Human Rights Protocol Considerations Research Group D. Gillmor
Internet-Draft ACLU
Intended status: Informational N. ten Oever
Expires: April 18, 2016 Article19
A. Doria
APC
October 16, 2015

Human Rights Protocol Considerations Glossary
draft-dkg-hrpc-glossary-01

Abstract

This document presents a glossary of terms used to map between concepts common in human rights discussions and engineering discussions. It is intended to facilitate work by the proposed Human Rights Protocol Considerations research group, as well as other authors within the IETF.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on April 18, 2016.

Table of Contents

1. Introduction

"There’s a freedom about the Internet: As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere."

[Berners-Lee]

The Human Rights Protocol Consideration Proposed Research Group aims to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights [UDHR] and the International Covenant ons Civil and Political Rights [ICCPR], specifically, but not limited to the right to freedom of expression and the right to freedom of assembly.

Comunications between people working on human rights and engineers working on Internet protocols can be improved with a shared vocabulary.

This document aims to provide a shared vocabulary to facilitate understanding of the intersection between human rights and Internet protocol design.

Discussion on this draft at: hrpc@irtf.org // https://www.irtf.org/mailman/admindb/hrpc

This document builds on the previous IDs published within the framework of the proposed hrpc research group [ID]

2. Glossary

In the analysis of existing RFCs central design and technical concepts have been found which impact human rights. This is an initial glossary of concepts that could bridge human rights discourse and technical vocabulary. These definitions should be improved and further aligned with existing RFCs.

Accessibility Full Internet Connectivity as described in [RFC4084] to provide unfettered access to the Internet

The design of protocols, services or implementation that provide an enabling environment for people with disabilities.

The ability to receive information available on the Internet

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

Anonymous A state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals (the anonymity set). [RFC6973]

Authenticity The act of confirming the truth of an attribute of a single piece of data or entity.

Censorship resistance Methods and measures to prevent Internet censorship.

Confidentiality The non-disclosure of information to any unintended person or host or party

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].

Content-agnosticism Treating network traffic identically regardless of content.

Debugging Debugging is a methodical process of finding and reducing the number of bugs, or defects, or malfunctions in a protocol or its implementation, thus making it behave as expected and analyse the consequences that might have emanated from the error. Debugging tends to be harder when various subsystems are tightly coupled, as changes in one may cause bugs to emerge in another. [WP-Debugging]

The process through which people troubleshoot a technical issue, which may include inspection of program source code or device configurations. Can also include tracing or monitoring packet flow.

Decentralized Opportunity for implementation or deployment of standards, protocols or systems without one single point of control.

End-to-End The principal of extending characteristics of a protocol or system as far as possible within the system. For example, end-to-end instant message encryption would conceal communications from one user's instant messaging application through any intermediate devices and servers all the way to the recipient's instant messaging application. If the message was decrypted at any intermediate point-for example at a service provider-then the property of end-to-end encryption would not be present.

One of the key architectural guidelines of the Internet is the end-to-end principle in the papers by Saltzer, Reed, and Clark [Saltzer] [Clark]. The end-to-end principle was originally articulated as a question of where best not to put functions in a communication system. Yet, in the ensuing years, it has evolved to address concerns of maintaining openness, increasing reliability and robustness, and preserving the properties of user choice and ease of new service development as discussed by Blumenthal and Clark in [Blumenthal]; concerns that were not part of the original articulation of the end-to-end principle. [RFC3724]

communication that takes place between communication end-points of the same physical or logical functional level

Federation The possibility of connecting autonomous systems into a single distributed system.

Heterogenity The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and internet service providers, each with their own separate policy concerns, there is a large heterogeneity of administrative domains and pricing structures. As a result, heterogeneity principle is proposed in [RFC1958] to be supported by design. [FIArch]

Integrity Maintenance and assurance of the accuracy and consistency of data to ensure it has not been (intentionally or unintentionally) altered

Internet censorship Internet censorship is the intentional suppression of information originating, flowing or stored on systems connected to the Internet where that information is relevant for decision making to some entity. [Elahi]

Inter-operable A property of a documented standard or protocol which allows different independent implementations to work with each other without any restricted negotiation, access or functionality.

Internet Standards as an Arena for Conflict Pursuant to the principle of constant change, since the function and scope of the Internet evolves, so does the role of the IETF in developing standards. Internet standards are adopted on the basis of a series of criteria, including high technical quality, support by community consensus, and their overall benefit to the Internet. The latter calls for an assessment of the interests of all affected parties and the specifications' impact on the Internet's users. In this respect, the effective exercise of the human rights of the Internet users is a relevant consideration that needs to be appreciated in the standardization process insofar as it is directly linked to the reliability and core values of the Internet. [RFC1958] [RFC0226] [RFC3724]

Internationalization (i13n) The practice of the adaptation and facilitation of protocols, standards, and implementation to different languages and scripts.

Open standards Conform [RFC2606]: Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be "open external standards" for the purposes of the Internet Standards Process.

Openness The quality of the unfiltered Internet that allows for free access to other hosts

Permissionless innovation The freedom and ability of to freely create and deploy new protocols on top of the communications constructs that currently exist

Privacy The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. [RFC4949]

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including government, companies and private individuals. It is often summarized as "the right to be left alone" but it encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognized as a core right that underpins human dignity and other values such as freedom of association and freedom of speech.

The right to privacy is also recognized in nearly every national constitution and in most international human rights treaties. It has been adjudicated upon both by international and regional bodies. The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.

Reliable Reliability ensures that a protocol will execute its function consistently and error resistant as described and function without unexpected result. A system that is reliable degenerates gracefully and will have a documented way to announce degradation. It also has mechanisms to recover from failure gracefully, and if applicable, allow for partial healing.

Resilience The maintaining of dependability and performance in the face of unanticipated changes and circumstances.

Robustness The resistance of protocols and their implementations to errors, and to involuntary, legal or malicious attempts to disrupt its mode of operations. [RFC0760] [RFC0791] [RFC0793] [RFC1122]

Scalable The ability to handle increased or decreased workloads predictably within defined expectations. There should be a clear definition of its scope and applicability. The limits of a systems scalability should be defined.

Stateless / stateful In computing, a stateless protocol is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and

response. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. In contrast, a protocol which requires keeping of the internal state on the server is known as a stateful protocol. [WP-Stateless]

Strong encryption / cryptography Used to describe a cryptographic algorithm that would require a large amount of computational power to defeat it. [RFC4949]

Transparent: "transparency" refers to the original Internet concept of a single universal logical addressing scheme, and the mechanisms by which packets may flow from source to destination essentially unaltered. [RFC2775]

The combination of reliability, confidentiality, integrity, anonymity, and authenticity is what makes up security on the Internet

```
 ( Reliability    )
(  Confidentiality )
(  Integrity       ) =  communication and information
(  Authenticity    )                 security (technical)
 ( Anonymity      )
```

The combination of End-to-End, Interoperability, resilience, reliability and robustness is what makes us connectivity on the Internet

```
                     ( End-to-End      )
 connectivity =     (  Interoperability )
                   (   Resilience        )
                   (   Reliability       )
                   (   Robustness        )
                    (  Autonomy         )
                     ( Simplicity      )
```

3. Security Considerations

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

4. IANA Considerations

This document has no actions for IANA.

5. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working 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

6. References

6.1. Informative References

[Berners-Lee] Berners-Lee, T. and M. Fischetti, "Weaving the Web,", HarperCollins p 208, 1999.

[Blumenthal] Blumenthal, M. and D. Clark, "Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world", ACM Transactions on Internet Technology, Vol. 1, No. 1, August 2001, pp 70-109. , 2001.

[Clark] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", Proc SIGCOMM 88, ACM CCR Vol 18, Number 4, August 1988, pp. 106-114. , 1988.

[Elahi] Elahi, T. and I. Goldberg, "CORDON - A taxonomy of Internet Censorship Resistance Strategies", 2012, <http://cacr.uwaterloo.ca/techreports/2012/cacr2012-33.pdf>.

[FIArch] "Future Internet Design Principles", January 2012, <http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", 1976, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[ID] ten Oever, N., Doria, A., and J. Varon, "Proposal for research on human rights protocol considerations", 2015, <http://tools.ietf.org/html/draft-doria-hrpc-proposal>.

[RFC0226] Karp, P., "Standardization of host mnemonics", RFC 226, DOI 10.17487/RFC0226, September 1971, <http://www.rfc-editor.org/info/rfc226>.

[RFC0760] Postel, J., "DoD standard Internet Protocol", RFC 760, DOI 10.17487/RFC0760, January 1980, <http://www.rfc-editor.org/info/rfc760>.

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

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

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

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <http://www.rfc-editor.org/info/rfc2606>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <http://www.rfc-editor.org/info/rfc2775>.

[RFC3724] Kempf, J., Austein., R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <http://www.rfc-editor.org/info/rfc3724>.

[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>.

[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>.

[Saltzer] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design", ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288. , 1984.

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

[WP-Debugging] "Debugging", n.d., <https://en.wikipedia.org/wiki/Debugging>.

[WP-Stateless] "Stateless protocol", n.d., <https://en.wikipedia.org/wiki/Stateless_protocol>.

6.2. URIs

[1] mailto:hrpc@ietf.org

Authors' Addresses

Daniel Kahn Gillmor
ACLU

EMail: dkg@fifthhorseman.net

Niels ten Oever
Article19

EMail: niels@article19.org

Avri Doria
APC

EMail: avri@apc.org

Human Rights Protocol Consideration RG
Internet-Draft
Intended status: Informational
Expires: April 20, 2016

A. Doria (ed)
Technicalities

October 18, 2015

Human Rights Protocol Considerations - Report
draft-doria-hrpc-report-00

Abstract

This document present an overview of the project to map engineering concepts at the protocol level that may be related to promotion and protection of the freedom of expression and association.

This first draft is intended to provide the framework for reporting on the study, initial results and basic considerations. At a later stage it will fold in the work being done in the Methodology and Glossary drafts as well as the work being done in the case studies. It also folds in some of the text included in the original proposal for the HRPC.

Discussion on this draft at: hrpc@irtf.org // https://www.irtf.org/mailman/admindb/hrpc

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on April 20, 2016.

Copyright Notice

Table of Contents

1. Background

The recognition that human rights have a role in Internet policies has become part of the general discourse. Several reports from former United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, have made such relation explicit, which lead to the approval of the landmark resolution "on the promotion, protection and enjoyment of human rights on the Internet" at the UN Human Rights Council (HRC). And, more recently, to the resolution "The right to privacy in the digital age" at the UN General Assembly. The NETmundial outcome document affirms that human rights, as reflected in the Universal Declaration of Human Rights [UDHR], should underpin Internet governance principles. Recently the UNESCO report:

Keystones to foster inclusive Knowledge Societies [UNESCO] focused on the importance of developing the Internet on the basis of human rights principles.

