freedom of association and assembly allow. The very word “protocol” found its way into the language of computer networking based on the need for collective agreement among a group of assembled network users [HafnerandLyon].

[RFC8280] discusses issues of FAA, specifically:

* The expansion of DNS as an enabler of association for minorities. The document argues that the expansion of the DNS to allow for new generic Top Level Domains (gTLDs) can have negative impacts on freedom of association because of restrictive policies by some registries and registrars. On the other hand, gTLDs could also enable communities to build clearly identifiable spaces for association (such as .gay).

* The impact of Distributed Denial of Service attacks on freedom of association. Whereas DDoS has been used as a tool for protest, in many cases it infringes on the freedom of expression of other parties. Furthermore, often devices (such as IoT devices and routers) are enlisted in such DDoS attacks without the owner's or user's consent. Thus they do not have the possibility to exit this assembly. Therefore the document concluded that the IETF "should try to ensure that their protocols cannot be used for DDoS attacks".

* The impact of middleboxes on the ability of users to connect to the Internet. Lack of connectivity can significantly impact freedom of assembly and association. In particular, if the user cannot retrieve the reason for their inability to connect, there may not be access to due process to dispute the lack of (secure or private) connectivity, either in general or to a specific service.

In June 2020, the United Nations High Commissioner for Human Rights concluded that technologies can be enablers of the exercise of FAA, but technology is also significantly used to interfere with those rights. Specifically, the report mentions network shutdowns and the use of technology to surveil or crack down on protesters, leading to human rights violations. This includes facial recognition technology, among other ways to violate the privacy of people engaged in an assembly or association. The report makes it explicit that companies play a significant role, by developing, providing or selling the technology, but also by directly causing these violations [UNHRC2020].

5.3. Specific questions raised from the literature review

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

1. Should protocols be designed to enable legitimate limitations on association in the interests of "national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms

of others", as stated in the ICCPR article 21 [ICCPR]? Where in the stack do we care for FAA?

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

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

4. Does protocol development sufficiently consider usable and accessible formats and technologies appropriate for all persons, including those with different kinds of abilities?

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

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

6. Analysis

As the Internet mediates collective action and collaboration, it impacts on freedom of association and assembly. To answer our research question regarding how Internet architecture enables and/or inhibits such human rights, we researched several independent and typical cases related to protocols that have been either adopted by the IETF, or are widely used on the Internet. Our goal is to determine how they facilitate freedom of assembly and association, or how they inhibit it through their design or implementation.

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

We use the literature review to guide our process of inquiry for each case, and to dive deeper in what can be found interesting about each case as it relates to freedom of association. In each section, we consider one of the questions identified in the review, and apply the protocol or application (with some overlaps) to that question.

6.1. Got No Peace: Spam and DDoS

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

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

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

> Whereas states have an obligation to protect human rights, there has been an increasing call for non-state actors, such as companies, also to respect human rights [UNGPBHR]. The UN adopted guiding principles on business and human rights [UNGPBHR] and talks within the HRC are ongoing about an international legally binding instrument to regulate the activities of transnational corporations and other business enterprises. This includes a chain-responsibility of actors: not only that the company’s own processes should not negatively impact human rights, but also that the company should also engage in due diligence processes, such as human rights impact assessments. This includes an assessment of whether the products that are sold, or the services that are provided, can be used to engage in human rights violations, or whether human rights violations occur in any stage of the supply chain of the company. If this is the case, measures should be taken to mitigate this.
>
> In the case of dual-use technologies, where technology could be used for legitimate purposes, but could also be used to limit freedom of association or assembly, this obligation might mean that producers or sellers should limit the parties they sell to, or even better, ensure that the illegitimate use of the technology is not technically possible anymore, or made more difficult.

6.1.1. Spam

> In the 1990s as the Internet became more widely adopted, spam came to be defined as irrelevant or unsolicited messages that were posted

many times to multiple news groups or mailing lists [Marcus]. Here questions of consent, but also harm, are crucial. In the 2000s a significant part of the technical and policy debate on spam revolved around the fact that certain corporations considered spam to be a form of "commercial speech", thus encompassed by free expression rights [Marcus]. Yet spam can be not only a nuisance, but a threat to systems and users.

