Human Rights Protocol Considerations Research Group G. Grover

Internet-Draft Centre for Internet and Society

Updates: 8280 (if approved) N. ten Oever

Intended status: Informational University of Amsterdam

Expires: 29 September 2022 28 March 2022

Guidelines for Human Rights Protocol and Architecture Considerations

draft-irtf-hrpc-guidelines-13

Abstract

This document sets guidelines for human rights considerations for

developers working on network protocols and architectures, similar to

the work done on the guidelines for privacy considerations [RFC6973].

This is an updated version of the guidelines for human rights

considerations in [RFC8280].

This document is not an Internet Standards Track specification; it is

published for informational purposes.

This informational document has consensus for publication from the

Internet Research Task Force (IRTF) Human Rights Protocol

Considerations Research Group. It has been reviewed, tried, and

tested by both by the research group as well as by researchers and

practitioners from outside the research group. The research group

acknowledges that the understanding of the impact of internet

protocols and architecture on society is a developing practice and is

a body of research that is still in development.

Status of This Memo

This Internet-Draft is submitted in full conformance with the

provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering

Task Force (IETF). Note that other groups may also distribute

working documents as Internet-Drafts. The list of current Internet-

Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months

and may be updated, replaced, or obsoleted by other documents at any

time. It is inappropriate to use Internet-Drafts as reference

material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 September 2022.

Grover & ten Oever Expires 29 September 2022 [Page 1]

Internet-Draft Guidelines for HRPC March 2022

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents (https://trustee.ietf.org/

license-info) in effect on the date of publication of this document.

Please review these documents carefully, as they describe your rights

and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as

described in Section 4.e of the Trust Legal Provisions and are

provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 3

2. Human rights threats . . . . . . . . . . . . . . . . . . . . 4

3. Conducting human rights reviews . . . . . . . . . . . . . . . 5

3.1. Analyzing drafts based on guidelines for a human rights

considerations model . . . . . . . . . . . . . . . . . . 6

3.2. Analyzing drafts based on their perceived or speculated

impact . . . . . . . . . . . . . . . . . . . . . . . . . 6

3.3. Expert interviews . . . . . . . . . . . . . . . . . . . . 6

3.4. Interviews with impacted persons and communities . . . . 6

3.5. Tracing impacts of implementations . . . . . . . . . . . 6

4. Guidelines for human rights considerations . . . . . . . . . 7

4.1. Connectivity . . . . . . . . . . . . . . . . . . . . . . 7

4.2. Reliability . . . . . . . . . . . . . . . . . . . . . . . 8

4.3. Content agnosticism . . . . . . . . . . . . . . . . . . . 9

4.4. Localization . . . . . . . . . . . . . . . . . . . . . . 10

4.5. Internationalization . . . . . . . . . . . . . . . . . . 11

4.6. Open Standards . . . . . . . . . . . . . . . . . . . . . 12

4.7. Heterogeneity Support . . . . . . . . . . . . . . . . . . 13

4.8. Integrity . . . . . . . . . . . . . . . . . . . . . . . . 14

4.9. Authenticity . . . . . . . . . . . . . . . . . . . . . . 15

4.10. Confidentiality . . . . . . . . . . . . . . . . . . . . . 16

4.11. Security . . . . . . . . . . . . . . . . . . . . . . . . 17

4.12. Privacy . . . . . . . . . . . . . . . . . . . . . . . . . 18

4.13. Pseudonymity . . . . . . . . . . . . . . . . . . . . . . 18

4.14. Anonymity . . . . . . . . . . . . . . . . . . . . . . . . 19

4.15. Censorship resistance . . . . . . . . . . . . . . . . . . 20

4.16. Outcome Transparency . . . . . . . . . . . . . . . . . . 21

4.17. Adaptability . . . . . . . . . . . . . . . . . . . . . . 22

4.18. Accessibility . . . . . . . . . . . . . . . . . . . . . . 23

4.19. Decentralization . . . . . . . . . . . . . . . . . . . . 24

4.20. Remedy . . . . . . . . . . . . . . . . . . . . . . . . . 25

4.21. Misc. considerations . . . . . . . . . . . . . . . . . . 25

Grover & ten Oever Expires 29 September 2022 [Page 2]

Internet-Draft Guidelines for HRPC March 2022

5. Document Status . . . . . . . . . . . . . . . . . . . . . . . 26

6. Acknowledgements . . . . . . . . . . . . . . . . . . . . . . 26

7. Security Considerations . . . . . . . . . . . . . . . . . . . 26

8. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 26

9. Research Group Information . . . . . . . . . . . . . . . . . 27

10. Informative References . . . . . . . . . . . . . . . . . . . 27

Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 33

1. Introduction

This document outlines a set of human rights protocol considerations

for protocol developers. It provides questions engineers should ask

themselves when developing or improving protocols if they want to

understand how their decisions can potentially influence the exercise

of human rights on the Internet. It should be noted that the impact

of a protocol cannot solely be deduced from its design, but its usage

and implementation should also be studied to form a full protocol

human rights impact assessment.

The questions are based on the research performed by the Human Rights

Protocol Considerations (hrpc) research group which has been

documented before these considerations. The research establishes

that human rights relate to standards and protocols, and offers a

common vocabulary of technical concepts that influence human rights

and how these technical concepts can be combined to ensure that the

Internet remains an enabling environment for human rights. With

this, the contours of a model for developing human rights protocol

considerations has taken shape.

This document is an iteration of the guidelines that can be found in

[RFC8280]. The methods for conducting human rights reviews

(Section 3.2), and guidelines for human rights considerations

(Section 3.3) in this document are being tested for relevance,

accuracy, and validity. The understanding of what human rights are

is based on the Universal Declaration of Human Rights [UDHR] and

subsequent treaties that jointly form the body of international human

rights law [UNHR].

This document does not provide a detailed taxonomy of the nature of

(potential) human rights violations, whether direct or indirect,

long-term or short-term, certain protocol choices might present. In

part because this is highly context-dependent, and in part, because

this document aims to provide a practical set of guidelines.

However, further research in this field would definitely benefit

developers and implementers.

This document is not an Internet Standards Track specification; it is

published for informational purposes.

Grover & ten Oever Expires 29 September 2022 [Page 3]

Internet-Draft Guidelines for HRPC March 2022

This informational document has consensus for publication from the

Internet Research Task Force (IRTF) Human Right Protocol

Considerations Research Group. It has been reviewed, tried, and

tested by both by the research group as well as by researchers and

practitioners from outside the research group. The research group

acknowledges that the understanding of the impact of internet

protocols and architecture on society is a developing practice and is

a body of research that is still in development.

2. Human rights threats

Threats to the exercise of human rights on the Internet come in many

forms. Protocols and standards may harm or enable the right to

freedom of expression, right to freedom of information, right to non-

discrimination, right to equal protection, right to participate in

cultural life, arts and science, right to freedom of assembly and

association, right to privacy, and the right to security. An end-

user who is denied access to certain services or content may be

unable to disclose vital information about the malpractices of a

government or other authority. A person whose communications are

monitored may be prevented or dissuaded from exercising their right

to freedom of association or participate in political processes

[Penney]. In a worst-case scenario, protocols that leak information

can lead to physical danger. A realistic example to consider is when

individuals perceived as threats to the state are subjected to

torture, extra-judicial killing or detention on the basis of

information gathered by state agencies through the monitoring of

network traffic.