Nevertheless, the direct relation between Internet Standards and human rights is still something to be explored and more clearly demonstrated.

Concerns for freedom of expression and association were a strong part of the world-view of the community involved in developing the first Internet protocols. Apparently, by intention or by coincidence, the Internet was designed with freedom and openness of communications as core values. But as the scale and the commercialization of the Internet has grown, the influence of such world-views had to compete with other values, such as ease of development and cost. The purpose of this research is to discover and document the consideration involved in taking human rights into account when creating protocols.

In a manner similar to the work done for RFC 6973 [RFC6973] on Privacy Consideration Guidelines, the premise of this research is that some standards and protocols can solidify, enable or threaten human rights.

As stated in RFC 1958 [RFC1958], the Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. Open, secure and reliable connectivity is essential for rights such as freedom of expression and freedom of association, as defined in the Universal Declaration of Human Rights [UDHR]. Therefore, considering connectivity as the ultimate objective of the Internet, this makes a clear case that the Internet is not only an enabler of human rights, but that human rights lie at the basis of, and are ingrained in, the architecture of the network.

An essential part of maintaining the Internet as a tool for communication and connectivity is security. Indeed, "development of security mechanisms is seen as a key factor in the future growth of the Internet as a motor for international commerce and communication" RFC 1984 [RFC1984] and according to the Danvers Doctrine RFC 3365 [RFC3365], there is an overwhelming consensus in the IETF that the best security should be used and standardized.

In RFC 1984 [RFC1984], the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, expressed: "concern by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy." Indeed, the IETF has been

doing a significant job in this area [RFC6973] [RFC7258], considering privacy concerns as a subset of security concerns. [RFC6973]

Besides privacy, it should be possible to highlight other aspects of connectivity embedded in standards and protocols that can have human rights considerations. This report focuses on freedom of expression and the right to association and assembly online.

2. Terminology

Currently defined in draft-dkg-hrpc-glossary to be folded in at appropriate time.

3. Link between protocols and human rights

- Include discussion of value laden engineering as discussed in [Cath].

This work discusses four basic architectural principles that are encoded in Internet Technology:

- Openness, Permissionless Innovation, and Content Agnosticism
- Interoperability
- Redundancy and the Distributed Architecture
- The End-to-End Principle

The work by Cath explores the relationship of the architectural principles to the human right of freedom of expression and asks whether the IETF has an repsonsiblity toward human rights. The fact that there is documentation of normative principles among the body of work of the IETF, is an indication that ethics are sometimes seen as within the purview of IETF consideraitons. The research question asked by the work is:

> "Should the right to freedom of speech be instantiated in the protocls and standards of the Internet Engineering Task Force?"

Becasue of the threat of fragmentation by countries that do not accept human rights, the answer given to the research question is negative: human rights should not be instantiated in the Interent in order to avoid fragmentation. Care must be taken to avoid making the protocols political targets. On the other hand the principles that are encoded in the Internet do make it better at enabling rights. This encourages work such as the work done for privacy considerations

in the IETF and the research being done on protocol consideration for the freedoms of expression and association.

- Include discussion of "Values and Networks" work by Roland Bless

tbd

- Include discussion of principles from NetMundial Multistakeholder Statement

tbd

3.1. Discussion of Universal Declaration of Human Rights (UDHR) and Internet Architecture

This project is focused on two rights defined in the UDHR [UDHR], Article 19 on Freedom of Expression and Article 20 of Freedom of Association.

Article 19 Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20 1 Everyone has the right to freedom of peaceful assembly and association.

2 No one may be compelled to belong to an association.

3.2. Theory

When looking at protocols the considerations can apply from several perspectives.

- The protocol’s direct effects on human rights on the Internet.

- The protocol’s direct effect on human rights in combination with other protocols

- The effect of specific protocol elements, separately or in combination with other protocol elements on human rights on the Internet

- The ability to determine when various effects are occurring, i.e. transparency

- The effect of deployment or non deployment. While this may be may seem beyond the protocol itself, often the design of protocol, its

difficulty in implementation and the degree to which it contains required elements, poison pills or other protocol artifacts that either encourage or discourse implementation or deployment can be significant in the overall human rights affect of a protocol.

3.3. Other relevant research

TBD : Look at, and summarize some of the academic research on the topic including Ian Brown [Brown], Laura Denardis [Denardis], David Post [Post], Jonathan Zittrain [Zittrain] among others.

4. Methodology

Currently defined in detail in draft-varon-hrpc-methodolgy to be folded in at appropriate time. this will largely be a reproduction of Section 3 of that document that focuses on the methodology

Briefly methodology has included:

- scoping the research problem
- determining terminology to be use linking engineering and human rights concepts
- establishing methodology
- case studies on a set of protocols
- derivation of possible considerations

5. Case Studies

In each of the case studies, the behavior of the protocols is analysed for its positive and negative effects. In some case these effects are due to the design of the protocol itself, in others they are due to existing or absent features.

Early versions of the analysis on the following protocols are currently being discussed on HRPC list. Once the discussions have matured those discussions will be folded in this section.

5.1. DNS

Text being done by Will Scott on the HRPC list, current snapshot included in [HRPC-Method].

5.2. IP

Text being done by Will Scott on HRPC list, current snapshot included in [HRPC-Method].

5.3. HTTP

Text being done by Nex / Claudio on HRPC list, current snapshot included in [HRPC-Method].

5.4. XMPP

Text being done by Will Scott on HRPC list, current snapshot included in [HRPC-Method].

5.5. P2P

Text being done by Nex on HRPC List, current snapshot included in [HRPC-Method].

6. Possible areas for protocol considerations

The case studies point to several areas of protocol behavior that may be appropriate for considerations:

- Character encoding for internationalization
- DNS Record
  - Distortion
  - Injection
  - Removal
- Network Poisoning
- Traffic
  - Interception
  - Manipulation
  - Throttling
- User Identification
  - Source and Destination visibility

- Tracking

Additionally, discussion of the rights themselves and the evidence of these rights being implicit in the IETF design principles [Clark] and in some of the existing architecture and protocols, [Cath] and [Liddicoat] suggest other considerations. [Cath] recommends that adhereing to the four fundamental architectural principles discussed above is a first step.

7. Next Steps

Once the first take at consideration are defined, what are the next steps for creating something that can be useabble for protocol designers and implementers in considering the human rights of freedom of expression and freedom of association in their work.

8. Acknowledgement

tbd : A section that includes mention the many contributors of text as well as commenters and those who are assisitng this project in existing.

9. IANA considerations

There shouldn’t be any.

10. Security Considerations

There shouldn’t be any.

11. Informative References

[Blumenthal] Blumenthal, M. and D. Clark, "Rethinking the design of the Internet The end-to-end arguments vs. the brave new world", ACM Transactions on Internet Technology, Vol. 1, No. 1, August 2001, pp 70-109. , 2001.

[Brown] Brown, I. and C. Marsden, "Regulating Code Good Governance and Better Regulation in the Information Age", 2013.

[Cath] Cath, C., "A case study of codeing rights", 2015.

[Clark] Clark, D., "The Design Philosophy of the DARPA Internet Protocols", Proc SIGCOMM 88, ACM CCR Vol 18, Number 4, August 1988, pp. 106-114. , 1988.

[Denardis]
Denardis, L., "Protocol Politics", 2013.

[Galloway]
Alexander Galloway, ., "Protocol", 2006.

[HRPC-GLOSSARY]
ten Oever, N., Doria, A., and D. Gillmor, "Human Rights Protocol Considerations Glossary", 2015, <https://www.ietf.org/id/draft-dkg-hrpc-glossary-00.txt>.

[HRPC-Method]
Varon, J. and C. Cath, "Human Rights Protocol Considerations Methodology", 2015, <https://www.ietf.org/id/draft-varon-hrpc-methodology-00.txt>.

[Liddicoat]
Liddicoat, J. and A. Doria, "Human Rights and Internet Protocols", n.d., <https://www.apc.org/en/pubs/human-rights-and-internet-protocols-comparing-proc>.

[Post] Post, D., "Internet Infrastructure and IP Censorship", 2015, <http://www.ipjustice.org/digital-rights/internet-infrastructure-and-ip-censorship-bydavid-post/>.

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

[RFC1984] IAB and , "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <http://www.rfc-editor.org/info/rfc1984>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <http://www.rfc-editor.org/info/rfc2026>.

[RFC2639] Hastings, T. and C. Manros, "Internet Printing Protocol/1.0: Implementer’s Guide", RFC 2639, DOI 10.17487/RFC2639, July 1999, <http://www.rfc-editor.org/info/rfc2639>.

[RFC2919] Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists", RFC 2919, DOI 10.17487/RFC2919, March 2001, <http://www.rfc-editor.org/info/rfc2919>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <http://www.rfc-editor.org/info/rfc3365>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <http://www.rfc-editor.org/info/rfc5891>.

[RFC5892] Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <http://www.rfc-editor.org/info/rfc5892>.

[RFC5893] Alvestrand, H., Ed. and C. Karp, "Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)", RFC 5893, DOI 10.17487/RFC5893, August 2010, <http://www.rfc-editor.org/info/rfc5893>.

[RFC6162] Turner, S., "Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Asymmetric Key Package Content Type", RFC 6162, DOI 10.17487/RFC6162, April 2011, <http://www.rfc-editor.org/info/rfc6162>.

[RFC6783] Levine, J. and R. Gellens, "Mailing Lists and Non-ASCII Addresses", RFC 6783, DOI 10.17487/RFC6783, November 2012, <http://www.rfc-editor.org/info/rfc6783>.

[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>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <http://www.rfc-editor.org/info/rfc7231>.

[RFC7232] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests", RFC 7232, DOI 10.17487/RFC7232, June 2014, <http://www.rfc-editor.org/info/rfc7232>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <http://www.rfc-editor.org/info/rfc7234>.

[RFC7235] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", RFC 7235, DOI 10.17487/RFC7235, June 2014, <http://www.rfc-editor.org/info/rfc7235>.

[RFC7236] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Authentication Scheme Registrations", RFC 7236, DOI 10.17487/RFC7236, June 2014, <http://www.rfc-editor.org/info/rfc7236>.

[RFC7237] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Method Registrations", RFC 7237, DOI 10.17487/RFC7237, June 2014, <http://www.rfc-editor.org/info/rfc7237>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

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

[UNESCO] "Keystones to foster inclusive Knowledge Societies", 2015.

[Zittrain] Zittrain, J., "The Future of the Internet And How to Stop It", 2008.

Author’s Address

Avri Doria
Technicalities

EMail: avri@acm.org

Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: April 21, 2016

M. Nottingham
October 19, 2015

The Internet is for End Users
draft-nottingham-for-the-users-02

Abstract

Internet standards serve and are used by a variety of communities. This document contains guidelines for explicitly identifying them, serving them, and determining how to resolve conflicts between their interests, when necessary.

