Freedom of Association on the Internet
draft-tenoever-hrpc-association-05

Abstract

   This document scopes the relation between Internet protocols and the
   right to freedom of assembly and association. Increasingly, the
   Internet mediates our lives, our relationships and our ability to
   exercise our human rights. The Internet provides a global public
   space, but one that is built predominantly on private infrastructure.
   Since Internet protocols play a central role in the management,
   development and use of the Internet, the relation between protocols
   and the aforementioned rights should be documented and any adverse
   impacts of this relation should be mitigated.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

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

   The Internet is a technology which shapes modern information
   societies. The ordering that the Internet provides is socio-
   technical, in other words, the Internet infrastructure and
   architecture consists of social and technological arrangements
   [StarRuhleder]. This ordering is not always apparent because
   infrastructure also tends to hide itself in the societal woodwork
   [Mosco], or with [Weiser]: 'The most profound technologies are those
   that disappear'. Next to that infrastructure is often taken for

granted by those using it. Infrastructure therefore is mostly known
by an epistemic community of experts [Haas] and only get recognized
by the larger public when it fails. With the increasing societal use
of the Internet the importance of the Internet is growing, and the
decisions made about its infrastructure and architecture therefore
also become more important. [RFC8280] established the relationship
between human rights and Internet protocols, and in this document we
seek to uncover the relation between two specific human rights and
the Internet infrastructure and architecture.

The rights to freedom of assembly and association protect collective
expression, in turn, systems and protocols that enable communal
communication between people and servers allow these rights to
prosper. The Internet itself was originally designed as "a medium of
communication for machines that share resources with each other as
equals" [NelsonHedlun], the Internet thus forms a basic
infrastructure for the right freedom of assembly and association.

The manner in which communication is designed and implemented impacts
the ways in which rights can be excercised. For instance a
decentralized and resilient architecture that protects anonymity and
privacy, offers a strong protection 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. In other words, different
architectural designs come with different affordances, or
characteristics. These characteristics should be taken into account
at the time of design, and when designing, updating and maintaining
other parts of the architecture and infrastructure.

This draft continues the work started in [RFC8280] by investigating
the exact impact of Internet protocols on specific human rights,
namely the right to freedom of assembly and association given their
importance for the Internet, in order to mitigate (potential)
negative impacts.

2. Vocabulary used

Architecture   The design of a structure

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

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

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

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.

3. Research questions

1. How does the internet architecture enable and/or inhibit freedom
    of association and assembly?

2. If the Internet is used to exercise the right to freedom of
    association, what are the implications for its architecture and
    infrastructure?

4. Methodology

In order to answer the research questions, first a number of cases
have been collected to analyze where Internet infrastructure and
protocols have either enabled or inhibited groups of people to
collaborate, cooperate or communicate. This overview does not aim to
cover all possible ways in which people can collectively organize or
reach out to each other using Internet infrastructure and Internet
protocols, but rather cover typical uses in an attempt at an an
ethnography of infrastructure [Star]. Subsequently we analyze the
cases with the theoretical framework provided in the literature
review and provide recommendations based on the findings.

5. Literature Review

The rights to freedom of assembly and association protects and
enables collective action and expression [UDHR] [ICCPR]. These
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 with political
leaders or governments [OSCE]. This is relevant because in the
process of democratic delibration, causes and opinions are more
widely heard when a group of people come together behind the same
cause or issue [Tocqueville].

In international law, the rights to freedom of assembly and
association protect any collective, gathered either permanently or
temporarily for "peaceful" purposes. It is important to underline
the property of "freedom" because the right to freedom of association
and assembly are 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.

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,
indoor meetings, strikes, processions, rallies or even sits-in
[UNHRC]. 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.

The right to freedom of assembly and association is quintessential
for the Internet, even if privacy and freedom of expression are the
most discussed human rights when it comes to the online world.
Online association and assembly are 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 and the #WomensMarch- 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, extend the range
of local coverage to international broadcast networks" and as
platform for contestation for "the future of civil society and
information infrastructure" [HussainHoward].

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

We are aware that some of 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. Nonetheless,
given that protocols are a part of the socio-technical ordering of
reality, we do recognize that in some cases the line between them and
applications, implementations, policies and offline realities are
often blurred and hard (if not impossible) to differentiate.