This document presents several examples of how threats to human

rights materialize on the Internet. Work of this nature is called “modeling”. This threat modeling is inspired

by [RFC6973] Privacy Considerations for Internet Protocols, which is

based on security threat analysis. This method is a work in progress

and by no means a perfect solution for assessing human rights risks

in Internet protocols and systems. Certain specific human rights

threats are indirectly considered in Internet protocols as part of

the security considerations [BCP72], but privacy considerations

[RFC6973] or reviews, let alone human rights impact assessments of

Protocols, are not standardized nor implemented.

Many threats, enablers, and risks are linked to different rights.

This is not surprising if one takes into account that human rights

are interrelated, interdependent, and indivisible. Here, however,

we are not discussing all human rights because not all human rights

are relevant to Information and Communication Technologies (ICTs) in general and protocols and standards in

particular [Bless]: "The main source of the values of human rights is

the International Bill of Human Rights that is composed of the

Universal Declaration of Human Rights [UDHR] along with the

Grover & ten Oever Expires 29 September 2022 [Page 4]

Internet-Draft Guidelines for HRPC March 2022

International Covenant on Civil and Political Rights [ICCPR] and the

International Covenant on Economic, Social and Cultural Rights

[ICESCR]. In the light of several cases of Internet censorship, United Nations

Human Rights Council Resolution 20/8 was adopted in 2012, affirming

that "the same rights that people have offline must also be protected

online." [UNHRC2016] In 2015, the Charter of Human Rights and

Principles for the Internet [IRP] was developed and released.

According to these documents, some examples of human rights relevant

for ICT systems are human dignity (Art. 1 UDHR), non-discrimination

(Art. 2), rights to life, liberty and security (Art. 3), freedom of

opinion and expression (Art. 19), freedom of assembly and association

(Art. 20), rights to equal protection, legal remedy, fair trial, due

process, presumed innocent (Art. 7-11), appropriate social and

international order (Art. 28), participation in public affairs (Art.

21), participation in cultural life, protection of the moral and

material interests resulting from any scientific, literary or

artistic production of which [they are] the author (Art. 27), and

privacy (Art. 12)." A partial catalog of human rights related to

Information and Communications Technologies, including economic

rights, can be found in [Hill2014].

This is by no means an attempt to exclude specific rights or

prioritize some rights over others.

3. Conducting human rights reviews

Ideally, protocol developers and collaborators should incorporate

human rights considerations into the design process itself (see

Guidelines for human rights considerations). This section provides

guidance on how to conduct a human rights review, i.e., gauge the

impact or potential impact of a protocol or standard on human rights.

Human rights reviews can take place at different stages of the

development process of an Internet-Draft. Generally speaking, it is

easier to influence the development of a technology at earlier stages

than at later stages. This does not mean that reviews at last-call

are not relevant, but they are less likely to result in significant

changes in the reviewed document.

Methods for analyzing technology for specific human rights impacts

are still quite nascent. Currently, five methods have been explored

by the Human Rights Review Team, often in conjunction with each

other:

Grover & ten Oever Expires 29 September 2022 [Page 5]

Internet-Draft Guidelines for HRPC March 2022

3.1. Analyzing drafts based on guidelines for human rights

considerations model

This analysis of Internet-Drafts uses the model as described in

section 3.3. The outlined categories and questions can be used to

review an Internet-Draft. The advantage of this is that it provides

a known overview, and document authors can go back to this document

as well as [RFC8280] to understand the background and the context.

3.2. Analyzing drafts based on their perceived or speculated impact

When reviewing an Internet-Draft, specific human rights impacts can

become apparent by doing a close reading of the draft and seeking to

understand how it might affect networks or society. While less

structured than the straight use of the human rights considerations

model, this analysis may lead to new speculative understandings of

links between human rights and protocols.

3.3. Expert interviews

Interviews with document authors, active members of the Working

Group, or experts in the field can help explore the characteristics

of the protocol and its effects. There are two main advantages to

this approach: on the one hand, it allows the reviewer to gain a

deeper understanding of the (intended) workings of the protocol; on

the other hand, it also allows for the reviewer to start a discussion

with experts or even document authors, which can help the review gain

traction when it is published.

3.4. Interviews with impacted persons and communities

Protocols impact users of the Internet. Interviews can help the

reviewer understand how protocols affect the people that use the

protocols. Since human rights are best understood from the

perspective of the rights-holder, this approach will improve the

understanding of the real-world effects of the technology. At the

same time, it can be hard to attribute specific changes to a

particular protocol, this is of course even harder when a protocol

has not been (widely) deployed.

3.5. Tracing impacts of implementations

The reality of deployed protocols can be at odds with the

expectations during the protocol design and development phase

[RFC8980]. When a specification already has associated running code,

the code can be analyzed either in an experimental setting or on the

Internet where its impact can be observed. In contrast to reviewing

the draft text, this approach can allow the reviewer to understand

Grover & ten Oever Expires 29 September 2022 [Page 6]

Internet-Draft Guidelines for HRPC March 2022

how the specifications work in practice, and potentially what

unknown or unexpected effects the technology has.

4. Guidelines for human rights considerations

This section provides guidance for document authors in the form of a

questionnaire about protocols and how technical decisions can shape

the exercise of human rights. The questionnaire may be useful at any

point in the design process, particularly after the document authors

have developed a high-level protocol model as described in [RFC4101].

These guidelines do not seek to replace any existing referenced

specifications, but rather contribute to them and look at the design

process from a human rights perspective.

Protocols and Internet Standards might benefit from a documented

discussion of potential human rights risks arising from potential

misapplications of the protocol or technology described in the RFC.

This might be coupled with an Applicability Statement for that RFC.

Note that the guidance provided in this section does not recommend

specific practices. The range of protocols developed in the IETF is

too broad to make recommendations about particular uses of data or

how human rights might be balanced against other design goals.

However, by carefully considering the answers to the following

questions, document authors should be able to produce a comprehensive

analysis that can serve as the basis for discussion on whether the

protocol adequately takes specific human rights threats into account.

This guidance is meant to help the thought process of a human rights

analysis; it does not provide specific directions for how to write a

human rights considerations section (following the example set in

[RFC6973]).

In considering these questions, authors will need to be aware of the

potential of technical advances or the passage of time to undermine

protections. In general, considerations of rights are likely to be

more effective if they are considered given a purpose and specific

use cases, rather than as abstract absolute goals.

Also note that while the section uses the word, 'protocol', the

principles identified in these questions may be applicable to other

types of solutions (extensions to existing protocols, architecture

for solutions to specific problems, etc.).

4.1. Connectivity

Question(s): Does your protocol add application-specific functions to

intermediary nodes? Could this functionality be added to end nodes

instead of intermediary nodes?

Grover & ten Oever Expires 29 September 2022 [Page 7]

Internet-Draft Guidelines for HRPC March 2022

Is your protocol optimized for low bandwidth and high latency

connections? Could your protocol also be developed in a stateless

manner?