It also motivates considering end users as the highest priority concern for Internet standards.

Note to Readers

The issues list for this draft can be found at https://github.com/mnot/I-D/labels/for-the-users .

The most recent (often, unpublished) draft is at https://mnot.github.io/I-D/for-the-users/ .

Recent changes are listed at https://github.com/mnot/I-D/commits/gh-pages/for-the-users .

Status of This Memo

Table of Contents

1. Introduction

As the Internet has become prevalent in many societies, it has also unavoidably become a profoundly political thing; it has helped overthrow governments, revolutionize social orders, control populations and reveal people's secrets. It has created wealth for some individuals and companies, while destroying others'.

The IETF, while focused on technical matters, is not neutral about the purpose of its work [RFC3935]:

> The IETF community wants the Internet to succeed because we believe that the existence of the Internet, and its influence on economics, communication, and education, will help us to build a better human society.

However, the IETF is most comfortable making purely technical decisions; our process is defined to favor technical merit, through our well-known bias towards "rough consensus and running code".

Nevertheless, the running code that results from our process (when things work well) inevitably has an impact beyond technical considerations, because the underlying decisions afford some uses, while discouraging others. Or, in the words of Lawrence Lessig [CODELAW]:

> Ours is the age of cyberspace. It, too, has a regulator... This regulator is code -- the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.

All of this raises the question: Who do we go through the pain of rough consensus and write the running code for?

There are a variety of identifiable parties in the larger Internet community that standards can provide benefit to, such as (but not limited to) end users, network operators, schools, equipment vendors, specification authors, specification implementers, content owners, governments, non-governmental organisations, social movements, employers, and parents.

Successful specifications will provide some benefit to all of the relevant parties, because standards do not represent a zero-sum game. However, there are often situations where we need to balance the benefits of a decision between two (or more) parties.

We regularly decide to take up work against those who attempt to use the Internet for goals that we do not believe are beneficial; for example, those who attempt to disrupt Internet access (denial-of-service attackers) and those who seek to obtain data or control over a system that is not authorised by its administrator.

Additionally, efforts are sometimes brought to the IETF that represent the needs of some parties but at the expense of others. When presented with such a proposal, we need to decide how to handle it.

Currently, these kinds of decisions occur in an ad hoc fashion, often without explicitly being discussed. This approach works reasonably well in many cases; even if a party is not directly represented in the process, there are often advocates for their interests, and ultimately protocols that disadvantage a particular party tend to be either rejected by it or eventually replaced.

However, we do sometimes expend a considerable amount of energy mitigating potential harm to under-represented members of the Internet community, and often such harm is not so onerous or obvious as to dissuade them from using something (e.g., [RFC6265]).

In other words - because our decisions have ethical implications, we should consider their impact and determine whether it is within our core values, and do so in a well-defined, open fashion.

To facilitate that, Section 3 outlines a set of guidelines for identifying the relevant parties to an Internet standard. The aim of doing so is to both clarify the decision-making process, and to aid external parties when engaging with and judging the results of the standards process.

In doing so, it becomes clear that Internet standards that give the highest priority to end users have the best chance of success, and of helping the IETF to succeed in its mission. As a result, Section 2 mandates that other parties cannot have a higher priority.

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. The Internet is for End Users

Internet standards MUST NOT consider any other party to have higher priority over end users.

While networks need to be managed, employers and equipment vendors need to meet business goals, etc., the IETF’s mission is to "build a better human society" [RFC3935] and - on the Internet - society is composed of what we call "end users."

Furthermore, the success of the Internet to date is arguably due largely to its bias towards end user concerns; without a firm preference for their benefit, trust in the Internet will erode, and its value - for everyone - will be greatly diminished.

This does not mean that end users have ultimate priority; there may be cases where genuine technical need of another party requires that end user requirements compromise. However, such tradeoffs need to be carefully examined, and avoided when there are alternate means of achieving the desired goals. If they cannot be, these choices and reasoning SHOULD be carefully documented.

For example, IPv6 [RFC2460] identifies each client with a unique address - even though this provides a way to track end user activity and helps identify them - because it is technically necessary to provide networking (and despite this, there are mechanisms like [RFC4941] to mitigate this effect, for those users who desire it).

This also does not mean that the IETF community has any specific insight into what is "good for end users"; as before, we will need to interact with the greater Internet community and apply our process to help us make decisions, deploy our protocols, and ultimately determine their success or failure.

3. Identifying Relevant Parties

The relevant parties to an Internet standard MUST be documented, along with their interrelationships.

For example, HTML does so using the "priority of constituencies" in the HTML Design Principles [PRIORITY]:

> In case of conflict, consider users over authors over implementors over specifiers over theoretical purity. In other words costs or difficulties to the user should be given more weight than costs to authors; which in turn should be given more weight than costs to implementors; which should be given more weight than costs to authors of the spec itself, which should be given more weight than those proposing changes for theoretical reasons alone. Of course, it is preferred to make things better for multiple parties at once.

Note how the relative priority is explicit; this is intentional and encouraged. However, it need not be a strict ranking in all cases; in some areas, it can be more useful to give equal weight to parties, so as to encourage the tussle [TUSSLE].

Likewise, the responsibilities of, or expectations upon, different parties to a standard can vary greatly. For example, end users of Web browsers cannot be reasonably expected to make informed decisions about security, and therefore design decisions there are biased towards default security. When applicable, the expectations upon a party SHOULD be documented.

Extensions to existing standards MUST consider how they interact with the extended standard's relevant parties. If they are not yet documented, this SHOULD be done in coordination with that standard's community and the IESG.

The burden of this documentation need not be high; if HTML can do it in a paragraph, so can most other standards. While it might be appropriate in a separate document (e.g., a requirements or use cases draft) or the specification itself, documenting relevant parties in the WG charter has considerable benefits, since it clarifies their relationships up-front.

Inevitably, documenting and interpreting these roles will become controversial; this is to be expected, and is still preferable to avoiding the discussion. The point is to make it explicit, so that the affected parties can be made aware of the discussion, and judge the outcome.

3.1. Handling Change in Relevant Parties

Changes in the use, deployment patterns, legal context, or other factors of a standard can bring pressure to re-balance the priorities of existing parties, or insert new ones (usually, when a standard is either extended or evolved).

Such changes MUST NOT diminish the priority of existing relevant parties without informed consent. Note that this may preclude the change completely, as it is often impossible to gain the informed consent of a large or diffuse group (e.g., end users).

For example, there has been increasing pressure to change HTTP [RFC7230] to make it more amenable to optimization, filtering, and interposition of other value-added services, especially in the face of wider use of encryption (through HTTPS URIs). However, since HTTPS is already defined as a two-party protocol with end-to-end encryption, inserting a third party in any fashion would violate the expectations of two existing parties; end users and content publishers. Therefore, the HTTP Working Group has refused to consider such changes.

3.2. Avoiding Unnecessary Parties

In protocol design, intermediation is often thought of as "those parties on the direct path between two people attempting to communicate"; e.g., middleboxes, proxies and so on.

When discussing the parties relevant to an Internet standard, this definition can be expanded to include those parties that have the

ability to prevent or control communication between two parties. This naturally includes middleboxes, but can also include third parties not directly on-path.

For example, HTTP has on-path intermediaries (proxies, gateways, etc.), but also off-path intermediaries, in the form of the DNS registrar, the DNS server, and also the Certificate Authority if TLS is in use. Certificate Transparency [RFC6962] potentially adds yet another intermediary to this protocol suite.

While there might be a good technical reason to interpose such an intermediary, it also introduces a new party, and thus needs to be done with due consideration of the impact on other parties.

Therefore, unnecessary parties SHOULD be avoided when possible in Internet standards.

4. IANA Considerations

This document does not require action by IANA.

5. Security Considerations

This document does not have direct security impact; however, applying its guidelines (or failing to) might affect security positively or negatively.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

6.2. Informative References

[CODELAW] Lessig, L., "Code Is Law: On Liberty in Cyberspace", 2000, <http://harvardmagazine.com/2000/01/code-is-law-html>.

[PRIORITY] van Kesteren, A. and M. Stachowiak, "HTML Design Principles", November 2007, <http://www.w3.org/TR/html-design-principles/#priority-of-constituencies>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3935] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <http://www.rfc-editor.org/info/rfc3935>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <http://www.rfc-editor.org/info/rfc4941>.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011, <http://www.rfc-editor.org/info/rfc6265>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <http://www.rfc-editor.org/info/rfc6962>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[TUSSLE] Clark, D., Sollins, K., Wroclawski, J., and R. Braden, "Tussle in Cyberspace: Defining Tomorrow’s Internet", 2002, <http://groups.csail.mit.edu/ana/Publications/PubPDFs/Tussle2002.pdf>.

Appendix A. Acknowledgements

Thanks to Jacob Appelbaum for making the suggestion that led to this document.

Thanks also to the WHATWG for blazing the trail.

Thanks to Edward Snowden for his comments regarding the priority of end users at IETF93.

Thanks to Harald Alvestrand for his substantial feedback and Stephen Farrell, Joe Hildebrand, Russ Housley, Niels ten Oever, and Martin Thomson for their suggestions.

Author's Address

Mark Nottingham

Email: mnot@mnot.net
URI: http://www.mnot.net/

Human Rights Protocol Considerations Research Group J. Varon
Internet-Draft Coding Rights
Intended status: Informational N. ten Oever
Expires: April 18, 2016 Article19
C. Guarnieri
Centre for Internet and Human Rights
W. Scott
University of Washington
C. Cath
Oxford Internet Institute
October 16, 2015

Human Rights Protocol Considerations Methodology
draft-varon-hrpc-methodology-01

Abstract

This document presents steps undertaken for developing a methodology to map engineering concepts at the protocol level that may be related to promotion and protection of Human Rights, particularly the right to freedom of expression and association. It feeds upon and is intended to facilitate the work done by the proposed Human Rights Protocol Considerations research group, as well as other authors within the IETF.

Exemplary work [RFC1984] [RFC6973] [RFC7258] has already been done in the IETF on privacy issues that should be considered when creating an Internet protocol. But, beyond privacy considerations, concerns for freedom of expression and association were also a strong part of the world-view of the community involved in developing the first Internet protocols. Indeed, promoting open, secure and reliable connectivity is essential for these rights. But how are this concepts addressed in the protocol level? Are there others? This ID is intended to explain research work done so far and to explore possible methodological approaches to move further on exploring and exposing the relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

Discussion on this draft at: hrpc@irtf.org //
https://www.irtf.org/mailman/listinfo/hrpc

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Copyright Notice

Table of Contents

1. Introduction

In a manner similar to the work done for [RFC6973] on Privacy Consideration Guidelines, the premise of this research is that some standards and protocols can solidify, enable or threaten human rights.

As stated in [RFC1958], the Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. Our research hypothesis is that Internet's objective of connectivity makes it an enabler of human rights and that its architectural design tends to converge in protecting and promoting the human rights framework.