This leaves us with an interesting case around spam mitigation: spam is currently handled mostly by mail providers on behalf of the user. Many countries are adopting regulatory opt-in regimes for mailing lists and commercial e-mail, with a possibility of serious fines in case of violation. Yet many ask: is spam not the equivalent of the fliers and handbills ever present in our offline world? The big difference between the proliferation of such messages offline and online is the scale. It is not hard for a single person to message a lot of people online, whereas if that person needed to go house by house the impact of their efforts would be much smaller. Conversely, if it were a common practice to expose people to unlimited unwanted messages online, users would be drowned in such messages. This puts a large burden on filtering, and in sifting through many messages, other expressions would be drowned out and would be severely hampered. Allowing unlimited sending of unsolicited messages would be a blow against freedom of speech: when everyone talks, nobody can hear.

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

6.1.2. DDoS

Distributed Denial of Service attacks are leveled against a server or service by a controller of multiple hosts by overloading the server or service’s bandwidth or resources (volume-based floods) or exploiting protocol behaviours (protocol attacks). DDoS attacks can thus stifle the right to assemble online for organisations whose websites are targeted. At the same time there are comparisons made between DDoS attacks and sit-in protests [Sauter]. However the main distinction is significant: only a small fragment of “participants”

(from controllers to compromised device owners) in DDoS attacks are aware or willing [RFC8280]. Notably, DDoS attacks are increasingly used to commit crimes such as extortion, which infringe on others' human rights.

Because of the interrelation of technologies, it cannot be said that there is one point in the technical stack where one can locate the characteristics of "peaceful" or "non-peaceful" association visible to protocol developers. In the cases of spam blocking and DDoS mitigation, "peaceful or non-peaceful" is not a meaningful heuristic, or even characteristic, of problematic content. Their commonalities are their volume, and the unrequested nature of participation in DDoS and the receiving of spam. One could say that the 'receivers' of demonstrations did not ask for it either, but in the case of spam the receivers are generally a larger group than one particular target, else the spam could be described as a DDoS attack against one target. This allows us to draw the conclusion that DDoS and spam are not examples of freedom of association or assembly.

6.2. Holistic Agency: Mailing Lists and Spam

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

6.2.1. Mailing lists

Since the beginning of the Internet mailing lists have been a key site of assembly and association [RFC0155] [RFC1211]. In fact, mailing lists were one of the 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 later, mailing lists are pervasive and help communities to engage, have discussions, share information, ask questions, and build ties. Even as social media and discussion forums grow, mailing lists continue to be widely used [AckermannKargerZhang] and are still a crucial tool to organise groups and individuals around themes and causes [APC3].

Mailing lists' pervasive use are partly explained because they allow for free and low-cost association: people subscribe (join) and unsubscribe (leave) as they please. Another contributor to their widespread use is that email functions on low bandwith connections and across platforms. Mailing lists also allow for association of

specific groups on closed lists. This enables agency of membership, a key component of freedom of association and assembly.

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

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

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

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

6.3.1. Email

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

6.3.2. Mailing lists

Not only are mailing lists a good example of how protocols can facilitate the necessary ingredient of agency in freedom of association, we can see how particular features of mailing lists enable or inhibit freedom of association and assembly.

The archival function of mailing lists allows for posterior accountability and analysis.

The ubiquity and interoperability of email, and by extension mailing lists, provides a low barrier to entry to an inclusive medium.

Association and assembly online can be undermined when right to privacy is at risk. One downside of mailing lists are the privacy and security concerns generally associated with email. End-to-end encryption with OpenPGP [RFC4880] and S/MIME [RFC5751] can keep email communications authenticated and confidential if properly configured, deployed and used, but users often do not have those protections. And with mailing lists, this protection is not typically possible, because with many lists the final recipients are not known to the sender. There have been experimental solutions to address this issue [Schleuder], but this has not been standardized or widely deployed.

6.3.3. IRC

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

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

For the purposes of civic participation and freedom of association and assembly in particular, it is critical that IRC’s federated design allows many interoperable, yet customisable, instances and basic assurance of confidentiality through transport encryption. IRC differs from email in the sense that it allows for real-time interaction, stimulating the sense of conversation. This allows people to organize, develop ideas as well as joint identities. This is strengthened through the federated nature of IRC, which gives

users the ability to use and connect through different servers, contributing to freedom of association. We investigate the particular aspect of agency in membership through moderation in the section 'Block Together Now: IRC and Refusals' below.

6.3.4. WebRTC

Multi-party video conferencing protocols like WebRTC [RFC6176] [RFC7118] allow for robust, bandwidth-adaptive, wideband and super-wideband video and audio discussions in groups. This facilitates exchanges over the Internet in a similar manner to IRC, but including the usage of audio and video. WebRTC can be configured as direct peer-to-peer videochat without sending data through a central server. This ability to function without a central server is a strong facilitator of freedom of association and assembly.