Explanation: The end-to-end principle [Saltzer] holds that certain

functions can and should be performed at 'ends' of the network.

[RFC1958] states "that in very general terms, the community believes

that the goal is connectivity [...] and the intelligence is end to

end rather than hidden in the network." Generally speaking, it is

easier to attain reliability of data transmissions with computation

at endpoints rather than at intermediary nodes.

Also considering the fact that network quality and conditions vary

across geography and time, it is also important to design protocols

such that they are reliable even on low bandwidth and high latency

connections.

Example: Encrypting connections, like done with HTTPS, can add a

significant network overhead and consequently make web resources less

accessible to those with low bandwidth and/or high latency

connections. [HTTPS-REL] Encrypting traffic is a net positive for

privacy and security, and thus protocol designers can acknowledge the

tradeoffs of connectivity made by such decisions.

Impacts:

\* Right to freedom of expression

\* Right to freedom of assembly and association

4.2. Reliability

Question(s): Is your protocol fault tolerant? Does it downgrade

gracefully, i.e., with mechanisms for fallback and/or notice? Can

your protocol resist malicious degradation attempts? Do you have a

documented way to announce degradation? Do you have measures in

place for recovery or partial healing from failure? Can your

protocol maintain dependability and performance in the face of

unanticipated changes or circumstances?

Explanation: Reliability and resiliency ensures that a protocol will

execute its function consistently and error resistant as described,

and function without unexpected result. Measures for reliability in

protocols assure users that their intended communication was

successfully executed.

Grover & ten Oever Expires 29 September 2022 [Page 8]

Internet-Draft Guidelines for HRPC March 2022

A system that is reliable degrades gracefully and will have a

documented way to announce degradation. It also will have mechanisms to

recover from failure gracefully, and if applicable, will allow for partial

healing.

It is important here to draw a distinction between random degradation

and malicious degradation. Many current attacks against TLS, for

example, exploit TLS' ability to gracefully downgrade to non-secure

cipher suites - from a functional perspective, this is useful; from a

security perspective, this can be disastrous. As with

confidentiality, the growth of the Internet and fostering innovation

in services depends on users having confidence and trust [RFC3724] in

the network. For reliability, it is necessary that services notify

the users if a delivery fails. In the case of real-time systems in

addition to the reliable delivery, the protocol needs to safeguard

timeliness.

Example: In the modern IP stack structure, a reliable transport layer

requires an indication that transport processing has successfully

completed, such as given by TCP's ACK message [RFC0793], and not

simply an indication from the Internet Protocol (IP) layer that the packet arrived.

Similarly, an application layer protocol may require an application-

specific acknowledgment that contains, among other things, a status

code indicating the disposition of the request (See [RFC3724]).

Impacts:

\* Right to freedom of expression

\* Right to security

4.3. Content agnosticism

Question(s): If your protocol impacts packet handling, does it use

user data (packet data that is not included in the header)? Is it

making decisions based on the payload of the packet? Does your

protocol prioritize certain content or services over others in the

routing process? Is the protocol transparent about the

prioritization that is made (if any)?

Explanation: Content agnosticism refers to the notion that network

traffic is treated identically regardless of payload, with some

exceptions where it comes to effective traffic handling, for instance

where it comes to delay-tolerant or delay-sensitive packets, based on

the header. If there is any prioritization based on the content or

metadata of the protocol, the protocol should be transparent about

such information and reasons thereof.

Grover & ten Oever Expires 29 September 2022 [Page 9]

Internet-Draft Guidelines for HRPC March 2022

Example: Content agnosticism prevents payload-based discrimination

against packets. This is important because changes to this principle

can lead to a two-tiered Internet, where certain packets are

prioritized over others on the basis of their content. Effectively

this would mean that although all users are entitled to receive their

packets at a certain speed, some users become more equal than others.

Impacts:

\* Right to freedom of expression

\* Right to non-discrimination

\* Right to equal protection

4.4. Localization

Question(s): Does your protocol uphold the standards of

internationalization? Have you made any concrete steps towards

localizing your protocol for relevant audiences?

Explanation: Localization refers to the adaptation of a product,

application or document content to meet the language, cultural and

other requirements of a specific target market (a locale)

[W3Ci18nDef]. For our purposes, it can be described as the practice

of translating an implementation to make it functional in a specific

language or for users in a specific locale (see

Internationalization).

Example: The Internet is a global medium, but many of its protocols

and products are developed with a certain audience in mind, that

often share particular characteristics like knowing how to read and

write in ASCII and knowing English. This limits the ability of a

large part of the world's online population from using the Internet

in a way that is culturally and linguistically accessible. An

example of a protocol that has taken into account the view that

individuals like to have access to data in their native language can

be found in [RFC5646]. This protocol labels the information content

with an identifier for the language in which it is written. And this

allows information to be presented in more than one language.

Impacts:

\* Right to non-discrimination

\* Right to participate in cultural life, arts and science

\* Right to freedom of expression

Grover & ten Oever Expires 29 September 2022 [Page 10]

Internet-Draft Guidelines for HRPC March 2022

4.5. Internationalization

Question(s): Does your protocol or specification define text string

elements, in the payload or headers, that have to be understood or

entered by humans? Does your specification allow Unicode? If so, do

you accept texts in one charset (which must be UTF-8), or several

(which is dangerous for interoperability)? If character sets or

encodings other than UTF-8 are allowed, does your specification

mandate a proper tagging of the charset? Did you have a look at

[RFC6365]?

Explanation: Internationalization refers to the practice of making

protocols, standards, and implementations usable in different

languages and scripts (see Localization). In the IETF,

internationalization means to add or improve the handling of non-

ASCII text in a protocol. [RFC6365] A different perspective, more

appropriate to protocols that are designed for global use from the

beginning, is the definition used by W3C:

"Internationalization is the design and development of a

product, application or document content that enables easy

localization for target audiences that vary in culture, region,

or language." {{W3Ci18nDef}}

Many protocols that handle text only handle one charset (US-ASCII),

or leave the question of what coded character set and encoding are

used up to local guesswork (which leads, of course, to

interoperability problems). If multiple charsets are permitted, they

must be explicitly identified [RFC2277]. Adding non-ASCII text to a

protocol allows the protocol to handle more scripts, hopefully

representing users across the world. In today's world, that is

normally best accomplished by allowing Unicode encoded in UTF-8 only.

In the current IETF policy [RFC2277], internationalization is aimed

at user-facing strings, not protocol elements, such as the verbs used

by some text-based protocols. (Do note that some strings are both

content and protocol elements, such as identifiers.) Given the

IETF's mission to make the Internet a global network of networks,

[RFC3935] developers should ensure that protocols work with languages

apart from English and character sets apart from Latin characters.

It is therefore crucial that at the very least, the content carried

by the protocol can be in any script, and that all scripts are

treated equally.

Example: See localization

Impacts:

Grover & ten Oever Expires 29 September 2022 [Page 11]

Internet-Draft Guidelines for HRPC March 2022

\* Right to freedom of expression

\* Right to political participation

\* Right to participate in cultural life, arts and science

4.6. Open Standards

Question(s): Is your protocol fully documented in a way that it could

be easily implemented, improved, built upon and/or further developed?