[6]. Cases and examples

   The Internet has become a central mediator for collective action and
   collaboration. This means the Internet has become a strong enabler
   of the rights to freedom of association and assembly.

   Here we will discuss different cases to give an overview of how the
   Internet protocol and architecture facilitates the freedom of
   assembly and association.

[6.1]. Conversing

   An interactive conversation between two or more people forms the
   basis for people to organize and associate. According to Anderson
   "the relationship between political conversation and engagement in
   the democratic process is strong." [Anderson]. By this definition,
   what defines the "political" is essentially assembly or association:
   a basis for the development of social cohesion in society.

[6.1.1]. Mailing Lists

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

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

   Mailinglist are still in wide use, also in the IETF because they
   allow for easy association and allow people to subscribe (join) and
   unsubscribe (leave) as they please. They also allow for association
   of specific groups on closed lists. Finally the archival function
   allows for accountabilty. The downsides of mailinglists are similar
   to the ones generally associated with e-mail, except that end-to-end
   encryption such as OpenPGP [RFC4880] and S/MIME [RFC5751] is not
   possible because the final recipients are not known. There have been
   experimental solutions to address this issue such as Schleuder
   [Schleuder], but this has not been standardized or widely deployed.

6.1.2. Multi-party video conferencing

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].

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 resilient channels of
communications, but on the other hand it also exposes information
about those who are using the tool which might lead to increased
surveillance, identification and the consequences that might be
derived from that. This is especially concerning because the usage
of a VPN does not protect against the exposure of IP addresses
[Crawford].

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

6.1.3. Internet Relay Chat

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

For order to be kept within the IRC network, special clases of users
become "operators" and are allowed to perform general maintenance
functions on the network: basic network tasks such as disconnecting
(temporary or permanently) and reconnecting servers as needed
[RFC2812]. One of the most controversial power of operators is the

ability to remove a user from the connected network by 'force', i.e.,
operators are able to close the connection between any client and
server [RFC2812].

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

6.2. Peer-to-peer networks and systems

At the organizational level, peer production is one of the most
relevant innovations from Internet mediated social practices.
According to [Benkler], 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." [Benkler] To ensure
that the knowledge generated is available for free use, commons-based
projects are often shared under an open license.

6.2.1. Peer-to-peer system 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 P2P has been defined as peers or nodes
that should be able to communicate directly between themselves
without passing intermediaries, and that the system should be self-
organizing and have decentralized control [RFC5694]. With this in
mind, the ultimate model of P2P is a completely decentralized system,
which is more resistant to speech regulation, immune to single points
of failure and 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
privileged set of servers" [NelsonHedlun].

Whether for resource sharing or data sharing, P2P systems are
enabling freedom of assembly and association. Not only do they allow
for effective dissemination of information, but because they leverage
computing resources by diminishing costs allowing for the formation
of open collectives at the network level. At the same time, in
completely decentralized systems the nodes are autonomous and can
join or leave the network as they want, which also makes the system
unpredicable: 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.

Additionally, when one architecturally asseses the role of P2P
systems one 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 advantage of
both centralized and decentralized architectures. Basically, to
maintain the scalability, similar to decentralized P2P systems, there
are no servers in hybrid P2P systems. However, peer nodes that are
more powerful than others can be selected to act as servers to serve
others. These nodes are often called super peers. In this way,
resource locating can be done by both decentralized search techniques
and centralized search techniques (asking super peers), and hence the
systems benefit from the search techniques of centralized P2P
systems." [Vu]

[6.2.2](). **Version control**

   Ever since developers needed to collaboratively write, maintain and
   discuss large code basis for the Internet there have been different
   approaches of doing so. 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.

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

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

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

[6.3](). **Grouping together (identities)**

   Collective identities are also protected by freedom of association
   and assembly. 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]()].

6.3.1. DNS

Domain names allow hosts to be identified by human parsable
information. Whereas an IP address might not be the expression of an
identity, a domain name can be, and often is. On the other hand the
grouping of a certain identity under a specific domain or even a Top
Level Domain brings about risks because connecting an identity to a
hierarchically structured identifier systems creates a central attack
surface. Some of these risks are the surveillance of the services
running on the domain, domain based censorship [RFC7754], 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 [RFC4033], and TLS [RFC5246].
These mitigations would, when implemented, not make censorship
impossible, but rather make it visible. The use of a centralized
authority always makes censorship through a registry or registrar
possible, as well as by using a fake resolver or using proposed
standards such as DNS Response Policy Zones [RPZ].

