Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: December 24, 2017

N. ten Oever
ARTICLE 19
G. Perez de Acha
Derechos Digitales

June 22, 2017

Freedom of Association on the Internet
draft-tenoever-hrpc-association-01

Abstract

This document aims to scope the relation between Internet protocols and the rights to freedom of assembly and association. The Internet increasingly mediates our lives and our ability to excercise human rights. Since Internet protocols play a central role in the management, development and use of the Internet, the relation between the mentioned rights should be documented and adverse impacts should be mitigated. As there have been methods of protest on the Internet -a form of freedom of assembly- that have proven to be harmful to connectivity and infrastructure, such as DDoS attacks, this text aims to document forms of protest, association and assembly that do not have a negative impact on the Internet infrastructure.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Freedom of assembly and freedom of association are two human rights that protect and enable collective action and expression [UDHR] [ICCPR]. Both rights ensure everyone in a society has the opportunity to express the opinions they hold in common with others, which in turn facilitates dialogue among citizens, as well as between them and political leaders or government [OSCE]. This is important in the process of democratic delibration because causes and opinions are more widely heard when a group of people come together behind the same cause or issue [Tocqueville]. The rights to freedom of assembly and association thus protect any collective, gathered either permanently or temporarily for peaceful purposes. It is indeed a "freedom" because it is voluntary and uncoerced: anyone can join or leave a group of choice, which in turn means not to be forced to either stay or leave.

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

An assembly is an intentional and temporary gathering of a collective in a private or public space for a specific purpose: demonstrations, inside meetings, strikes, processions, rallies or even sits-in [UNHRC]. It is essentially a gathering. The right to protest is encompassed by this right, and it coincides with the right to freedom of expression and the right to hold an opinion. Nonetheless protest, unlike assembly, involves an element of dissent that can be exercised individually whereas assembly always has a collective component [ARTICLE19]. Association on the other hand has a more formal and established nature. It refers to a group of individuals or legal entities brought together in order to collectively act, express, pursue or defend a field of common interests [UNGA]. Within this category we can think about civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions or foundations.

Rights to assembly and association are crucial for the Internet, even if privacy and freedom of expression are the most discussed human rights when it comes to the online world. It is undeniable that communities, collaboration and joint action lie at the heart of the Internet. Even at at linguistical level, the words "networks" and "associations" are close synonyms. Both interconnected groups and assemblies of people depend on "links" and "relationships" [Swire]. One could even argue that as a whole, the networked internet constitutes a big collective, and thus an assembly and an association.

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

In less democratic or authoritarian countries, online association and assembly have been crucial to mobilise groups and people where physical gatherings have been impossible or dangerous [APC]. Throughout the world -from the Arab Spring to Latin American student movements- the Internet has also played a crucial role by providing a means for the fast dissemination of information that was otherwise mediated by broadcast media, 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', facilitate protest, 'extend the range of local coverage to international broadcast networks' and as platform for contestation for the future of 'the future of civil society and information infrastructure' [HussainHoward].

Some of these examples go beyond the use of Internet protocols and flow over into the applications layer or examples in the offline world whereas the purpose of the following document is to break down the relationship between Internet protocols and the right to freedom of assembly and association. We do recognize however that in some cases the line between protocols, applications, implementations, policies, and the offline world are often blurry and hard (if not impossible) to differentiate, since protocols are a part of the socio-technical ordering of the world.

In draft-irtf-hrpc-research the relationship between human rights and Internet protocols has been shown, and guidelines for considerations of human rights impact in protocol design have been provided. Further research is needed to understand the exact impact of Internet protocols on human rights, including assembly and association given their importance for the Internet, in order to mitigate (potential) negative impacts. This is the aim of this document.

2. Vocabulary used

Anonymity The condition of an identity being unknown or concealed. [RFC4949]

Censorship resistance Methods and measures to mitigate Internet censorship.

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.

Pseudonymity The ability to disguise one's identity online with a different name than the "real" one, allowing for diverse degrees of disguised identity and privacy. It is strengthened when less personal data can be linked to the pseudonym; when the same pseudonym is used less often and across fewer contexts; and when independently chosen pseudonyms are more frequently used for new actions (making them, from an observer's or attacker's perspective, unlinkable)." [RFC6973]

3. Research questions

How does the internet architecture enables and/or inhibits freedom of association and assembly.