Do you depend on proprietary code for the implementation, running or

further development of your protocol? Does your protocol favor a

particular proprietary specification over technically-equivalent

competing specification(s), for instance by making any incorporated

vendor specification "required" or "recommended" [RFC2026]? Do you

normatively reference another standard that is not available without

cost (and could you do without it)? Are you aware of any patents

that would prevent your standard from being fully implemented

[RFC8179] [RFC6701]?

Explanation: The Internet was able to be developed into the global

network of networks because of the existence of open, non-proprietary

standards [Zittrain]. They are crucial for enabling

interoperability. Yet, open standards are not explicitly defined

within the IETF. On the subject, [RFC2026] states: "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 at the IETF. 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." Similarly, [RFC3935] does not define open standards but

does emphasize the importance of an "open process", i.e., "any

interested person can participate in the work, know what is being

decided, and make his or her voice heard on the issue."

Open standards (and open-source software) allow users to glean

information about how the tools they are using work, including the

tools' security and privacy properties. They additionally allow for

permissionless innovation, which is important to maintain the freedom

and ability to freely create and deploy new protocols on top of the

communications constructs that currently exist. It is at the heart

of the Internet as we know it, and to maintain its fundamentally open

nature, we need to be mindful of the need for developing open

standards.

Grover & ten Oever Expires 29 September 2022 [Page 12]

Internet-Draft Guidelines for HRPC March 2022

All standards that need to be normatively implemented should be

freely available and with reasonable protection for patent

infringement claims, so it can also be implemented in open source or

free software. Patents have often held back open standardization or

been used against those deploying open standards, particularly in the

domain of cryptography [newegg]. An exemption of this is sometimes

made when a protocol is standardized that normatively relies on

specifications produced by others Standards Development Organizations (SDOs) that are not freely available.

Patents in open standards or in normative references to other

standards should have a patent disclosure [notewell], royalty-free

licensing [patentpolicy], or some other form of fair, reasonable and

non-discriminatory terms.

Example: [RFC6108] describes a system for providing critical end-user

notifications to web browsers, which has been deployed by Comcast, an

Internet Service Provider (ISP). Such a notification system is being

used to provide near-immediate notifications to customers, such as to

warn them that their traffic exhibits patterns that are indicative of

malware or virus infection. There are other proprietary systems that

can perform such notifications, but those systems utilize Deep Packet

Inspection (DPI) technology. In contrast, that document describes a

system that does not rely upon DPI, and is instead based on open IETF

standards and open-source applications.

Impacts:

\* Right to freedom of expression

\* Right to participate in cultural life, arts and science

4.7. Heterogeneity Support

Question(s): Does your protocol support heterogeneity by design?

Does your protocol allow for multiple types of hardware? Does your

protocol allow for multiple types of application protocols? Is your

protocol liberal in what it receives and handles? Will it remain

usable and open if the context changes?

Grover & ten Oever Expires 29 September 2022 [Page 13]

Internet-Draft Guidelines for HRPC March 2022

Explanation: 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, the

heterogeneity principle proposed in [RFC1958] needs to be supported

by design [FIArch].

Heterogeneity support in protocols can thus enable a wide range of

devices and (by extension) users to participate on the network.

Example: Heterogeneity is inevitable and needs be supported by

design. Multiple types of hardware must be allowed for, e.g.,

transmission speeds differing by at least 7 orders of magnitude,

various computer word lengths, and hosts ranging from memory-starved

microprocessors up to massively parallel supercomputers. Multiple

types of application protocols must be allowed for, ranging from the

simplest such as remote login up to the most complex such as commit

protocols for distributed databases. [RFC1958].

Impacts:

\* Right to freedom of expression

\* Right to political participation

4.8. Integrity

Question(s): Does your protocol maintain, assure and/or verify the

accuracy of payload data? Does your protocol maintain and assure the

consistency of data? Does your protocol in any way allow for the

data to be (intentionally or unintentionally) altered?

Explanation: Integrity refers to the maintenance and assurance of the

accuracy and consistency of data to ensure it has not been

(intentionally or unintentionally) altered.

Example: Integrity verification of data is important to prevent

vulnerabilities and attacks from on-path attackers. These attacks

happen when a third party (often for malicious reasons) intercepts a

communication between two parties, inserting themselves in the middle

changing the content of the data. In practice this looks as follows:

Grover & ten Oever Expires 29 September 2022 [Page 14]

Internet-Draft Guidelines for HRPC March 2022

Alice wants to communicate with Bob. Corinne forges and sends a

message to Bob, impersonating Alice. Bob cannot see that the data from

Alice was altered by Corinne. Corinne intercepts and alters the

communication as it is sent between Alice and Bob. Corinne is able

to control the communication content.

Impacts:

\* Right to freedom of expression

\* Right to security

4.9. Authenticity

Question(s): Do you have sufficient measures to confirm the truth of

an attribute of a single piece of data or entity? Can the attributes

get garbled along the way (see security)? If relevant, have you

implemented IPsec, DNSsec, HTTPS and other Standard Security Best

Practices?

Explanation: Authenticity ensures that data does indeed come from the

source it claims to come from. This is important to prevent certain

attacks or unauthorized access and use of data.

At the same time, authentication should not be used as a way to

prevent heterogeneity support, as is often done for vendor lock-in or

digital rights management.

Example: Authentication of data is important to prevent

vulnerabilities, and attacks from on-path attackers. These attacks

happen when a third party (often for malicious reasons) intercepts a

communication between two parties, inserting themselves in the middle

and posing as both parties. In practice this looks as follows:

Alice wants to communicate with Bob. Alice sends data to Bob.

Corinne intercepts the data sent to Bob. Corinne reads (and

potentially alters) the message to Bob. Bob cannot see that the data did

not come from Alice but from Corinne.

When there is proper authentication the scenario would be as follows:

Alice wants to communicate with Bob. Alice sends data to Bob.

Corinne intercepts the data sent to Bob. Corinne reads and alters

the message to Bob. Bob can see that the data did not come from Alice.

Impacts:

\* Right to privacy

Grover & ten Oever Expires 29 September 2022 [Page 15]

Internet-Draft Guidelines for HRPC March 2022

\* Right to freedom of expression

\* Right to security

4.10. Confidentiality

Question(s): Does this protocol expose the transmitted data over the

wire? Does the protocol expose information related to identifiers or

data? If so, does it do so to each other protocol entity (i.e.,

recipients, intermediaries, and enablers) [RFC6973]? What options

exist for protocol implementers to choose to limit the information

shared with each entity? What operational controls are available to

limit the information shared with each entity?

What controls or consent mechanisms does the protocol define or

require before personal data or identifiers are shared or exposed via

the protocol? If no such mechanisms or controls are specified, is it

expected that control and consent will be handled outside of the

protocol?

Does the protocol provide ways for initiators to share different

pieces of information with different recipients? If not, are there

mechanisms that exist outside of the protocol to provide initiators

with such control?

Does the protocol provide ways for initiators to limit the sharing or

express individuals' preferences to recipients or intermediaries with

regard to the collection, use, or disclosure of their personal data?

If not, are there mechanisms that exist outside of the protocol to

provide users with such control? Is it expected that users will have

relationships that govern the use of the information (contractual or

otherwise) with those who operate these intermediaries? Does the

protocol prefer encryption over clear text operation?