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

6.3.2. Autonomous Systems

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

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

In 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 an AS and engage in peering

relation with other ASes. 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 to the policies of the network.

It can be noted also that there is no standard and deployed way for
the edge-user to choose the routes her packets will go through.
[RFC0791], section 3.1, standardized "source routing" but it was
never deployed, mostly because of serious security issues. There is
not even a way for the edge-user to know about the routes that
packets have actually taken, and which ASes a packet has traversed.
[RFC0791], section 3.1, standardized "record route" but it was never
deployed. In practice, the user must accept policies of ASes he has
no relationship with, and didn't choose. For instance, there is no
way to direct the packets to avoid the Five Eyes, not even to know
after the fact where the packet went. [FiveEyes] [SchengenRouting]
(Traceroutes give you an idea but the path may change before and
after the traceroute.)

7. Discussion: Protocols vs Platforms

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

Often these non-interoperable platforms are built on open-protocols
but do not allow for inter-operability or data-portability. In the
case of these large platforms this leads to strong network
externalities, also know as a network effect; because the users are
there, users will be there. The use of social-media platforms has
enabled groups to associate, but is has also led to a 'tactical
freeze' because of the inability to change the platforms [Tufekci].
Whereas these networks are a ready-to-hand networked public sphere,
they do not allow their inhabitants to change, or fully understand,
their workings.

This potentially has a significant impact on the distributed nature
of the Internet [RFC1287].

8. Conclusions

   This document scopes the relation between Internet protocols and the
   right to freedom of assembly and association. For this reason, the
   current research started out with two main questions. First, how
   does the internet architecture enable and/or inhibit freedom of
   association and assembly? And secondly: if the Internet is used to
   exercise the right to freedom of association, what are the
   implications for its architecture and infrastructure?

   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].
   Taking legal definitions given in international human rights law
   jurisprudence, we could assert that the right to freedom of assembly
   and association protect collective expression. These rights protect
   any collective, gathered either permanently or temporarily for
   "peaceful" purposes. It is voluntary and uncoerced.

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

   Regarding the second question, after reviewing protocols that allow
   mailing lists, to multi-party video conferencing, IRC, peer-to-peer
   architectures, version control or the functioning of autonomous
   systems, we can conclude that the way in which infrastructure is
   designed and implemented impacts the exercise of freedom of assembly
   and association. This is because different architectural designs
   come with different affordances, or characteristics. If a
   decentralized architecture protects anonymity and privacy, both
   freedoms in the online environment will be enabled. On the other
   hand, centralized solutions have allowed users to group together and
   visibilise groups. enabled people to group together in recognizable
   places and helped the visbility of groups.

   Lastly, the increasing shift towards closed and non-interoperable
   platforms in chat and social media networks have a significant impact
   on the distributed and open nature of the Internet. Often these non-
   interoperable platforms are built on open-protocols but do not allow
   for inter-operability or data-portability. The use of social-media
   platforms has enabled groups to associate, but is has also rendered

users unable to change platforms, therefore leading to a sort of
"forced association" that stirs faraway from freedom.

9. Acknowledgements

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

- Stephane Bortzmeyer for several concrete text suggestions that
  found their way in this document (such as the AS filtering
  example)

- Mark Perkins for finding a lot of typos

- the hrpc mailinglist at large for a very constructive discussion
  on a hard topic.

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 [1].
Information on the group and information on how to subscribe to the
list is at https://www.irtf.org/mailman/listinfo/hrpc [2]

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

13. References

13.1. Informative References

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

[AckermannKargerZhang]
           Ackerman, M., Karger, D., and A. Zhang, "Mailing Lists:
           Why Are They Still Here, What's Wrong With Them, and How
           Can We Fix Them?", Mit. edu (2017): 1. , 2017,
           <https://people.csail.mit.edu/axz/papers/
           mailinglists.pdf>.