However, WebRTC comes with many different configuration options, which can leave users open to unexpected privacy leakages:

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

[AndersonGuarnieri]

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

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

6.3.5. Peer-to-peer networking

Since the ARPANET project, the original idea behind the Internet was conceived as what we would now call a peer-to-peer system [RFC0001]. Over time it has increasingly shifted towards a client/server model with “millions of consumer clients communicating with a relatively privileged set of servers” [NelsonHedlun]. However, the foundational networking protocol of the modern Internet, the Border Gateway Protocol [RFC1163] [RFC1164] [RFC4271], still functions like original peer to peer network, with an extensive practice of peering and transit [MeierHahn2015]. For an example higher up the stack one could look at the peer-to-peer architecture of BitTorrent [RFC5694].

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

In his book The Wealth of Networks, [Benkler2] significantly expands on his definition of commons-based peer production. In his view, what distinguishes commons-based production is that it 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.” To ensure that the knowledge generated is available for free use, commons-based projects are often shared under an open license

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

nodes are organized into two layers: the upper tier servers and the lower tier common nodes [Vu].

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

6.4. Universal Access: The Web

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

6.4.1. Accessibility

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

6.4.2. Internationalization

The IETF uses English as its primary working language, both in its documentation and in its communication. This is also the case for reference implementations. It is estimated that roughly 20% of the Earth’s population speaks English, whereas only 360 million speak English as their first language. [RFC2277] states that ‘"Internationalization is for humans. This means that protocols are not subject to internationalization; text strings are.", this implies that protocol developers, as well as people that work with protocols, are not people, or that protocol developers all speak English. As a result, it may be significantly easier for people who have a command of the English language to become a protocol developer. It could also lead to a divergence, with the development of separate protocols that are developed within large language communities that don't use English language or Latin script. This makes it harder for people who seek to shape their own space of

association and assembly on the Internet to do so. Communities may therefore be driven to rely on proprietary and non-interoperable services, such as Facebook and Weibo, where use of their own script and language is supported.

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

6.5. Block Together Now: IRC and Refusals

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

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

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

Moderation and de-federation can be a tool to uphold freedom of association and assembly, because it allows groups to have control over their own make up. IRC servers may deploy different policies for the ability of users to create their own channels or 'rooms', and for the delegation of 'operator'-rights in such spaces. However, these controls can also seriously hamper the ability of a group to get together. Some argue that the low cost of creating a new group

is a protection against this, however, this could lead to a repetition of crises of moderation of membership and speech.

7. Conclusions: What can we learn from these case studies?

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

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

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

Lastly, the increasing shift away from federated and interoperable messaging exchange towards closed platforms with non-interoperable chat and media-sharing functionality have a significant impact on

the distributed and open nature of the use of the Internet. Often these platforms are built on open protocols but do not allow for interoperability or data portability. Future research could further investigate how the use of social media platforms has enabled individuals to associate in groups, but at the same time rendered those groups unable to change or transcend platforms, therefore leading to sorts of "bounded association" and "forced association" both of which inhibit people from fully exercising their freedom of assembly and association.

8. Acknowledgements

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

*Fred Baker and Jefsey for work on Internet definitions.

*Stephane Bortzmeyer, ICNL, and Lisa Vermeer for several concrete text suggestions that found their way in this document.

*Mark Perkins and Gurshabad for finding a lot of typos.

*Nick Doty, Gurshabad Grover, an anonymous reviewer, ICNL, Lisa Vermeer, and Sandra Braman for full reviews.

*The hrpc mailinglist at large for a very constructive discussion on a hard topic.

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

9. Work Space

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

10. Security Considerations

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

11. IANA Considerations

This document has no actions for IANA.

12. Research Group Information

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

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

13. Informative References

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

[AckermannKargerZhang] Ackerman, M. S., Karger, D. R., and A. X. Zhang, "Mailing Lists: Why Are They Still Here, 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>.

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

[Benkler] Benkler, Y., "Peer Production and Cooperation", 2009, <http://www.benkler.org/Peer%20production%20and%20cooperation%2009.pdf>.

[Benkler2] Benkler, Y., "The wealth of Networks - How social production transforms markets and freedom", New Haven and

London - Yale University Press , 2006, <http://is.gd/rxUpTQ>.

[Bloketal] Blok, A., Nakazora, M., and B. R. Winthereik, "Infrastructuring Environments", Science as Culture 25:1, 1-22. , 2016.

[Bowker] Bowker, G., "Information mythology and infrastructure", In: L. Bud (Ed.), Information Acumen: The Understanding and use of Knowledge in Modern Business,Routledge,London, 1994,pp.231-247 , 1994.