Explanation: Confidentiality refers to keeping your data secret from

unintended listeners [BCP72]. The growth of the Internet depends on

users having confidence that the network protects their personal data

[RFC1984]. The possibility of pervasive monitoring and surveillance

undermines users' trust, and can be mitigated by ensuring

confidentiality, i.e., passive attackers should gain little or no

information from observation or inference of protocol activity.

[RFC7258][RFC7624].

Example: Protocols that do not encrypt their payload make the entire

content of the communication available to the idealized attacker

along their path. Following the advice in [RFC3365], most such

protocols have a secure variant that encrypts the payload for

confidentiality, and these secure variants are seeing ever-wider

Grover & ten Oever Expires 29 September 2022 [Page 16]

Internet-Draft Guidelines for HRPC March 2022

deployment. A noteworthy exception is DNS [RFC1035], as DNSSEC

[RFC4033] does not have confidentiality as a requirement. This

implies that, in the absence of the use of more recent standards like

DNS over TLS [RFC7858] or DNS over HTTPS [RFC8484], all DNS queries

and answers generated by the activities of any protocol are available

to the attacker. When store-and-forward protocols are used (e.g.,

SMTP [RFC5321]), intermediaries leave this data subject to

observation by an attacker that has compromised these intermediaries,

unless the data is encrypted end-to-end by the application-layer

protocol or the implementation uses an encrypted store for this data

[RFC7624].

Impacts:

\* Right to privacy

\* Right to security

4.11. Security

Question(s): Did you have a look at Guidelines for Writing RFC Text

on Security Considerations [BCP72]? Have you found any attacks that

are somewhat related to your protocol/specification, yet considered

out of scope of your document? Would these attacks be pertinent to

the human rights enabling features of the Internet (as described

throughout this document)?

Explanation: Security is not a single monolithic property of a

protocol or system, but rather a series of related but somewhat

independent properties. Not all of these properties are required for

every application. Since communications are carried out by systems

and access to systems is through communications channels, security

goals obviously interlock, but they can also be independently

provided. [BCP72].

Typically, any protocol operating on the internet can be the target

of passive attacks (when the attacker can access and read packets on

the network); active attacks (when an attacker is capable of writing

information to the network packets). [BCP72]

Example: See [BCP72].

Impacts:

\* Right to freedom of expression

\* Right to freedom of assembly and association

Grover & ten Oever Expires 29 September 2022 [Page 17]

Internet-Draft Guidelines for HRPC March 2022

\* Right to non-discrimination

\* Right to security

4.12. Privacy

Question(s): Did you have a look at the Guidelines in the Privacy

Considerations for Internet Protocols [RFC6973] section 7? Does your

protocol maintain the confidentiality of metadata? Could your

protocol counter traffic analysis? Does your protocol adhere to data

minimization principles? Does your document identify potentially

sensitive data logged by your protocol and/or for how long that needs

to be retained for technical reasons?

Explanation: Privacy refers to the right of an entity (normally a

person), acting on 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]. If a protocol provides insufficient privacy protection it

may have a negative impact on freedom of expression as users self-

censor for fear of surveillance, or find themselves unable to express

themselves freely.

Example: See [RFC6973]

Impacts:

\* Right to freedom of expression

\* Right to non-discrimination

4.13. Pseudonymity

Question(s): Does the protocol collect personally derived data? Does

the protocol generate or process anything that can be, or be tightly

correlated with, personally identifiable information? Does the

protocol utilize data that is personally-derived, i.e., derived from

the interaction of a single person, or their device or address? If

yes, can the protocol be implemented in a way that does not rely on

personally identifiable information? If not, does the specification

describe how any such data be handled? Have you considered the

Privacy Considerations for Internet Protocols [RFC6973], especially

section 6.1.2?

Explanation: Pseudonymity means using a pseudonym instead of one's

"real" name. There are many reasons for users to use pseudonyms, for

instance to: hide their gender, protect themselves against

harassment, protect their families' privacy, frankly discuss

Grover & ten Oever Expires 29 September 2022 [Page 18]

Internet-Draft Guidelines for HRPC March 2022

sexuality, or develop an artistic or journalistic persona without

repercussions from an employer, (potential) customers, or social

surrounding. [geekfeminism] The difference between anonymity and

pseudonymity is that a pseudonym often is persistent. "Pseudonymity

is strengthened when less personal data can be linked to the

pseudonym; when the same pseudonym is used less often and across

fewer contexts; and when independently chosen pseudonyms are more

frequently used for new actions (making them, from an observer's or

attacker's perspective, unlinkable)." [RFC6973]

Pseudonymity - the ability to use a persistent identifier not linked

to one's offline identity - is an important feature for many end-

users, as it allows them different degrees of disguised identity and

privacy online. This can allow an enabling environment for users to

exercise other rights, including freedom of expression and political

participation, without fear or direct identification or

discrimination.

Example: Generally, pseudonymous identifiers cannot be simply reverse

engineered. Some early approaches took approaches such as simple

hashing of IP addresses, but these could then be simply reversed by

generating a hash for each potential IP address and comparing it to

the pseudonym.

Example: There are also efforts for application layer protocols, like

Oblivious DNS Over HTTPS, [draft-pauly-dprive-oblivious-doh] that can

separate identifiers from requests.

Impacts:

\* Right to non-discrimination

\* Right to freedom of expression

\* Right to political participation

\* Right to freedom of assembly and association

4.14. Anonymity

Question(s): Does your protocol make use of persistent identifiers?

Can it be done without them? Did you have a look at the Privacy

Considerations for Internet Protocols [RFC6973], especially section

6.1.1 of that document?

Explanation: Anonymity refers to the condition of an identity being

unknown or concealed [RFC4949]. Even though full anonymity is hard

to achieve, it is a non-binary concept. Making pervasive monitoring

Grover & ten Oever Expires 29 September 2022 [Page 19]

Internet-Draft Guidelines for HRPC March 2022

and tracking harder is important for many users as well as for the

IETF [RFC7258]. Achieving a higher level of anonymity is an

important feature for many end-users, as it allows them different

degrees of privacy online. Anonymity is an inherent part of the

right to freedom of opinion and expression and the right to privacy.

Avoid adding identifiers, options or configurations that create or

might lead to patterns or regularities that are not explicitly

required by the protocol.

If your protocol collects data and seeks to distribute it to more

entities than the originally-intended recipients (see [RFC6235] as

an example), you should anonymize the data, but keep in mind that

"anonymizing" data is notoriously hard. For example, just dropping

the last byte of an IP address does not "anonymize" data.

If your protocol allows for identity management, there should be a

clear barrier between the identities to ensure that they cannot

(easily) be associated with each other.

A protocol that uses data that could help identify a sender (items of

interest) should be protected from third parties. For instance, if

one wants to hide the source/destination IP addresses of a packet,

the use of IPsec in tunneling mode (e.g., inside a virtual private

network) can be helpful to protect from third parties likely to

eavesdrop packets exchanged between the tunnel endpoints.

Example: An example is DHCP where sending a persistent identifier as

the client name was not mandatory but, in practice, done by many

implementations, before [RFC7844].