[Anderson]
           Andersson, E., "The political voice of young citizens
           Educational conditions for political conversation - school
           and social media", Utbildning & Demokrati: Tidskrift foer
           Didaktik och Utbildningspolitik, Volume 21, Number 1,
           2012, pp. 97-119(23) , 2012,
           <http://www.ingentaconnect.com/content/
           doaj/11026472/2012/00000021/00000001/art00006>.

[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>.

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

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

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

[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/>.

[FiveEyes]
          Wikipedia, ., "Five Eyes", 2018,
          <https://en.wikipedia.org/wiki/Five_Eyes>.

[GithubIETF]
          Thomson, M. and A. Atlas, "Using GitHub at the IETF",
          2017.

[Haas]   Haas, P., "Introduction: epistemic communities and
          international policy coordination", International
          Organization, special issue: Knowledge, Power, and
          International Policy Coordination, Cambridge Journals. 46
          (1): 1-35. , 1992.

[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", 1966,
          <http://www.ohchr.org/EN/ProfessionalInterest/Pages/
          CCPR.aspx>.

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

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

[Mosco]   Mosco, V., "The Digital Sublime: Myth, Power, and
          Cyberspace", 2005,
          <https://mitpress.mit.edu/books/digital-sublime>.

[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>.

[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/info/rfc1>.

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

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791,
          DOI 10.17487/RFC0791, September 1981,
          <https://www.rfc-editor.org/info/rfc791>.

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

[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,
          <https://www.rfc-editor.org/info/rfc1287>.

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

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

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

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

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

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

   [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "DNS Security Introduction and Requirements",
              RFC 4033, DOI 10.17487/RFC4033, March 2005,
              <https://www.rfc-editor.org/info/rfc4033>.

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

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

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

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246,
              DOI 10.17487/RFC5246, August 2008,
              <https://www.rfc-editor.org/info/rfc5246>.

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

   [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet
              Mail Extensions (S/MIME) Version 3.2 Message
              Specification", RFC 5751, DOI 10.17487/RFC5751, January
              2010, <https://www.rfc-editor.org/info/rfc5751>.

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

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

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

   [RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E.
              Nordmark, "Technical Considerations for Internet Service
              Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754,
              March 2016, <https://www.rfc-editor.org/info/rfc7754>.

   [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, <https://www.rfc-editor.org/info/rfc7858>.

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

   [RPZ]   Vixie, P. and V. Schyver, "DNS Response Policy Zones
              (RPZ)", 2017,
              <https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00>.

   [SchengenRouting]
              Wikipedia, ., "Schengen Routing", 2018,
              <https://en.wikipedia.org/wiki/Schengen_Routing>.

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

   [Sink]   Sink, E., "Version Control by Example", 2011,
              <http://ericsink.com/vcbe/>.

   [Star]   Star, S., "The Ethnography of Infrastructure", American
              Behavioral Scientist, Volume 43 (3), 377-391. , 1999,
              <http://journals.sagepub.com/doi/
              abs/10.1177/00027649921955326>.

   [StarRuhleder]
              Star, S. and K. Ruhleder, "Steps toward an ecology of
              infrastructure: Design and access for large information
              spaces", Information Systems Research 7 (1) (1996)
              111-134. , 1996.

   [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", 1840, <http://
              classiques.uqac.ca/classiques/De_tocqueville_alexis/
              democracy_in_america_historical_critical_ed/
              democracy_in_america_vol_2.pdf p. 304>.

   [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>.

   [Tufekci] Tufekci, Z., "Twitter and Tear Gas: The Power and
              Fragility of Networked Protest", 2017,
              <https://www.twitterandteargas.org/>.

   [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>.

     [Weiser]   Weiser, L., "The Computer for the 21st Century",
                 Scientific American Ubicomp Paper after Sci Am editing ,
                 1991, <https://web.archive.org/web/20141022035044/
                 http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>.

     [Wugh]   Nottingham, M., "Using Third Party Services for IETF
                 Work", 2017, <https://datatracker.ietf.org/doc/
                 draft-nottingham-wugh-services/>.

13.2. URIs

   [1] mailto:hrpc@ietf.org

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

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

Authors' Addresses

   Niels ten Oever
   University of Amsterdam

   EMail: mail@nielstenoever.net

   Gisela Perez de Acha
   Derechos Digitales

   EMail: gisela@derechosdigitales.org