4. Cases and examples

Whereas rights to freedom of assembly and association protect collective expression, systems and protocols than enable comunal communication between people or between servers allow these rights to prosper. The Internet itself was originally designed as "a medium for communication for machines that share resources with each other as equals" [NelsonHedlun]. In this sense, decentralized architectures that protect anonimity and privacy, assure a resilient network of speakers and recipients or receivers and thus ensure better conditions for the exercise of such freedoms in the online environment. At the same time, centralized solutions have enabled people to group together in recognizable places and helped the visbility of groups. Here we will discuss different cases to bring out the affordances of different protocols, technologies and architectual features. This issue is particularly timely since an increasing trend of centralization and consolidation on the Internet can be observed. This is trend can be parallely observed on the application level, among Content Distribution Networks, hosting providers, as well as Internet access providers. Through the discussion of specific case we will try to further understand how this impact freedom of assembly, freedom of association as well as the distributed nature of the Internet [RFC1287].

4.1. Communicating

The ability to produce, receive and spread information is an essential pre-requisite for discussing and organizing. Protocols that enable private, open, collaborative and non-excluding communication models are the best fitted to foster and enable assembly and association rights.

4.1.1. Mailinglists

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. By this time, 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 discussion, share information, ask questions, and build ties. Even as social media and discussion forums grew, mailing lists continue to be widely used [AckermannKargerZhang]. They are a crucial tool to organise groups and individuals around themes and causes [APC].

4.1.2. Multi party video conferencing and risks

Multi party video conferencing protocols such as 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].

'The disclosure of network addresses presents a specific risk to individuals that use privacy tools to conceal their real IP address to sites that they visit. Typically, when a user browses the Internet over a VPN, the only address that should be recorded by sites they visit would be that of the VPN provider itself. Using the WebRTC STUN function allows a site to additionally enumerate the addresses that are associated with the computer that the visitor is using - rather than those of intermediaries. This means that if a user is browsing the Internet on an ADSL connection over a VPN, a malicious site they visit could potentially surreptitious record the home address of the user.' [AndersonGuarnieri].

While facilitating freedom of assembly and association multi party video conferencing tools might pose concrete risks for those who use them. One the one hand webRTC is providing a resilient channels of communications, but on the other hand it also exposed information about those who are using the tool which might lead to increased surveillance, identification and the consequences that might be derived from that. 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 made more clear to the user (or improved) which would result in a more secure and/or private excercise or the right of freedom of assembly or association.

4.2. Peer-to-peer networks and systems

4.2.1. Peer-to-peer system achitectures

Peer-to-peer (P2P) is esentially 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" and where each participating node typically acts both as a server and as a client [Vu]. In RFC 5694 it has been defined that peers or nodes 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 censorship, immune to single points of failure and have a higher performance and scalability. Nonetheless, in practice some P2P systems are supported by centralized servers and some others have hybrid models where nodes are organized into two layers: the upper tier servers and the lower tier common nodes [Vu].

Since the ARPANET project, the original idea behind the Internet was conceived as what we would now call a peer-to-peer system [RFC0001]. Over time it has increasingly shifted towards a client/server model with "millions of consumer clients communicating with a relatively priviledged set of servers" [NelsonHedlun]. Whether for resource sharing or data sharing, P2P systems are a form of enabling freedom of assembly and association. Not only they allow for effective dissemination of information, but they also because leverage computing resources by diminishing costs allowing for the formation of open collectives at the network level. At the same time, in completely descentralized systems the nodes are autonomous and can join or leave the network as they want also makes the system unpredicable: a resource might be only sometimes available, and some others it might be missing or incomplete [Vu]. Lack of information might in turn make association or assembly more difficult.

Additionally, when one architecturally asseses the role of P2P systems on can 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 ad- vantages 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 se- lected 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}}

4.2.2. Version control

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

In his book The Wealth of Networks, Benkler significantly expands on his definition of commons-based peer production. According to Benkler, 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.