Impacts:

\* Right to non-discrimination

\* Right to political participation

\* Right to freedom of assembly and association

\* Right to security

4.15. Censorship resistance

Question(s): Can your protocol contribute to filtering? Could your protocol be

implemented to censor data or services? Could it be designed to

ensure this doesn't happen? Does your protocol make it apparent or

transparent when access to a resource is restricted and the reasons why it is restricted

? Does your protocol introduce new identifiers or re-use

existing identifiers (e.g., MAC addresses) that might be associated

Grover & ten Oever Expires 29 September 2022 [Page 20]

Internet-Draft Guidelines for HRPC March 2022

with persons or content?

Explanation: Governments and service providers block or filter

content or traffic, often without the knowledge of end-users.

[RFC7754] See [draft-irtf-pearg-censorship] for a survey of

censorship techniques employed across the world, which lays out

protocol properties that have been exploited to censor access to

information. Censorship resistance refers to the methods and

measures to prevent Internet censorship.

Example: Identifiers of content exposed within a protocol might be

used to facilitate censorship, as in the case of Application Layer

based censorship, which affects protocols like HTTP. In HTTP, denial

or restriction of access can be made apparent by the use of status

code 451, which allows server operators to operate with greater

transparency in circumstances where issues of law or public policy

affect their operation [RFC7725].

If a protocol potentially enables censorship, protocol designers

should strive towards creating error codes that capture different

scenarios (blocked due to administrative policy, unavailable because

of legal requirements, etc.) to minimize ambiguity for end-users.

In the development of the IPv6 protocol, it was discussed to embed a

Media Access Control (MAC) address into unique IP addresses. This

would make it possible for eavesdroppers and other information

collectors to identify when different addresses used in different

transactions actually correspond to the same node. This is why

standardisation efforts like Privacy Extensions for Stateless Address

Autoconfiguration in IPv6 [RFC4941] and MAC address randomization

[draft-zuniga-mac-address-randomization] have been pursued.

Impacts:

\* Right to freedom of expression

\* Right to political participation

\* Right to participate in cultural life, arts, and science

\* Right to freedom of assembly and association

4.16. Outcome Transparency

Question(s): Are the effects of your protocol fully and easily

comprehensible, including with respect to unintended consequences of

protocol choices?

Grover & ten Oever Expires 29 September 2022 [Page 21]

Internet-Draft Guidelines for HRPC March 2022

Explanation: Certain technical choices may have unintended

consequences.

Example: Lack of authenticity may lead to lack of integrity and

negative externalities, of which spam is an example. Lack of data

that could be used for billing and accounting can lead to so-called

"free" arrangements which obscure the actual costs and distribution

of the costs, for example the barter arrangements that are commonly

used for Internet interconnection; and the commercial exploitation of

personal data for targeted advertising which is the most common

funding model for the so-called "free" services such as search

engines and social networks. Other unexpected outcomes might not be

technical, but rather architectural, social or economic.

Impacts:

\* Right to freedom of expression

\* Right to privacy

\* Right to freedom of assembly and association

\* Right to access to information

4.17. Adaptability

Question(s): Is your protocol written in such a way that it would be

easy for other protocols to be developed on top of it, or to interact

with it? Does your protocol impact permissionless innovation? (See

Open Standards)

Explanation: Adaptability is closely interrelated with permissionless

innovation: both maintain the freedom and ability to freely create

and deploy new protocols on top of the communications constructs that

currently exist. It is at the heart of the Internet as we know it,

and to maintain its fundamentally open nature, we need to be mindful

of the impact of protocols on maintaining or reducing permissionless

innovation to ensure the Internet can continue to develop.

Grover & ten Oever Expires 29 September 2022 [Page 22]

Internet-Draft Guidelines for HRPC March 2022

Adaptability and permissionless innovation can be used to shape

information networks as preferenced by groups of users. Furthermore,

a precondition of adaptability is the ability of the people who can

adapt the network to be able to know and understand the network.

This is why adaptability and permissionless innovation are inherently

connected to the right to education and the right to science as well

as the right to freedom of assembly and association as well as the

right to freedom of expression. Since it allows the users of the

network to determine how to assemble, collaborate, and express

themselves.

Example: WebRTC generates audio and/or video data. In order to

ensure that WebRTC can be used in different locations by different

parties, it is important that standard Javascript APIs are developed

to support applications from different voice service providers.

Multiple parties will have similar capabilities, in order to ensure

that all parties can build upon existing standards these need to be

adaptable, and allow for permissionless innovation.

Impacts:

\* Right to education

\* Right to science

\* Right to freedom of expression

\* Right to freedom of assembly and association

4.18. Accessibility

Question(s): Is your protocol designed to provide an enabling

environment for all? Have you looked at the W3C Web Accessibility

Initiative for examples and guidance?

Explanation: Sometimes in the design of protocols, websites, web

technologies, or web tools, barriers are created that exclude people

from using the Web. The Internet should be designed to work for all

people, whatever their hardware, software, language, culture,

location, or physical or mental ability. When the Internet

technologies meet this goal, it will be accessible to people with a

diverse range of hearing, movement, sight, and cognitive ability.

[W3CAccessibility]

Example: The HTML protocol as defined in [HTML5] specifically

requires that every image must have an alt attribute (with a few

exceptions) to ensure images are accessible for people that cannot

themselves decipher non-text content in web pages.

Grover & ten Oever Expires 29 September 2022 [Page 23]

Internet-Draft Guidelines for HRPC March 2022

Another example is the work that is done in the AVT and AVTCORE

working groups in the IETF that enable text conversation in

multimedia, text telephony, wireless multimedia and video

communications for sign language and lip-reading (i.e.. [RFC9071]).

Impacts:

\* Right to non-discrimination

\* Right to freedom of assembly and association

\* Right to education

\* Right to political participation

4.19. Decentralization

Question(s): Can your protocol be implemented without a single point

of control? If applicable, can your protocol be deployed in a

federated manner? Does your protocol create additional centralized

points of control?

Explanation: Decentralization is one of the central technical

concepts of the architecture of the Internet, and is embraced as such

by the IETF [RFC3935]. It refers to the absence or minimization of

centralized points of control, a feature that is assumed to make it

easy for new users to join and new uses to unfold [Brown]. It also

reduces issues surrounding single points of failure, and distributes

the network such that it continues to function even if one or several

nodes are disabled. With the commercialization of the Internet in

the early 1990s, there has been a slow move away from

decentralization, to the detriment of the technical benefits of

having a decentralized Internet. For a more detailed discussion of

this topic, please see [arkkoetal].

Example: The bits traveling the Internet are increasingly susceptible

to monitoring and censorship, from both governments and Internet

service providers, as well as third (malicious) parties. The ability

to monitor and censor is further enabled by the increased

centralization of the network that creates central infrastructure

points that can be tapped into. The creation of peer-to-peer

networks and the development of voice-over-IP (VoIP) protocols using peer-

to-peer technology in combination with distributed hash table (DHT)

for scalability are examples of how protocols can preserve

decentralization [Pouwelse].