Open, secure and reliable connectivity is essential for human rights such as freedom of expression and freedom of association, as defined in the Universal Declaration of Human Rights [UDHR]. Therefore, considering connectivity as the ultimate objective of the Internet, makes a clear case that the Internet is not only an enabler of human rights, but that human rights lie at the basis of, and are ingrained in, the architecture of the network.

But, while the Internet was designed with freedom and openness of communications as core values, as the scale and the commercialization of the Internet has grown greatly, the influence of such world-views started to compete with other values. Therefore, decisive and human rights enabling characteristics of the Internet might be degraded if they're not properly defined, described and protected as such. And,

on the other way around, not protecting these characteristics could also result in (partial) loss of functionality and connectivity, thus, in the internet architecture design itself.

An essential part of maintaining the Internet as a tool for communication and connectivity is security. Indeed, "development of security mechanisms is seen as a key factor in the future growth of the Internet as a motor for international commerce and communication" [RFC1984] and according to the Danvers Doctrine [RFC3365], there is an overwhelming consensus in the IETF that the best security should be used and standardized.

In [RFC1984], the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, expressed: "concern by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy." Indeed, the IETF has been doing a significant job in this area [RFC6973] [RFC7258], considering privacy concerns as a subset of security concerns.

Besides privacy, it should be possible to highlight other aspects of connectivity embedded in standards and protocols that can have human rights considerations, such as freedom of expression and the right to association and assembly online. This ID is willing to explain research work done so far and explore possible methodological approaches to move further on exploring and exposing these relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

To move this debate further, information has been compiled at the https://datatracker.ietf.org/rg/hrpc/ and discussions are happening through the list hrpc@irtf.org

This document builds on the previous IDs published within the framework of the proposed hrpc research group [ID]

2. Research Topic

The growing impact of the Internet on the lives of individuals makes Internet standards and protocols increasingly important to society. The IETF itself, in [RFC2026], specifically states that the 'interests of the Internet community need to be protected'. There are various examples of protocols and standards having a direct impact on society, and by extension the human rights of end-users. Privacy is just one example. Therefore, this proposal for research methodology is addressing as research topics the rights to freedom of

expression and association and it’s relations to standards and protocols.

These two rights are described in the Universal Declaration of Human Rights:

Article 19 - Freedom of Expression (FoE) "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Article 20 - Freedom of Association (FoA) "Everyone has the right to freedom of peaceful assembly and association."

But how to talk about human rights in an engineering context?

But can we translate these concepts into Internet architecture technical terms?

What standards and protocols could have any relationship with freedom of expression and association?

What are the possible relationships between them?

3. Methodology

Mapping the relation between human rights and protocols and architectures is a new research challenge, which requires a good amount of interdisciplinary and cross organizational cooperation to develop a consistent methodology. While the authors of this first draft are involved in both human rights advocacy and research on Internet technologies - we believe that bringing this work into the IRTF facilitates and improves this work by bringing human rights experts together with the community of researchers and developers of Internet standards and technologies.

In order to map the potential relation between human rights and protocols, so far, the HRPC proposed research group has been gathered the data from three specific sources:

a. Discourse analysis of RFCs To start addressing the issue, a mapping exercise analyzing Internet architecture and protocols features, vis-a-vis possible impact on human rights is being undertaken. Therefore, research on the language used in current and historic RFCs and mailing list discussions is underway to expose core architectural principles, language and deliberations on human rights of those affected by the network.

b. Interviews with members of the IETF community during the Dallas meeting of March 2015 Interviews with the current and past members of the Internet Architecture Board (IAB), current and past members of the Internet Engineering Steering Group(IESG) and chairs of selected working groups and RFC authors. To get an insider understanding of how they view the relationship (if any) between human rights and protocols to play out in their work.

c. Participant observation in Working Groups By participating in various working groups information was gathered about the IETFs day-to-day work. From which which general themes and use-cases about human rights and protocols were extracted.

All this data was then processed using the following three consecutive strategies:

3.1. Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA Activity: Mapping of protocols and standards that potentially enable the internet as a tool for freedom of expression Expected Outcome: list of RFCs that describe standards and protocols that are potentially more closely related to FoE and FoA.

Step 1.2 - Extracting concepts from mapped RFCs Activity: Read the selected RFCs to highlight central design and technical concepts which impact human rights. Expected Outcome 1: a list of technical terms that combined create the enabling environment for freedom of expression and freedom of association. Expected Outcome 2: Possible translations of human rights concepts to technical terms.

Step 1.3 - Building a common glossary In the analysis of existing RFCs, central design and technical concepts shall be found which impact human rights. Expected Outcome: a Glossary for human rights protocol considerations with a list of concepts and definitions of technical concepts

3.2. Map cases of protocols being exploited or enablers

Step 1.1 - Cases of protocols being exploited Activity 1: Map cases in which users rights have been exploited, violated or compromised, analyze which protocols or vulnerabilities in protocols are invovled with this. Activity 2: Understand technical rationale for the use of particular protocols that undermine human rights. Expected Outcome: list of protocols that have been exploited to expose users to rights violation and rationale.

Step 1.2 - Cases of protocols being enablers Activity: Map cases in which users rights have been enabled, promoted and protected and analyze which characteristics in the protocols are involved with this. Expected Outcome: list of characteristics in the protocols that have been key to promote and protect the rights to freedom of expression and association that could be added to our glossary

3.3. Apply human rights technical definitions to the cases mapped

Step 1 - Glossary and Cases Activity: Investigate alternative technical options from within list of technical design principle (see [HRPC-GLOSSARY]) that could have been applied in the mapped cases to strengthen our technical definition of FoE and FoA, and hence human rights and connectivity of the network.

Expected Outcome: Identify best (and worst) current practices. Develop procedures to systematically evaluate protocols for potential human rights impact.

4. Preliminary findings achieved by applying current proposed methodology

4.1. Current status: Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA

Below are some examples of these protocols and standards that might be related to FoE and FoA and FoE:

HTTP Websites made it extremely easy for individuals to publish their ideas, opinions and thoughts. Never before has the world seen an infrastructure that made it this easy to share information and ideas with such a large group of other people. The HTTP architecture and standards, including [RFC7230], [RFC7231], [RFC7232], [RFC7234], [RFC7235], [RFC7236], and [RFC7237], are essential for the publishing of information. The HTTP protocol, therefore, forms an crucial enabler for freedom of expression, but also for the right to freely participate in the culture life of the community (Article 27) [UDHR], to enjoy the arts and to share in scientific advancement and its benefits.

Real time communications through XMPP and WebRTC Collaborations and cooperation via the Internet have take a large step forward with the progress of chat and other other real time communications protocols. The work on XMPP [RFC6162] has enabled new methods of global interactions, cooperation and human right advocacy. The WebRTC work being done to standardize the API and protocol elements to support

real-time communications for browsers, mobile applications and IoT by the World Wide Consortium (W3C) and the IETF is another artifact enabling human rights globally on the Internet.

Mailing lists Collaboration and cooperation have been part of the Internet since its early beginning, one of the instruments of facilitating working together in groups are mailing lists (as described in [RFC2639], [RFC2919], and [RFC6783]. Mailing lists are critical instruments and enablers for group communication and organization, and therefore form early artifacts of the (standardized) ability of Internet standards to enable the right to freedom of assembly and association.

IDNs English has been the lingua franca of the Internet, but for many Internet user English is not their first language. To have a true global Internet, one that serves the whole world, it would need to reflect the languages of these different communities. The Internationalized Domain Names IDNA2008 ([RFC5890], [RFC5891], [RFC5892], and [RFC5893]), describes standards for the use of a broad range of strings and characters (some also written from right to left). This enables users who use other characters than the standard LDH ascii typeset to have their own URLs. This shows the ambition of the Internet community to reflect the diversity of users and to be in line with Article 2 of the Universal Declaration of Human Rights which clearly stipulates that "everyone is entitles to all rights and freedoms "[...]", without distinction of any kind, such as "[...]" language "[...]"." [UDHR]

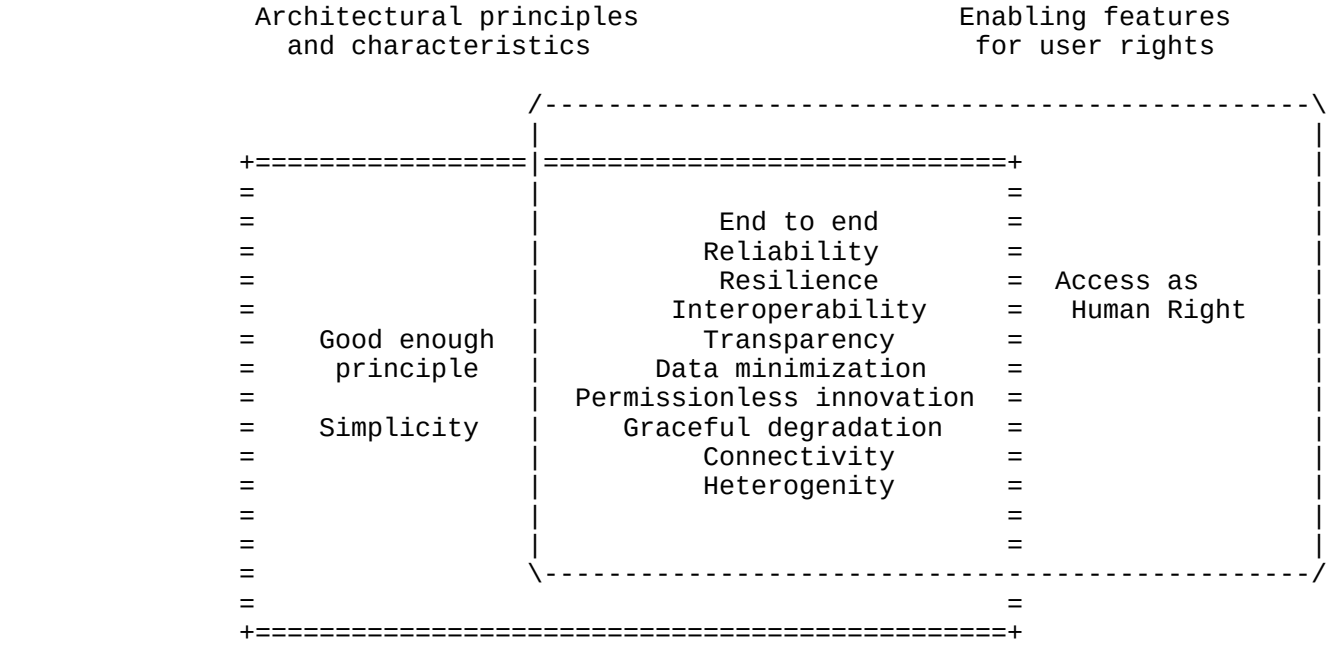
4.2. Current Status: Mapping protocols and standards related to FoE and FoA

Based on these standards and protocols as well as an analysis of existing RFCs and literature, a listing of architectural concepts has been made.