Ever since developers needed to collaboratively write, maintain and discuss large code basis for the Internet there have been different approaches of doing so. One approach is discussing code through mailing lists, but this has proven to be hard in case of maintaining the most recent versions. There are many different versions and characteristics of version control systems.

4.3. Reaching out

4.3.1. Spam, filter bubbles, and unrequested messaging

In the 1990s as the internet became more and more commercial, spam came to be defined as irrelevant or unsolicited messages that were porsted many times to multiple news groups or mailing lists [Marcus]. Here the question of consent is 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 "comercial speech", thus encompassed by free expression rights [Marcus]. Nonetheless, 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.

This leaves us with an interesting case: spam is currently handled mostly by mailproviders on behalf of the user, next to that countries are increasingly adopting opt-in regimes for mailinglists and commercial e-mail, with a possibility of serious fines in case of violation.

This protects the user from being confronted with unwanted messages, but it also makes it legally and technically very difficult to communicate a message to someone who did not explicitly ask for this. In public offline spaces we regularly get exposed to flyers, invitations or demonstrations where our opinions get challenged, or we are invited to consider different viewpoints. There is no equivalent on the Internet with the technical and legal regime that currently operates in it. In other words, it is nearly impossible to provide information, in a proportionate manner, that someone is not explicility expecting or asking for. This reinforces a concept that is regularly discussed on the application level, called ’filter bubble’: "The proponents of personalization offer a vision of a custom-tailored world, every facet of which fits us perfectly. It’s a cozy place, populated by our favorite people and things and ideas." [Pariser]. "The filter bubble’s costs are both personal and cultural. There are direct consequences for those of us who use personalized filters. And then there are societal consequences, which emerge when masses of people begin to live a filter bubbled-life (...). Left to their own devices, personalization filters serve up a kind of invisible autopropaganda, indoctrinating us with our own ideas, amplifying our desire for things that are familiar and leaving us oblivious to the dangers lurking in the dark territory of the uknown." [Pariser]. It seem that the ’filter bubble’-effect can also be observed at the infrastructure level, which actually strenghtens the impact and thus hampers the effect of collective expression.

This could be interpretated as an argument for the injection of unrequested messages, spam or other unrequested notifications. But the big difference between the proliferation of such messages offline and online is the investment that is needed. It is not hard for a single person to message a lot of people, whereas if that person needed to go house by house the scale and impact of their actions would be much smaller.

4.3.2. Distributed Denial of Service Attacks

One of the most common examples of association at the infrastructure level are Distributed Denial of Service Attacks (DDoS) in which the infrastructure of the Internet is used to express discontent with a specific cause [Abibil] [GreenMovement]. Unfortunately DDoS are often used to stifle freedom of expression as they complicate the ability of independent media and human rights organizations to exercise their right to (online) freedom of association, while facilitating the ability of governments to censor dissent. This is one of the reasons protocols should seek to mitigate DDoS attacks [BCP72]. As described in draft-irtf-hrpc-research: "Uses of DDoS might or might not be legitimate for political reasons, but the IETF has no means or methods to assess this, and in general enabling DDoS would mean a deterioration of the network and thus freedom of expression". This is argued from the vector of freedom of expression, but if we would analyze it from the perspective of freedom of association the argument could be as follows: If the Internet is an association, any attack should be prevented and mitigated because it prevents the possibility of exercising a right to collective expression, which is consistent with [BCP72].

On the other hand, it must be taken into consideration that DDoS attacks are a form of forced assembly when done without the agreement -or even knowledge- of the involved parts. This point was also described in draft-irtf-hrpc-research: "When it comes to comparing DDoS attacks to protests in offline life, it is important to remember that only a limited number of DDoS attacks involved solely willing participants. In most cases, the clients are hacked computers of unrelated parties that have not consented to being part of a DDoS (for exceptions see Operation Abibil [Abibil] or the Iranian Green Movement DDoS [GreenMovement]).""