Impacts:

Grover & ten Oever Expires 29 September 2022 [Page 24]

Internet-Draft Guidelines for HRPC March 2022

\* Right to freedom of expression

\* Right to freedom of assembly and association

4.20. Remedy

Question(s): Can your protocol facilitate a negatively impacted

party's right to remedy without disproportionately impacting other

parties' human rights, especially their right to privacy?

Explanation: Providing access to remedy by states and corporations is

a part of the UN Guiding Principles on Business and Human Rights

[UNGP]. Access to remedy may help victims of human rights violations

in seeking justice, or allow law enforcement agencies to identify a

possible violator. However, mechanisms in protocols that try to

enable 'attribution' to individuals will impede the exercise of the

right to privacy. The former Special Rapporteur for Freedom of

Expression has also argued that anonymity is an inherent part of

freedom of expression [Kaye]. Considering the potential adverse

impact of attribution on the right to privacy and freedom of

expression, enabling attribution on an individual level is most

likely not consistent with human rights.

Example: Adding personally identifiable information (PII) to data streams

might help in identifying a violator of human rights and provide

access to remedy, but this would disproportionally affect all users’

right to privacy, anonymous expression, and association.

Impacts:

\* Right to remedy

\* Right to security

\* Right to privacy

4.21. Misc. considerations

Question(s): Have you considered potential negative consequences

(individual or societal) that your protocol or document might have?

Explanation: Publication of a particular RFC under a certain status

has consequences. Publication as an Internet Standard as part of the

Standards Track may signal to implementers that the specification has

a certain level of maturity, operational experience, and consensus.

Similarly, publication of a specification of an experimental document as

part of the non-standards track would signal to the community that

the document "may be intended for eventual standardization but [may]

Grover & ten Oever Expires 29 September 2022 [Page 25]

Internet-Draft Guidelines for HRPC March 2022

not yet [be] ready" for wide deployment. The extent of the

deployment, and consequently its overall impact on end-users, may

depend on the document status presented in the RFC. See [BCP9] and

updates to it for a fuller explanation.

5. Document Status

This RG document currently documents best practices and

guidelines for human rights reviews of network protocols,

architectures and other Internet-Drafts and RFCs.

6. Acknowledgements

Thanks to:

\* Corinne Cath-Speth for work on [RFC8280].

\* Theresa Engelhard, Joe Hall, Avri Doria, Joey Salazar, Corinne

Cath-Speth, Farzaneh Badii, Sandra Braman, Colin Perkins, John

Curran, Eliot Lear, Mallory Knodel, and the hrpc list for reviews

and suggestions.

\* Individuals who conducted human rights reviews for their work and

feedback: Amelia Andersdotter, Beatrice Martini, Karan Saini and

Shivan Kaul Sahib.

7. Security Considerations

Article three of the Universal Declaration of Human Rights reads:

"Everyone has the right to life, liberty and security of person.".

This article underlines the importance of security and its

interrelation with human life and liberty, but since human rights are

indivisible, interrelated and interdependent, security is also

closely linked to other human rights and freedoms. This document

seeks to strengthen human rights, freedoms, and security by relating

and translating these concepts to concepts and practices as they are

used in Internet protocol and architecture development. The aim of

this is to secure human rights and thereby improve the sustainability,

usability, and effectiveness of the network. The document seeks to

achieve this by providing guidelines as done in section three of this

document.

8. IANA Considerations

This document has no actions for IANA.

Grover & ten Oever Expires 29 September 2022 [Page 26]

Internet-Draft Guidelines for HRPC March 2022

9. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations

Research Group is located at the e-mail address hrpc@ietf.org

(mailto:hrpc@ietf.org). Information on the group and information on

how to subscribe to the list is at

https://www.irtf.org/mailman/listinfo/hrpc

(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 (https://www.irtf.org/mail-

archive/web/hrpc/current/index.html)

10. Informative References

[arkkoetal]

Arkko, J., Trammell, B., Notthingham, M., Huitema, C.,

Thomson, M., Tantsure, J., and N. ten Oever,

"Considerations on Internet Consolidation and the Internet

Architecture", 2019,

<https://datatracker.ietf.org/doc/html/draft-arkko-iab-

internet-consolidation-02>.

[BCP72] IETF, "Guidelines for Writing RFC Text on Security

Considerations", 2003,

<https://datatracker.ietf.org/doc/bcp72/>.

[BCP9] Bradner, S. and IETF, "The Internet Standards Process --

Revision 3", 1996,

<https://datatracker.ietf.org/doc/rfc2026/>.

[Bless] Bless, R. and C. Orwat, "Values and Networks", 2015.

[Brown] Brown, I. and M. Ziewitz, "A Prehistory of Internet

Governance", Research Handbook on Governance of the

Internet. Cheltenham, Edward Elgar, 2013.

[draft-irtf-pearg-censorship]

Hall, J., Aaron, M., Adams, S., Jones, B., and N.

Feamster, "A Survey of Worldwide Censorship Techniques",

2020,

<https://tools.ietf.org/html/draft-irtf-pearg-censorship>.

[draft-pauly-dprive-oblivious-doh]

Kinnear, E., McManus, P., Pauly, T., Verma, T., and C.A.

Wood, "Oblivious DNS Over HTTPS", 2022,

<https://tools.ietf.org/html/draft-pauly-dprive-oblivious-

doh>.

Grover & ten Oever Expires 29 September 2022 [Page 27]

Internet-Draft Guidelines for HRPC March 2022

[draft-zuniga-mac-address-randomization]

Zuniga, JC., Bernardos, CJ., and A. Andersdotter, "MAC

address randomization", 2020,

<https://tools.ietf.org/html/draft-irtf-pearg-censorship>.

[FIArch] "Future Internet Design Principles", January 2012,

<http://www.future-internet.eu/uploads/media/

FIArch\_Design\_Principles\_V1.0.pdf>.

[geekfeminism]

Geek Feminism Wiki, "Pseudonymity", 2015,

<http://geekfeminism.wikia.com/wiki/Pseudonymity>.

[Hill2014] Hill, R., "Partial Catalog of Human Rights Related to ICT

Activities", 2014,

<http://www.apig.ch/UNIGE%20Catalog.pdf>.

[HTML5] W3C, "HTML5", 2014, <https://www.w3.org/TR/html5/>.

[HTTPS-REL]

Meyer, E., "Securing Web Sites Made Them Less Accessible",

2018, <https://meyerweb.com/eric/thoughts/2018/08/07/

securing-sites-made-them-less-accessible/>.

[ICCPR] United Nations General Assembly, "International Covenant

on Civil and Political Rights", 1976,

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

CCPR.aspx>.

[ICESCR] United Nations General Assembly, "International Covenant

on Economic, Social and Cultural Rights", 1966,

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

CESCR.aspx>.

[IRP] Internet Rights and Principles Dynamic Coalition, "10

Internet Rights & Principles", 2014,

<http://internetrightsandprinciples.org/site/wp-

content/uploads/2014/06/

IRPC\_10RightsandPrinciples\_28May2014-11.pdf>.

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

communications", 2015,

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

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

Grover & ten Oever Expires 29 September 2022 [Page 28]

Internet-Draft Guidelines for HRPC March 2022

[newegg] Mullin, J., "Newegg on trial: Mystery company TQP rewrites

the history of encryption", 2013, <http://arstechnica.com/

tech-policy/2013/11/newegg-on-trial-mystery-company-tqp-

re-writes-the-history-of-encryption/>.