Step 1.2 - Extracting concepts from mapped RFCs The list of RFCs as well as relevant literature has used to extract key architectural principles. The main architectural concepts were subsequently listed in the glossary [HRPC-GLOSSARY].

4.3. Current Status: Extracting concepts from mapped RFCs

Expected Outcome 1: a list of technical terms that combined create the enabling environment for human rights, such a freedom of expression and freedom of association.



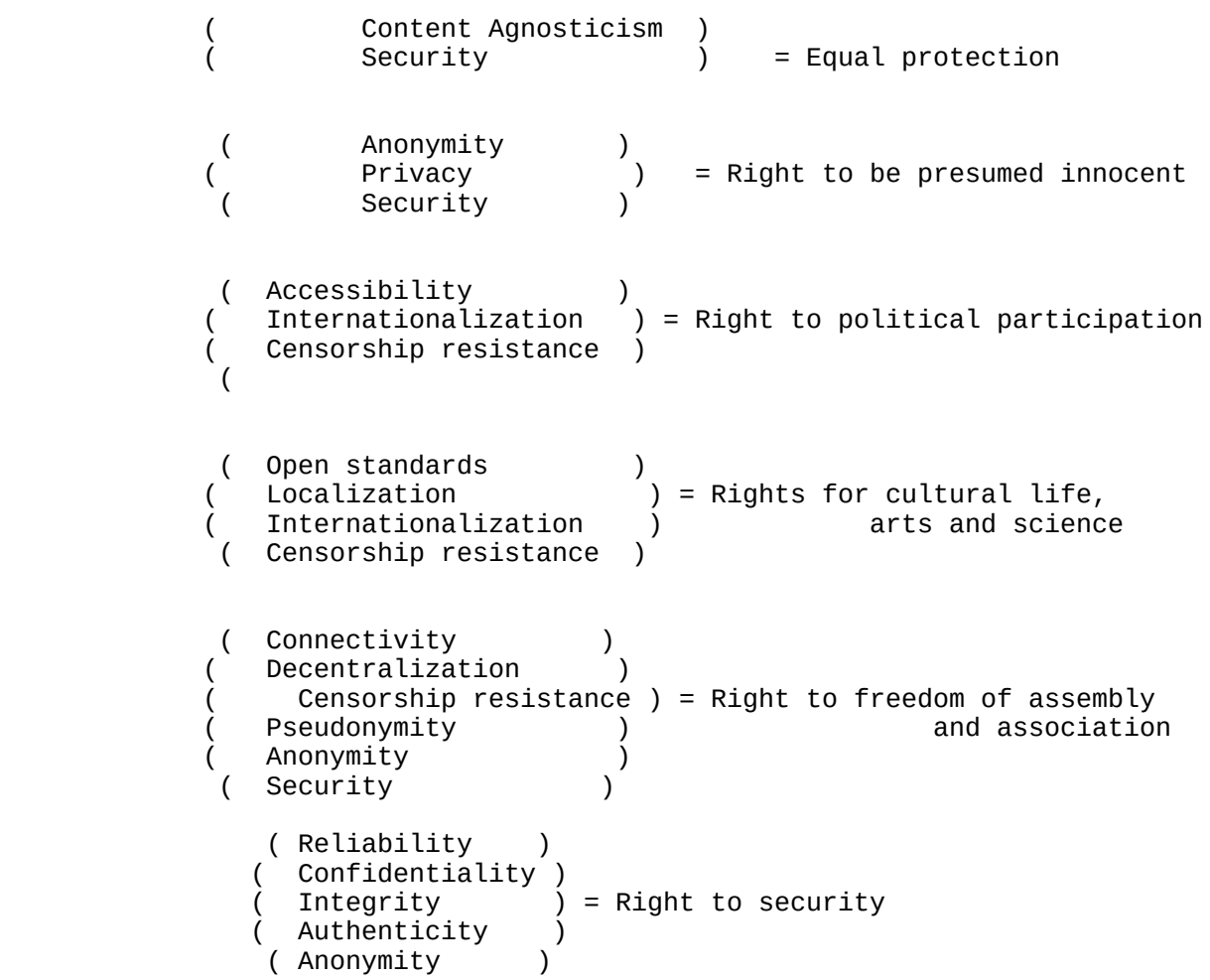
4.4. Current status: Translating human rights to technical terms

Expected outcome 2: This analysis aims to translate human rights concepts that impact or are impacted by the Internet as follows:

The combination of content agnosticism, connectivity, security, privacy (as defined in [RFC6973], and open standards are the technical principles that underlay freedom of expression on the Internet.

(Connectivity)
(Privacy)
(Security) = freedom of expression
(Content agnosticism)
(Internationalization)
(Censorship resistance)
(Open Standards)
(Heterogeneity support)

(Anonymity)
(Privacy) = Non-discrimination
(Pseudonymity)
(Content agnosticism)



Step 1.3 - Build a common glossary

4.5. Current status: Building of a common glossary

Expected Outcome: A glossary has been developed, which aims to build on other relevant published glossaries by the IETF and relevant literature: [HRPC-GLOSSARY]). This document aims to provide a description of relevant architectural principals as well as technical concepts that are relevant for describing the impact of protocols on human rights.

4.6. Current status: Map cases of protocols being exploited or enablers

4.6.1. IP

The Internet Protocol version 4, known as 'layer 3' of the internet, and specified as a common encapsulation and protocol header, is defined by [RFC0791]. The evolution of Internet communications have led to continued development in this area, encapsulated in the development of version 6 of the protocol in [RFC2460]. In spite of this updated protocol, we find that 25 years after the specification of version 6 of the protocol, the older v4 standard continues to account for a sizable majority of internet traffic.

The internet was designed as a platform for free and open communication, most notably encoded in the end-to-end principle, and that philosophy is also present in the technical implementation of the Internet Protocol. [RFC3724] While the protocol was designed to exist in an environment where intelligence is at the end hosts, it has proven to provide sufficient information that a more intelligent network core can make policy decisions and enforce policy shaping and restricting the communications of end hosts. These capabilities for network control and limitations of the freedom of expression by end hosts can be traced back to the IPv4 design, helping us understand which technical protocol decisions have led to harm of these human rights.

Two major shifts have occurred to harm freedom of expression through misuse of the Internet Protocol. The first is the network's exploitation of the public visibility of the host pairs for all communications, and the corresponding ability to discriminate and block traffic as a result of that metadata. The second is the selective development of IP options. Protocol extensions including Mobility and Multicasting have proposed alternate communication modes and suggest that different forms of assemply could be supported by an a robust IP layer. Instead, the protocol has limited the deployability of such extensions by not providing a mechanism for appropriate fallback behavior when unrecognized extensiosn are encountered.

4.6.1.1. Network visibility of Source and Destination

The IPv4 protocol header contains fixed location fields for both the source and destination IP addresses [RFC0791]. These addresses identify both the host sending and receiving each message, and allow the core network to understand who is talking to whom, and to practically limit communication selectively between pairs of hosts. Blocking of communication based on the pair of source and destination is one of the most common limitations on the ability for hosts to

communicate today, [caida] and can be seen as a restriction of the ability for those hosts to assemble or to consensually express themselves.

Inclusion of an Internet-wide identified source in the IP header is not the only possible design, especially since the protocol is most commonly implemented over Ethernet networks exposing only link-local identifiers. [RFC0894] A variety of alternative designs including source routing, and spoofing of the source IP address are technicaly supported by the protocol, but neither are regularly allowed on the Internet. While projects like [torproject] provide an alternative implementation of anonymity in connections, they have been developed in spite of the IPv4 protocol design.

4.6.1.2. Protocols

The other major feature of the IP protocol header is that it specifies the protocol encapsulated in each message in an easily observable form, and does not encourage a design where the encapsulated protocol is not available to a network observer. This design has resulted in a proliferation of routers which inspect the inner protocol, and has resulted in a stagnation where only the TCP and UDP protocols are widely supported across the Internet. While the IP protocol was designed as the entire set of metadata needed for routing, subsequent enhanced routers have found value on making policy decisions based on the contents of TCP and UDP headers as well, and are encoded with the assumption that only these protocols will be used for data transfer. [spdy] [RFC4303] defines an encrypted encapsulation of additional protocols, but lacks widespread deployment and faces the same challenge as any other protocol of providing sufficient metadata with each message for routers to make positive policy decisions. Protocols like [RFC4906] have seen limited wide-area uptake, and these alternate designs are frequently re-implemented on top of UDP. [quic]

4.6.1.3. Address Translation and Mobility

A major structural shift in the Internet which has undermined the protocol design of IPv4, and has significantly reduced the freedom of end users to communicate and assemble in the introduction network address translation. [RFC1631] Network address translation is a process whereby organizations and autonomous systems to connect two networks by translating the IPv4 source and destination addresses between the two. This process puts the router performing the translation into a privileged position, where it can decide which subset of communications are worthy of translation, and whether an unknown request for communication will be correctly forwarded to a host on the other network.

This process of translation has widespread adoption despite promoting a process that goes against the stated end-to-end process of the underlying protocol [natusage]. In contrast, the proposed mechanism to provide support for mobility and forwarding to clients which may move, encoded instead as an option in the IP protocol in [RFC5944], has failed to gain traction. This situation again suggests that the compromise made in design of the protocol has resulted in a technology which failed to technical encode the freedom of expression goals it was designed to promote.

4.6.2. DNS

The Domain Name System (DNS) [RFC1035], provides service discovery capabailities, and provides a mechanism to associate human readable names with services. The DNS system is organized around a set of independently operated 'Root Servers' run by organizations around the web which enact ICANN's policy by answering queries for which organizations have been delegated to manage registration under each Top Level Domain (TLD). Top Level domains are maintained and determined by ICANN. These namespaces encompass several classes of services. The initial name spaces including '.Com' and '.Net', provide common spaces for expression of ideas, though their policies are enacted through US based companies. Other name spaces are delegated to specific nationalities, and may impose limits designed to focus speech in those forums both to promote speech from that nationality, and to comply with local limits on expression and social norms. Finally, the system has been recently expanded with additional generic and sponsored name spaces, for instance '.travel' and '.ninja', which are operated by a range of organizations which may independently determine their registration policies.

DNS has significant privacy issues per [RFC7626]. Most notable are the lack of encryption to limit the visibility of requests for domain resolution from intermediary parties, and a limited deployment of DNSSEC to provide authentication, allowing the client to know that they have received a correct, "authoritative", answer to a query. Together, this situation results in ongoing harm to freedom of expression as interference with the operation of DNS has become one of the central mechanisms used to block access to websites. This interference limits both the freedom of expression of the publisher to offer their content, and the freedom of assembly for clients to congregate in a shared virtual space.