4.4. Grouping together (identities)

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

4.4.1. DNS

Domain names allow hosts to be identified by human parsable information. Whereas an IP address might not be the expression of an identity, a domain name can be, and often is. On the other hand the grouping of a certain identity under a specific domain, or even a Top Level Domain, also brings about risks because connecting an identity to a hierarchically structured identifier systems also bring risks about. Risks could be surveillance of the services running on the domain, domain based censorship, or impersonation of the domain through DNS cache poisoning. Several technologies have been developed in the IETF to mitigated these risks such as DNS over TLS [RFC7858], DNSSEC, and TLS.

The structuring of DNS as a hierarchical authority structure also brings about specific characteristic, namely the possibility of centralized policy making on the management and operation of domain names, which is what (in part) happens at ICANN. The impact of ICANN processes on human rights will not be discussed here.

4.4.2. ISPs

In order for edge-users to connect to the Internet, a user needs to be connected to a network. This means that in the process of accessing the Internet the edge-user needs to accept the policies and practices of the edge network that provides them access to the other networks. This means that in order to users to be able to join the assembly of a 'network of networks', they always need to connect through an intermediary.

While access the Internet through an intermediary, the user is forced to accept the policies, practices and principles of a network. This could impede the rights of the edge-user, depending on the implemented policies and practices on the network and how (if at all) they are communicated to the end-user. In terms of rights infringing habits one could think of filtering, blocking, extensive logging or other invasive practices that are not clearly communicated to the user.

In some cases it also means that there is no other way for the edge-user to connect to the network of networks, and is thus forced into accepting the policies of a specific network, because it is not trivial for an edge-user to operate its own Autonomous System. This design, combined with the increased importance of the Internet to make use of basic services, forces edge-user to engage in association with a specific network eventhough the user does not consent with the policies of the network.

5. Conclusions

- Internet has impact for on the ability for people to excercise their right to freedom of association and assembly.

- The Internet itself is a form of an associtation and assembly, and should thus be protected.

- To get access to the Internet one could argued on is caught in a forced assembly with the access network.

- It need to be further researched which level of the network is responsible for these impacts, and considerations could be developed for this.

6. Acknowledgements

7. Security Considerations

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

8. IANA Considerations

This document has no actions for IANA.

9. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research Group is located at the e-mail address hrpc@ietf.org [1]. 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

10. References

10.1. Informative References

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

[Abibil] Danchev, D., "Dissecting ’Operation Ababil’ - an OSINT Analysis", 2012, <http://ddanchev.blogspot.be/2012/09/dissecting-operation-ababil-osint.html>.

[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>.

[ARTICLE19] ARTICLE 19, "The Right to Protest Principles: Background Paper", 2016, <https://www.article19.org/data/files/medialibrary/38581/Protest-Background-paper-Final-April-2016.pdf page 7>.

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

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

[GreenMovement]
Villeneuve, N., "Iran DDoS", 2009, <https://www.nartv.org/2009/06/16/iran-ddos/>.

[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>.

[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", 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[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>.

[Melucci] Melucci, A., "The Process of Collective Identity", Temple University Press, Philadelphia , 1995.

[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>.

[OSCE] OSCE Office for Democratic Institutions and Human Rights, "Guidelines on Freedom of Peaceful Assembly", page 24 , 2010, <https://www.osce.org/odihr/73405?download=true>.

[Pariser] Pariser, E., "The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think", Peguin Books, London. , 2012.

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

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

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

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

[RFC1287] Clark, D., Chapin, L., Cerf, V., Braden, R., and R. Hobby, "Towards the Future Internet Architecture", RFC 1287, DOI 10.17487/RFC1287, December 1991, <http://www.rfc-editor.org/info/rfc1287>.

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

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

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

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

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

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[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, <http://www.rfc-editor.org/info/rfc7118>.

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

[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>.

[Tocqueville] de Tocqueville, A., "Democracy in America", n.d., <http://classiques.uqac.ca/classiques/De_tocqueville_alexis/democracy_in_america_historical_critical_ed/democracy_in_america_vol_2.pdf p. 304>.

[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>.

[UNHRC] 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>.

[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>.

10.2. URIs

[1] mailto:hrpc@ietf.org

Authors' Addresses

Niels ten Oever
ARTICLE 19

EMail: niels@article19.org

Gisela Perez de Acha
Derechos Digitales

EMail: gisela@derechosdigitales.org