[CERD] United Nations, "Convention on the Elimination of all forms of Racial Discrimination", 1966, <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/2F70352A0B65EB67CA256B6E0075FE13>.

[CoE] Council of Europe, "Freedom of assembly and association on the Internet", 2015, <https://mk0rofifiqa2w3u89nud.kinstacdn.com/wp-content/uploads/COE-report-on-FOAA-rights-on-the-internet-.pdf>.

[Crawford] Crawford, D., "The WebRTC VPN “Bug” and How to Fix", 2015, <https://www.bestvpn.com/the-webrtc-vpn-bug-and-how-to-fix-it/>.

[CRC] Wikipedia, "Lorum", 2000, <https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/E123F4F71DCAE3E7CA256B4F007F2905>.

[CRPD] United Nations, "Convention on the Rights of Persons with Disabilities", 2007, <http://www.austlii.edu.au/au/other/dfat/treaties/2008/12.html>.

[FoAdef] Wikipedia, "Freedom of association", 2021, <https://en.wikipedia.org/wiki/Freedom_of_association>.

[Glasius] Glasius, M., Schalk, J., and M. De Lange, "Illiberal Norm Diffusion: How Do Governments Learn to Restrict Nongovernmental Organizations?", 2020, <https://academic.oup.com/isq/article/64/2/453/5823498>.

[HafnerandLyon] Hafnerand, K. and M. Lyon, "Where Wizards Stay Up Late. The Origins of the Internet", First Touchstone Edition (1998): 93. , 1998, <https://doi.org/10.1111/misr.12020>.

[HRPC-charter] Human Rights Protocol Consideration RG, "Charter for Research Group", 2015, <https://datatracker.ietf.org/doc/charter-irtf-hrpc/>.

[HussainHoward] Hussain, M. M. and P. N. Howard, "What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring", Int Stud Rev (2013) 15 (1): 48-66. , 2013, <https://doi.org/10.1111/misr.12020>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1966, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[Kaye] Kaye, D., "The use of encryption and anonymity in digital communications", 2015, <https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>.

[Loi] Loi, M. and M. Christen, "Two Concepts of Group Privacy", 2020, <https://link.springer.com/article/10.1007/s13347-019-00351-0>.

[Mainwaringetal] Mainwaring, S. D., Chang, M. F., and K. Anderson, "Infrastructures and Their Discontents: Implications for Ubicomp", DBLP Conference: Conference: UbiComp 2004: Ubiquitous Computing: 6th International Conference, Nottingham, UK, September 7-10, 2004. Proceedings , 2004, <http://www.dourish.com/classes/readings/Mainwaring-Infrastructure.pdf>.

[Marcus] Marcus, J., "Commercial Speech on the Internet: Spam and the first amendment", 1998, <http://www.cardozoaelj.com/wp-content/uploads/2013/02/Marcus.pdf>.

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

[Nasser] Nasser, R., "قلب", 2013, <https://nas.sr/%D9%82%D9%84%D8%A8/>.

[NelsonHedlun] Minar, N. and M. Hedlun, "A Network of Peers: Models Through the History of the Internet", Peer to Peer: Harnessing the Power of Disruptive Technologies, ed: Andy Oram , 2001, <http://library.uniteddiversity.coop/REconomy_Resource_Pack/More_Inspirational_Videos_and_Useful_Info/Peer_to_Peer-Harnessing_the_Power_of_Disruptive_Technologies.pdf>.

[Nyokabi] Nyokabi, D. M., Diallo, N., Ntesang, N. W., White, T. K., and T. Ilori, "The right to development and internet shutdowns: Assessing the role of information and

communications technology in democratic development in Africa", 2019, <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1582/3.Global%20article%20HRDA_2_2019.pdf?sequence=4&isAllowed=y>.

[Pensado] Jaime Pensado, "Student Activism. Utopian Dreams.", ReVista. Harvard Review of Latin America (2012). , 2012, <http://revista.drclas.harvard.edu/book/student-activism>.

[PipekWulf] Pipek, V. and W. Wolf, "Infrastructuring: Towards an Integrated Perspective on the Design and Use of Information Technology", Journal of the Association for Information Systems (10) 5, pp. 306-332 , 2009.

[RFC0001] Crocker, S., "Host Software", RFC 1, DOI 10.17487/RFC0001, April 1969, <https://www.rfc-editor.org/rfc/rfc1>.

[RFC0155] North, J., "ARPA Network mailing lists", RFC 155, DOI 10.17487/RFC0155, May 1971, <https://www.rfc-editor.org/rfc/rfc155>.