There have been several mechanisms used impose these limitations based on the technical design of the DNS protocol. These have led to a number of situations where limits on expression have been imposed through subversion of the DNS protocol. Each of these situations has accompanying aspects of protocol design enabling those limitations.

4.6.2.1. Removal of records

There have been a number of cases where the records for a domain are removed from the name system due to real-world events. Examples of this removal includes the ’seizure’ of wikileaks [bbc-wikileaks] and the names of illegally operating gambling operations by the United States ICE unit, which compelled the US-based registry in charge of the .com TLD to hand ownership of those domains over to the government. The same technique has been notably used by Libya to remove sites in violation of "our Country’s Law and Morality (which) do not allow any kind of pornography or its promotion." [techyum]

At a protocol level, there is no technical auditing for name ownership, as in alternate systems like [namecoin]. As a result, there is no ability for users to differentiate seizure from the legitimate transfer of name ownership, which is purely a policy decision of registrars. While DNSSEC addresses network distortion events described below, it does not tackle this problem, which has the cooperation of (or compelled action by) the registry.

4.6.2.2. Distortion of records

The most common mechanism by which the DNS system is abused to limit freedom of expression is through manipulation of protocol messages by the network. One form occurs at an organizational level, where client computers are instructed to use a local DNS resolver controlled by the organization. The DNS resolver will then selectively distort responses rather than request the authoritative lookup from the upstream system. The second form occurs through the use of deep packet inspection, where all DNS protocol messages are inspected by the network, and objectionable content is distorted, as in [turkey].

A notable instance of distortion has occurred in Greece [ververis], where a study found evidence of both of deep packet inspection to distort DNS replies, and overblocking of content, where ISPs prevented clients from resolving the names of domains which they were not instructed to do through the governmental order prompting the blocking systems there.

At a protocol level, the effectiveness of these attacks is made possible by a lack of authentication in the DNS protocol. DNSSEC provides the ability to determine authenticity of responses when used, but it is not regularly checked by resolvers. DNSSEC is not effective when the local resolver for a network is complicit in the distortion, for instance when the resolver assigned for use by an ISP is the source of injection. Selective distortion of records has also been made possible by the predictable structure of DNS messages,

which make it computationally easy for a network device to watch all passing messages even at high speeds, and the lack of encryption, which allows the network to distort only an objectionable subset of protocol messages. Specific distortion mechanisms are discussed further in [draft-hall-censorship-tech-01].

4.6.2.3. Injection of records

Responding incorrectly to requests for name lookups is the most common mechanism that in-network devices use to limit the ability of end users to discover services. A deviation which accomplishes a similar objective, though may be seen as different from a freedom of expression perspective, is the injection of incorrect responses to queries. The most prominent example of this behavior occurs in China, where requests for lookups of sites which have been deemed inappropriate will trigger the network to respond with a bogus response, causing the client to ignore the real response when it subsequently arrives. [greatfirewall] Unlike the other forms of discussion discussed above, injection does not stifle the ability of a server to announce it’s name, it instead provides another voice which answers sooner. This is effective because without DNSSEC, the protocol will respond to whichever answer is received first, without listening for subsequent answers.

4.6.3. HTTP

The Hypertext Transfer Protocol (HTTP), described in its version 1.1 in RFC 7230 to 7237, is a request-response application protocol developed throughout the 1990s, and factually contributed to the exponential growth of the Internet and the inter-connection of populations around the world. Because of its simple design, HTTP has become the foundation of most modern Internet platforms and communication systems, from websites, to chat systems, and computer-to-computer applications. In its manifestation with the World Wide Web, HTTP has radically revolutionized the course of technological development and the ways people interact with online content and with each other. However, HTTP is also a fundamentally insecure protocol, that doesn’t natively provide encryption properties. While the definition of the Secure Sockets Layer (SSL), and later of Transport Layer Security (TLS), also happened during the 1990s, the fact that HTTP doesn’t mandate the use of such encryption layers to developers and service providers, caused a very late adoption. Only in the middle of the 2000s we observed big Internet service providers, such as Google, starting to provide encrypted access to their web services.

The lack of sensitivity and understanding of the critical importance of securing web traffic incentivized malicious and offensive actors

to develop, deploy and utilize at large interception systems and later active injection attacks, in order to swipe large amounts of data, compromise Internet-enabled devices. The commercial availability of systems and tools to perform these types of attacks also led to a number of human rights abuses that have been discovered and reported over the years and that painted a dark picture on the current state of control over the Internet.

Generally we can identify in Traffic Interception and Traffic Manipulation the two most problematic attacks that can be performed against applications employing a clear-text HTTP transport layer.

4.6.3.1. Traffic Interception

While we are seeing an increasing trend in the last couple of years to employ SSL/TLS as a secure traffic layer for HTTP-based applications, we are still far from seeing an ubiquitous use of encryption on the World Wide Web. It is important to consider that the adoption of SSL/TLS is also a relatively recent phenomena. Google introduced an option for its GMail users to navigate with SSL only in 2008 [Rideout], and turned SSL on by default later in 2010 [Schillace]. It took an increasing amount of scandalous security breaches and revelations on global surveillance from Edward Snowden to have other Internet service providers to follow Google’s lead. For example, Yahoo enabled SSL/TLS by default on its webmail services only towards the end of 2013 [Peterson].

As we learned through the Snowden’s revelations, intelligence agencies have been intercepting and collecting unencrypted traffic at large for many years. There are documented examples of such mass surveillance programs with GCHQ’s TEMPORA and NSA’s XKEYSCORE. Through these programs NSA/GCHQ have been able to swipe large amounts of data including email and instant messaging communications which have been transported by the respective providers in clear for years, unsuspecting of the pervasiveness and scale of governments’ efforts and investment into global mass surveillance capabilities.

However, similar mass interception of unencrypted HTTP communications is also often employed at a nation-level by less democratic countries by exercising control over state-owned Internet Service Providers (ISP) and through the use of commercially available monitoring, collection, and censorship equipment. Over the last few years a lot of information has come to public attention on the role and scale of a surveillance industry dedicated to develop interception gear of different types. We have several records of such equipment being sold and utilized by oppressive regimes in order to monitor entire segments of population especially at times of social and political distress, uncovering massive human rights abuses. For example, in

2013 the group Telecomix revealed that the Syrian regime was making use of BlueCoat products in order to intercept clear-text traffic as well as to enforce censorship of unwanted content [RSF]. Similarly in 2012 it was found that the French Amesys provided the Gaddafi's government with equipment able to intercept emails, Facebook traffic, and chat messages ad a country level. The use of such systems, especially in the context of the Arab Spring and of civil uprisings against the dictatorships, has caused serious concerns of significant human rights abuses in Libya.

4.6.3.2. Traffic Manipulation

The lack of a secure transport layer over HTTP connections not only exposes the users to interception of the content of their communications, but is more and more commonly abused as a vehicle for active compromises of computers and mobile devices. If an HTTP session travels in clear over the network, any node positioned at any point in the network is able to perform man-in-the-middle attacks and observe, manipulate, and hijack the session and modify the content of the communication in order to trigger unexpected behavior by the application generating the traffic. For example, in the case of a browser the attacker would be able to inject malicious code in order to exploit vulnerabilities in the browser or any of its plugins. Similarly, the attacker would be able to intercept, trojanize, and repackage binary software updates that are very commonly downloaded in clear by applications such as word processors and media players. If the HTTP session would be encrypted, the tampering of the content would not be possible, and these network injection attacks would not be successful.

While traffic manipulation attacks have been long known, documented, and prototyped especially in the context of WiFi and LAN networks, in the last few years we observed an increasing investment into the production and sale of network injection equipment both available commercially as well as deployed at scale by intelligence agencies. For example we learned from some of the documents provided by Edward Snowden to the press, that the NSA has constructed a global network injection infrastructure, called QUANTUM, able to leverage mass surveillance in order to identify targets of interests and subsequently task man-on-the-side attacks to ultimately compromise a selected device. Among other attacks, NSA makes use of an attack called QUANTUMINSERT [Haagsma] which intercepts and hijacks an unencrypted HTTP communication and forces the requesting browser to redirect to a host controlled by NSA instead of the intended website. Normally, the new destination would be an exploitation service, referred in Snowden documents as FOXACID, which would attempt at executing malicious code in the context of the target's browser. The Guardian reported in 2013 that NSA has for example been using these

techniques to target users of the popular anonymity service Tor [Schneier]. The German NDR reported in 2014 that NSA has also been using its mass surveillance capabilities to identify Tor users at large [Appelbaum]. Recently similar capabilities of Chinese authorities have been reported as well in what has been informally called the "Great Cannon" [Marcak], which raised numerous concerns on the potential curb on human rights and freedom of speech due to the increasing tighter control of Chinese Internet communications and access to information. Network injection attacks are also made widely available to state actors around the world through the commercialization of similar, smaller scale equipment that can be easily acquired and deployed at a country-wide level. Companies like FinFisher and HackingTeam are known to have network injection gear within their products portfolio, respectively called FinFly ISP and RCS Network Injector [Marquis-Boire]. The technology devised and produced by HackingTeam to perform network traffic manipulation attacks on HTTP communications is even the subject of a patent application in the United States [Googlepatent]. Access to offensive technologies available on the commercial lawful interception market has been largely documented to have lead to human rights abuses and illegitimate surveillance of journalists, human rights defenders, and political activists in many countries around the world. Companies like FinFisher and HackingTeam have been found selling their products to oppressive regimes with little concern for bad human rights records [Collins]. While network injection attacks haven’t been the subject of much attention, they do enable even unskilled attackers to perform silent and very resilient compromises, and unencrypted HTTP remains one of the main vehicles.

4.6.4. XMPP

The Extensible Messaging and Presence Protocol (XMPP), specified in RFC 3920, provides a standard for interactive chat messaging, and has evolved to encompass interoperable text, voice, and video chat. The protocol is structured as a federated network of servers, similar to email, where users register with a local server which acts one their behalf to cache and relay messages. This protocol design has many advantages, allowing servers to shield clients from denial of service and other forms of retribution for their expression, and designed to avoid central entities which could control the ability to communicate or assemble using the protocol.

None-the-less, there are plenty of aspects of the protocol design of XMPP which shape the ability for users to communicate freely, and to assembly through the protocol. In addition to issues of user registration and a lack of protocol specification of the registration policy, the protocol also has facets that may stifle speech as users

self-censor for fear of surveillance, or find themselves unable to express themselves naturally.

4.6.4.1. User Identification

The XMPP specification specifies that clients are identified with a resource (node@domain/home [1] / node@domain/work [2]) to distinguish the conversations to specific devices. This has the side effect of enabling tracking of user behavior by a remote friend or server, who are able to track presence not only of the user, but of each individual device. This has proven to be misleading to many users, since many clients only expose user level rather than device level presence. Likewise, user invisibility so that communication can occur while users don't notify all buddies and other servers of their availability is not part of the formal protocol, and has only been added as an extension within the XML stream rather than enforced by the protocol.