[notewell] IETF, "Note Well", 2015,

<https://www.ietf.org/about/note-well.html>.

[patentpolicy]

W3C, "W3C Patent Policy", 2004,

<https://www.w3.org/Consortium/Patent-Policy-20040205/>.

[Penney] Penney, J., "Chilling Effects: Online Surveillance and

Wikipedia Use", 2016, <http://papers.ssrn.com/sol3/

papers.cfm?abstract\_id=2769645>.

[Pouwelse] Pouwelse, Ed, J., "Media without censorship", 2012,

<https://tools.ietf.org/html/draft-pouwelse-censorfree-

scenarios>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7,

RFC 793, DOI 10.17487/RFC0793, September 1981,

<https://www.rfc-editor.org/info/rfc793>.

[RFC1035] Mockapetris, P., "Domain names - implementation and

specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,

November 1987, <https://www.rfc-editor.org/info/rfc1035>.

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

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

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

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic

Technology and the Internet", BCP 200, RFC 1984,

DOI 10.17487/RFC1984, August 1996,

<https://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,

<https://www.rfc-editor.org/info/rfc2026>.

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

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

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

Grover & ten Oever Expires 29 September 2022 [Page 29]

Internet-Draft Guidelines for HRPC March 2022

[RFC3365] Schiller, J., "Strong Security Requirements for Internet

Engineering Task Force Standard Protocols", BCP 61,

RFC 3365, DOI 10.17487/RFC3365, August 2002,

<https://www.rfc-editor.org/info/rfc3365>.

[RFC3724] Kempf, J., Ed., 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,

<https://www.rfc-editor.org/info/rfc3724>.

[RFC3935] Alvestrand, H., "A Mission Statement for the IETF",

BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004,

<https://www.rfc-editor.org/info/rfc3935>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.

Rose, "DNS Security Introduction and Requirements",

RFC 4033, DOI 10.17487/RFC4033, March 2005,

<https://www.rfc-editor.org/info/rfc4033>.

[RFC4101] Rescorla, E., and IAB, "Writing Protocol Models", RFC 4101,

DOI 10.17487/RFC4101, June 2005,

<https://www.rfc-editor.org/info/rfc4101>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy

Extensions for Stateless Address Autoconfiguration in

IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007,

<https://www.rfc-editor.org/info/rfc4941>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2",

FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007,

<https://www.rfc-editor.org/info/rfc4949>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,

DOI 10.17487/RFC5321, October 2008,

<https://www.rfc-editor.org/info/rfc5321>.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying

Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646,

September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[RFC6108] Chung, C., Kasyanov, A., Livingood, J., Mody, N., and B.

Van Lieu, "Comcast's Web Notification System Design",

RFC 6108, DOI 10.17487/RFC6108, February 2011,

<https://www.rfc-editor.org/info/rfc6108>.

Grover & ten Oever Expires 29 September 2022 [Page 30]

Internet-Draft Guidelines for HRPC March 2022

[RFC6235] Boschi, E. and B. Trammell, "IP Flow Anonymization

Support", RFC 6235, DOI 10.17487/RFC6235, May 2011,

<https://www.rfc-editor.org/info/rfc6235>.

[RFC6365] Hoffman, P. and J. Klensin, "Terminology Used in

Internationalization in the IETF", BCP 166, RFC 6365,

DOI 10.17487/RFC6365, September 2011,

<https://www.rfc-editor.org/info/rfc6365>.

[RFC6701] Farrel, A. and P. Resnick, "Sanctions Available for

Application to Violators of IETF IPR Policy", RFC 6701,

DOI 10.17487/RFC6701, August 2012,

<https://www.rfc-editor.org/info/rfc6701>.

[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,

<https://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an

Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May

2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T.,

Trammell, B., Huitema, C., and D. Borkmann,

"Confidentiality in the Face of Pervasive Surveillance: A

Threat Model and Problem Statement", RFC 7624,

DOI 10.17487/RFC7624, August 2015,

<https://www.rfc-editor.org/info/rfc7624>.

[RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles",

RFC 7725, DOI 10.17487/RFC7725, February 2016,

<https://www.rfc-editor.org/info/rfc7725>.

[RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E.

Nordmark, "Technical Considerations for Internet Service

Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754,

March 2016, <https://www.rfc-editor.org/info/rfc7754>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity

Profiles for DHCP Clients", RFC 7844,

DOI 10.17487/RFC7844, May 2016,

<https://www.rfc-editor.org/info/rfc7844>.

Grover & ten Oever Expires 29 September 2022 [Page 31]

Internet-Draft Guidelines for HRPC March 2022

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D.,

and P. Hoffman, "Specification for DNS over Transport

Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May

2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8179] Bradner, S. and J. Contreras, "Intellectual Property

Rights in IETF Technology", BCP 79, RFC 8179,

DOI 10.17487/RFC8179, May 2017,

<https://www.rfc-editor.org/info/rfc8179>.

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

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

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

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS

(DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018,

<https://www.rfc-editor.org/info/rfc8484>.

[RFC8980] Arkko, J. and T. Hardie, "Report from the IAB Workshop on

Design Expectations vs. Deployment Reality in Protocol

Development", RFC 8980, DOI 10.17487/RFC8980, February

2021, <https://www.rfc-editor.org/info/rfc8980>.

[RFC9071] Hellström, G., "RTP-Mixer Formatting of Multiparty Real-

Time Text", RFC 9071, DOI 10.17487/RFC9071, July 2021,

<https://www.rfc-editor.org/info/rfc9071>.

[Saltzer] Saltzer, J.H., Reed, D.P., and D.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/>.

[UNGP] United Nations, "United Nations Guiding Principles on

Business and Human Rights", 2011,

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

guidingprinciplesbusinesshr\_en.pdf>.

[UNHR] United Nations, "The Core International Human Rights

Instruments and their monitoring bodies", 2011,

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

coreinstruments.aspx>.

[UNHRC2016]

United Nations Human Rights Council, "UN Human Rights

Council Resolution "The promotion, protection and

Grover & ten Oever Expires 29 September 2022 [Page 32]

Internet-Draft Guidelines for HRPC March 2022

enjoyment of human rights on the Internet" (A/HRC/32/

L.20)", 2016, <https://documents-dds-

ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/

G1613189.pdf?OpenElement>.

[W3CAccessibility]

W3C, "Accessibility", 2015,

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

[W3Ci18nDef]

W3C, "Localization vs. Internationalization", 2010,

<http://www.w3.org/International/questions/qa-i18n.en>.

[Zittrain] Zittrain, J., "The Future of the Internet - And How to

Stop It", Yale University Press , 2008,

<https://dash.harvard.edu/bitstream/handle/1/4455262/

Zittrain\_Future%20of%20the%20Internet.pdf?sequence=1>.

Authors' Addresses

Gurshabad Grover

Centre for Internet and Society

Email: gurshabad@cis-india.org

Niels ten Oever

University of Amsterdam

Email: mail@nielstenoever.net

Grover & ten Oever Expires 29 September 2022 [Page 33]