[RFC0903] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", STD 38, RFC 903, DOI 10.17487/RFC0903, June 1984, <https://www.rfc-editor.org/rfc/rfc903>.

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

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

[RFC1211] Westine, A. and J. Postel, "Problems with the maintenance of large mailing lists", RFC 1211, DOI 10.17487/RFC1211, March 1991, <https://www.rfc-editor.org/rfc/rfc1211>.

[RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, DOI 10.17487/RFC1771, March 1995, <https://www.rfc-editor.org/rfc/rfc1771>.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <https://www.rfc-editor.org/rfc/rfc1930>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://www.rfc-editor.org/rfc/rfc1958>.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <https://www.rfc-editor.org/rfc/rfc2277>.

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

[RFC2812] Kalt, C., "Internet Relay Chat: Client Protocol", RFC 2812, DOI 10.17487/RFC2812, April 2000, <https://www.rfc-editor.org/rfc/rfc2812>.

[RFC3233] Hoffman, P. and S. Bradner, "Defining the IETF", BCP 58, RFC 3233, DOI 10.17487/RFC3233, February 2002, <https://www.rfc-editor.org/rfc/rfc3233>.

[RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <https://www.rfc-editor.org/rfc/rfc4084>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/rfc/rfc4271>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/rfc/rfc4880>.

[RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, DOI 10.17487/RFC5694, November 2009, <https://www.rfc-editor.org/rfc/rfc5694>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message

Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/rfc/rfc5751>.

[RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March 2011, <https://www.rfc-editor.org/rfc/rfc6176>.

[RFC7118] Baz Castillo, I., Millan Villegas, J., and V. Pascual, "The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)", RFC 7118, DOI 10.17487/RFC7118, January 2014, <https://www.rfc-editor.org/rfc/rfc7118>.

[RFC7194] Hartmann, R., "Default Port for Internet Relay Chat (IRC) via TLS/SSL", RFC 7194, DOI 10.17487/RFC7194, August 2014, <https://www.rfc-editor.org/rfc/rfc7194>.

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

[RutzenZenn] Rutzen, D. and J. Zenn, "Association and Assembly in the Digital Age", The International Journal of Not-for-Profit Law, Volume 13, Issue 4 , December 2011.

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

[Schleuder] Nadir, "Schleuder - A gpg-enabled mailinglist with remailing-capabilities.", 2017, <https://schleuder.nadir.org/>.

[Stanford] Brownlee, K. and D. Jenkins, "Freedom of Association", 2019, <https://plato.stanford.edu/entries/freedom-association/>.

[Swire] Peter Swire, "Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection", North Carolina Law Review (2012) 90 (1): 104. , 2012, <https://ssrn.com/abstract=1989516 or http://dx.doi.org/10.2139/ssrn.1989516>.

[Troncosoetal] Troncoso, C., Isaakdis, M., Danezis, G., and H. Halpin, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments", Proceedings on Privacy Enhancing Technologies ; 2017 (4):

307-329 , 2017, <https://www.petsymposium.org/2017/papers/issue4/paper87-2017-4-source.pdf>.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <http://www.un.org/en/documents/udhr/>.

[UNGA] Hina Jilani, "Human rights defenders", A/59/401 , 2004, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/401 para. 46>.

[UNGC37] United Nations Human Rights Committee, "Human Rights Committee “General comment No. 37 (2020) on the right of peaceful assembly (article 21)”, CCPR/C/GC/3", 2020, <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11>.

[UNGPBHR] United Nations, "Guiding Principles on Business and Human Rights", 2011, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

[UNHRC2018] United Nations Human Rights Council, "UN Human Rights Council Resolution 'The promotion, protection and enjoyment of human rights on the Internet' (A/HRC/32/L.20)", 2016, <https://digitallibrary.un.org/record/1639840?ln=en>.

[UNHRC2020] Michelle Bachelet and United Nations, "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Report of the United Nations High Commissioner for Human Rights A/HRC/44/24, 2020", 2000, <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx>.

[UNSRFAA2019] Clément Voule and United Nations, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 2019, <https://undocs.org/A/HRC/41/41>.

[UNSRFOAA2012] Maina Kiai and United Nations, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", A/HRC/20/27", 2012, <http://freeassembly.net/wp-content/uploads/2013/10/A-HRC-20-27_en-annual-report-May-2012.pdf>.

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

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

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

Authors' Addresses

Niels ten Oever
University of Amsterdam

Email: mail@nielstenoever.net

Stéphane Couture
Université de Montréal

Email: stephane.couture@umontreal.ca

Mallory Knodel
Center for Democracy & Technology

Email: mknodel@cdt.org