Documentation of this form of harm: https://developer.pidgin.im/ticket/4322

4.6.4.2. Character Encoding

Localization is a source of frustration in many protocols, and appears in some forms of XMPP. The XMPP protocol specifies a requirement for UTF-8 and UTF-16 support [Saint-Andre], though documentation admits that many implementations may not support UTF-16. In practice, this leads to cases where text encoded outside of a standard english language ascii encoding will fail to render on all clients, limiting the ability of users to communicate in their native languages. Some examples are failure of XMPP servers to handle non-ascii passwords [Polvorin], and gateways which simply strip all non-ascii from the conversation stream.

At the protocol level, XMPP only defines the conversation as an XML block, and leaves the implementation of character sets to the XMPP parsers of each individual client and server. While there have been attempts to define UTF-16 support as part of the protocol specification, the lack of actual implementation of the more extensible character set by all clients has shaped the protocol to harm the full range of expression users may desire.

Documentation of this form of harm: - [Saint-Andre] - http://xmpp.org/rfcs/rfc6120.html#streams-error-conditions-unsupported-encoding - [Polvorin]

4.6.4.3. Surveillance of Communication

The XMPP protocol specifies the standard by which communication of channels may be encrypted, but it does not provide visibility to clients of whether their communications are encrypted on each link. In particular, even when both clients ensure that they have an encrypted connection to their XMPP server to ensure that their local network is unable to read or disrupt the messages they send, the protocol does not provide visibility into the encryption status between the two servers. As such, clients may be subject to selective disruption of communications by an intermediate network which disrupts communications based on keywords found through Deep Packet Inspection.

In particular, section 13.14 of the protocol specification [RFC6120] explicitly acknowledges the existence of a downgrade attack where an adversary controlling an intermediate network can force the inter domain federation between servers to revert to a non-encrypted protocol were selective messages can then be disrupted.

Documentation of this form of harm: - https://raw.githubusercontent.com/stpeter/manifesto/master/manifesto.txt - [RFC6120]

4.6.4.4. Group Chat Limitations

Group chat in the XMPP protocol is defined as an extension within the XML specification of the XMPP protocol (http://xmpp.org/extensions/xep-0045.html). However, it is not encoded or required at a protocol level, and not uniformly implemented by clients.

The design of multi-user chat in the XMPP protocol suffers from extending a protocol that was not designed with assembly of many users in mind. In particular, in the federated protocol provided by XMPP, multi-user communities are implemented with a distinguished ’owner’, who is granted control over the participants and structure of the conversation.

Multi-user chat rooms are identified by a name specified on a specific server, so that while the overall protocol may be federated, the ability for users to assemble in a given community is moderated by a single server. That server may block the room and prevent assembly unilaterally, even between two users neither of whom trust or use that server directly.

4.6.5. Peer to Peer

Peer-to-Peer (P2P) is a network architecture (defined in RFC7574) in which all the participant nodes are equally responsible engaged into the storage and dissemination of information. A P2P network is a logical overlay that lives on top of the physical network, and allows nodes (or "peers") participating to it to establish contact and exchange information directly from one to each other. The implementation of a P2P network may very widely: it may be structured or unstructured, and it may implement stronger or weaker cryptographic and anonymity properties. While its most common application has traditionally been file-sharing (and other types of content delivery systems), P2P is increasingly becoming a popular architecture for networks and applications that require (or encourage) decentralization. A prime example is Bitcoin (and similar cryptocurrencies), as well as Skype, Spotify and other proprietary multimedia applications.

In a time of heavily centralized online services, peer-to-peer is often seen as an alternative, more democratic, and resistant architecture that displaces structures of control over data and communications and delegates all peers equally to be responsible for the functioning, integrity, and security of the data. While in principle peer-to-peer remains critical to the design and development of future content distribution, messaging, and publishing systems, it poses numerous security and privacy challenges which are mostly delegated to individual developers to recognize, analyze, and solve in each implementation of a given P2P network.

4.6.5.1. Network Poisoning

Since content, and in some occasions peer lists, are safeguarded and distributed by its members, P2P networks are prone to what are generally defined as "poisoning attacks". Poisoning attacks might be directed directly at the data that is being distributed, for example by intentionally corrupting it, or at the index tables used to instruct the peers where to fetch the data, or at routing tables, with the attempt of providing connecting peers with lists of rogue or non-existing peers, with the intention to effectively cause a Denial of Service on the network.

4.6.5.2. Throttling

Peer-to-Peer traffic (and BitTorrent in particular) represents a high percentage of global Internet traffic and it has become increasingly popular for Internet Service Providers to perform throttling of customers lines in order to limit bandwidth usage [torrentfreak1] and

sometimes probably as an effect of the ongoing conflict between copyright holders and file-sharing communities [wikileaks].

Throttling the peer-to-peer traffic makes some uses of P2P networks ineffective and it might be coupled with stricter inspection of users' Internet traffic through Deep Packet Inspection techniques which might pose additional security and privacy risks.

4.6.5.3. Tracking and Identification

One of the fundamental and most problematic issues with traditional peer-to-peer networks is a complete lack of anonymization of its users. For example, in the case of BitTorrent, all peers' IP addresses are openly available to the other peers. This has lead to an ever-increasing tracking of peer-to-peer and file-sharing users [ars]. As the geographical location of the user is directly exposed, and so could be his identity, the user might become target of additional harassment and attacks, being of physical or legal nature. For example, it is known that in Germany lawfirms have made extensive use of peer-to-peer and file-sharing tracking systems in order to identify downloaders and initiate legal actions looking for compensations [torrentfreak2].

It is worth nothing that there are varieties of P2P networks that implement cryptographic practices and that introduce anonymization of its users. Such implementations proved to be successful in resisting censorship of content, and tracking of the network peers. A primary example is FreeNet [freenet1], a free software application designed to significantly increase the difficulty of users and content identification, and dedicated to foster freedom of speech online [freenet2].

4.6.5.4. Conclusions

Encrypted P2P and Anonymous P2P networks already emerged and provided viable platforms for sharing material, publish content anonymously, and communicate securely [bitmessage]. If adopted at large, well-designed and resistant P2P networks might represent a critical component of a futuresecure and distributed Internet, enabling freedom of speech and freedom of information at scale.

4.6.6. Virtual Private Network

4.6.6.1. Introduction

A Virtual Private Network (VPN) is a point-to-point connection that enables two computers to communicate over an encrypted tunnel. There are multiple implementations and protocols used in provisioning a

VPN, and they generally diversify by encryption protocol or particular requirements, most commonly in proprietary and enterprise solutions. VPNs are used commonly either to enable some devices to communicate through peculiar network configurations, or in order to use some privacy and security properties in order to protect the traffic generated by the end user; or both. VPNs have also become a very popular technology among human rights defenders, dissidents, and journalists worldwide to avoid local illegitimate wiretapping and eventually also to circumvent censorship. Among human rights defenders VPNs are often debated as a potential alternative to Tor or other anonymous networks. Such comparison is mislead, as some of the privacy and security properties of VPNs are often misunderstood by less tech-savvy users, which could ultimately lead to unintended problems.

As VPNs increased in popularity, commercial VPN providers have started growing in business and are very commonly picked by human rights defenders and people at risk, as they are normally provided with an easy-to-use service and sometimes even custom applications to establish the VPN tunnel. Not being able to control the configuration of the network, and even less so the security of the application, assessing the general privacy and security state of common VPNs is very hard. Often such services have been discovered leaking information, and their custom applications have been found flawed. While Tor and similar networks receive a lot of scrutiny from the public and the academic community, commercial or non-commercial VPN networks are way less analyzed and understood, and it might be valuable to establish some standards to guarantee a minimal level of privacy and security to those who need them the most.

4.6.6.2. False sense of Anonymity

One of the common misconception among users of VPNs is the level of anonymity VPN can provide. This sense of anonymity can be betrayed by a number of attacks or misconfugrations of the VPN provider. It is important to remember that, contrarily to Tor and similar systems, VPN was not designed to provide anonymity properties. From a technical point of view, the VPN might leak identifiable information, or might be subject of correlation attacks that could expose the originating address of the connecting user. Most importantly, it is vital to understand that commercial and non-commercial VPN providers are bound by the law of the jurisdiction they reside in or in which their infrastructure is located, and they might be legally forced to turn over data of specific users if legal investigations or intelligence requirements dictate so. In such cases, if the VPN providers retain logs, it is possible that the information of the user is provided to the user’s adversary and leads to his or her identification.

4.6.6.3. Logging

With VPN being point-to-point connections, the service providers are in fact able to observe the original location of the connecting users and they are able to track at what time they started their session and eventually also to which destinations they're trying to connect to. If the VPN providers retain logs for long enough, they might be forced to turn over the relevant data or they might be otherwise compromised, leading to the same data getting exposed. A clear log retaining policy could be enforced, but considering that countries enforce very different levels of data retention policies, VPN providers should at least be transparent on what information do they store and for how long is being kept.

4.6.6.4. 3rd Party Hosting

VPN providers very commonly rely on 3rd parties to provision the infrastructure that is later going to be used to run VPN endpoints. For example, they might rely on external dedicated server hosting providers, or on uplink providers. In those cases, even if the VPN provider itself isn't retaining any significant logs, the information on the connecting users might be retained by those 3rd parties instead, introducing an additional collection point for the adversary.

4.6.6.5. IPv6 Leakage

Some studies proved that several commercial VPN providers and applications suffer of critical leakage of information through IPv6 due to improper support and configuration [PETS2015VPN]. This is generally caused by a lack of proper configuration of the client's IPv6 routing tables. Considering that most popular browsers and similar applications have been supporting IPv6 by default, if the host is provided with a functional IPv6 configuration, the traffic that is generated might be leaked if the VPN application isn't designed to manipulate such traffic properly.

4.6.6.6. DNS Leakage

Similarly, VPN services that aren't handling DNS requests and are not running DNS servers of their own, might be prone to DNS leaking which might not only expose sensitive information on the activity of the user, but could also potentially lead to DNS hijacking attacks and following compromises.

4.6.6.7. Traffic Correlation

As revelations of mass surveillance have been growing in the press, additional details on attacks on secure Internet communications have come to the public's attention. Among these, VPN appeared to be a very interesting target for attacks and collectiong efforts. Some implementations of VPN appear to be particularly vulnerable to identification and collection of key exchanges which, some Snowden documents revealed, are systematically collected and stored for future reference. The ability of an adversary to monitor network connections at many different points over the Internet, can allow them to perform traffic correlation attacks and identify the origin of certain VPN traffic by cross referencing the connection time of the user to the endpoint and the connection time of the endpoint to the final destination. These types of attacks, although very expensive and normally only performed by very resourceful adversaries, have been documented [spiegel] to be already in practice and could completely vanify the use of a VPN and ultimately expose the activity and the identity of a user at risk.

5. Next Steps of the Methodology still to be applied

5.1. Apply human rights technical definitions to the cases mapped

6. Next Steps of the Methodology still to be developed

6.1. Future research questions

All of the steps mentioned above raise the following question that need to be addressed after the research methodological steps outlined above have been completed:

How can the rights enabling environment be safeguarded in (future) protocol development?

How can (nontransparent) human rights violations be minimized in (future) protocol development?

Can we propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, specially in relation to freedom of expression and freedom of association, in a manner similar to the work done for Privacy Considerations in [RFC6973]?

Assuming that the research produces useful results, can the objective evolve into the creation of a set of recommended considerations for the protection of applicable human rights?

7. Acknowledgements

Special thanks to all members of the hrpc proposed RG who contributed to this draft. The following deserve a special mention: Stephane Bortzmeyer, dkg and Tim Sammut.

8. Security Considerations

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

9. IANA Considerations

This document has no actions for IANA.

10. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working group is located at the e-mail address hrpc@ietf.org [3]. 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

11. References

11.1. Informative References

[Appelbaum] Appelbaum, J., Gibson, A., Kabish, V., Kampf, L., and L. Ryge, "NSA targets the privacy-conscious", 2015, <http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html>.

[Collins] Collins, K., "Hacking Team’s oppressive regimes customer list revealed in hack", 2015, <http://www.wired.co.uk/news/archive/2015-07/06/hacking-team-spyware-company-hacked>.

[Googlepatent] Google, ., "Method and device for network traffic manipulation", 2012, <https://www.google.com/patents/EP2601774A1?cl=en>.

[HRPC-GLOSSARY]
ten Oever, N., Doria, A., and D. Gillmor, "Human Rights Protocol Considerations Glossary", 2015, <https://www.ietf.org/id/draft-dkg-hrpc-glossary-00.txt>.

[Haagsma] Haagsma, L., "Deep dive into QUANTUM INSERT", 2015, <http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/>.

[ID] ten Oever, N., Doria, A., and J. Varon, "Proposal for research on human rights protocol considerations", 2015, <http://tools.ietf.org/html/draft-doria-hrpc-proposal>.

[Marcak] Marcak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., and V. Paxson, "China's Great Fire Cannon", 2015, <https://citizenlab.org/2015/04/chinas-great-cannon/>.

[Marquis-Boire]
Marquis-Boire, M., "Schrodinger's Cat Video and the Death of Clear-Text", 2014, <https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/>.

[PETS2015VPN]
Pera, V., Barbera, M., Tyson, G., Haddadi, H., and A. Mei, "A Glance through the VPN Looking Glass", 2015, <http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf>.

[Peterson]
Peterson, A., Gellman, B., and A. Soltani, "Yahoo to make SSL encryption the default for Webmail users. Finally.", 2013, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[Polvorin]
Polvorin, P., "Fix cyrsasl_digest RFC-2831 2.1.2.1", 2010, <https://support.process-one.net/browse/EJAB-476>.

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

[RFC0894] Hornig, C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks", STD 41, RFC 894, DOI 10.17487/RFC0894, April 1984, <http://www.rfc-editor.org/info/rfc894>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC1631] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, <http://www.rfc-editor.org/info/rfc1631>.

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

[RFC1984] IAB and , "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <http://www.rfc-editor.org/info/rfc1984>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <http://www.rfc-editor.org/info/rfc2026>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2639] Hastings, T. and C. Manros, "Internet Printing Protocol/1.0: Implementer’s Guide", RFC 2639, DOI 10.17487/RFC2639, July 1999, <http://www.rfc-editor.org/info/rfc2639>.

[RFC2919] Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists", RFC 2919, DOI 10.17487/RFC2919, March 2001, <http://www.rfc-editor.org/info/rfc2919>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <http://www.rfc-editor.org/info/rfc3365>.

[RFC3724] Kempf, J., Austein., R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <http://www.rfc-editor.org/info/rfc3724>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[RFC4906] Martini, L., Ed., Rosen, E., Ed., and N. El-Aawar, Ed., "Transport of Layer 2 Frames Over MPLS", RFC 4906, DOI 10.17487/RFC4906, June 2007, <http://www.rfc-editor.org/info/rfc4906>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <http://www.rfc-editor.org/info/rfc5891>.

[RFC5892] Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <http://www.rfc-editor.org/info/rfc5892>.

[RFC5893] Alvestrand, H., Ed. and C. Karp, "Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)", RFC 5893, DOI 10.17487/RFC5893, August 2010, <http://www.rfc-editor.org/info/rfc5893>.

[RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", RFC 5944, DOI 10.17487/RFC5944, November 2010, <http://www.rfc-editor.org/info/rfc5944>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[RFC6162] Turner, S., "Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Asymmetric Key Package Content Type", RFC 6162, DOI 10.17487/RFC6162, April 2011, <http://www.rfc-editor.org/info/rfc6162>.

[RFC6783] Levine, J. and R. Gellens, "Mailing Lists and Non-ASCII Addresses", RFC 6783, DOI 10.17487/RFC6783, November 2012, <http://www.rfc-editor.org/info/rfc6783>.

[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>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <http://www.rfc-editor.org/info/rfc7231>.

[RFC7232] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests", RFC 7232, DOI 10.17487/RFC7232, June 2014, <http://www.rfc-editor.org/info/rfc7232>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <http://www.rfc-editor.org/info/rfc7234>.

[RFC7235] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", RFC 7235, DOI 10.17487/RFC7235, June 2014, <http://www.rfc-editor.org/info/rfc7235>.

[RFC7236] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Authentication Scheme Registrations", RFC 7236, DOI 10.17487/RFC7236, June 2014, <http://www.rfc-editor.org/info/rfc7236>.

[RFC7237] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Method Registrations", RFC 7237, DOI 10.17487/RFC7237, June 2014, <http://www.rfc-editor.org/info/rfc7237>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <http://www.rfc-editor.org/info/rfc7626>.

[RSF] RSF, ., "Syria using 34 Blue Coat Servers to spy on Internet users", 2013, <https://en.rsf.org/syria-syria-using-34-blue-coat-servers-23-05-2013,44664.html>.

[Rideout] Rideout, A., "Making security easier", 2008, <http://gmailblog.blogspot.de/2008/07/making-security-easier.html>.

[Saint-Andre] Saint-Andre, P., "Inconsistent/redundant character encoding requirements", 2003, <http://mail.jabber.org/pipermail/xmppwg/2003-August/001460.html>.

[Schillace] Schillace, S., "Default https access for Gmail", 2010, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[Schneier] Schneier, B., "Attacking Tor - how the NSA targets users' online anonymity", 2013, <http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>.

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

[ars] Anderson, N., "P2P researchers - use a blocklist or you will be tracked... 100% of the time", 2007, <http://arstechnica.com/uncategorized/2007/10/p2p-researchers-use-a-blocklist-or-you-will-be-tracked-100-of-the-time/>.

[bbc-wikileaks] BBC, "Whistle-blower site taken offline", 2008, <http://news.bbc.co.uk/2/hi/technology/7250916.stm>.

[bitmessage] Bitmessage, "Bitmessage Wiki?", 2014, <https://bitmessage.org/wiki/Main_Page>.

[caida] Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., and A. Pescape, "Analysis of Country-wide Internet Outages Caused by Censorship", 2013, <http://www.caida.org/publications/papers/2014/outages_censorship/outages_censorship.pdf>.

[draft-hall-censorship-tech-01]
Hall, J., Aaron, M., and B. Jones, "A Survey of Worldwide Censorship Techniques", 2015, <https://tools.ietf.org/html/draft-hall-censorship-tech-01>.

[freenet1]
Freenet, "What is Freenet?", n.d., <https://freenetproject.org/whatis.html>.

[freenet2]
Ian Clarke, ., "The Philosphy behind Freenet?", n.d., <https://freenetproject.org/philosophy.html>.

[greatfirewall]
Anonymous, ., "Towards a Comprehensive Picture of the Great Firewall's DNS Censorship", 2014, <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>.

[namecoin]
Namecoin, "Namecoin - Decentralized secure names", 2015, <https://namecoin.info/>.

[natusage]
Maier, G., Schneider, F., and A. Feldmann, "NAT usage in Residential Broadband networks", 2011, <http://www.icsi.berkeley.edu/pubs/networking/NATusage11.pdf>.

[quic] The Chromium Project, "QUIC, a multiplexed stream transport over UDP", 2014, <https://www.chromium.org/quic>.

[spdy] The Chromium Project, "SPDY - An experimental protocol for a faster web", 2009, <https://www.chromium.org/spdy/spdy-whitepaper>.

[spiegel] SPIEGEL, "Prying Eyes - Inside the NSA's War on Internet Security", 2014, <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>.

[techyum] Violet, ., "Official - vb.ly Link Shortener Seized by Libyan Government", 2010, <http://techyum.com/2010/10/official-vb-ly-link-shortener-seized-by-libyan-government/>.

[torproject]
The Tor Project, ., "Tor Project - Anonymity Online", 2007, <https://www.torproject.org/>.

[torrentfreak1]
Van der Sar, E., "Proposal for research on human rights protocol considerations", 2015, <https://torrentfreak.com/is-your-isp-messing-with-bittorrent-traffic-find-out-140123/>.

[torrentfreak2]
Andy, ., "LAWYERS SENT 109,000 PIRACY THREATS IN GERMANY DURING 2013", 2014, <https://torrentfreak.com/lawyers-sent-109000-piracy-threats-in-germany-during-2013-140304/>.

[turkey] Akguel, M. and M. Kirlidoğ, "Internet censorship in Turkey", 2015, <http://policyreview.info/articles/analysis/internet-censorship-turkey>.

[ververis]
Vasilis, V., Kargiotakis, G., Filasto, A., Fabian, B., and A. Alexandros, "Understanding Internet Censorship Policy - The Case of Greece", 2015, <https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-update.pdf>.

[wikileaks]
Sladek, T. and E. Broese, "Market Survey - Detection & Filtering Solutions to Identify File Transfer of Copyright Protected Content for Warner Bros. and movielabs", 2011, <https://wikileaks.org/sony/docs/05/docs/Anti-Piracy/CDSA/EANTC-Survey-1.5-unsecured.pdf>.

11.2. URIs

[1] mailto:node@domain/home

[2] mailto:node@domain/work

[3] mailto:hrpc@ietf.org

Authors’ Addresses

Joana Varon
Coding Rights

EMail: joana@codingrights.org

Niels ten Oever
Article19

EMail: niels@article19.org

Claudio Guarnieri
Centre for Internet and Human Rights

EMail: nex@nex.sx

Will Scott
University of Washington

EMail: wrs@cs.washington.edu

Corinne Cath
Oxford Internet Institute

EMail: corinne.cath@oii.ox.ac.uk