Analysis of current Internet protocols in terms of Human Rights

rev: 03

Values of Internet Technologies workshop 3 @ SWITCH, Sep 11 2018

Hernâni Marques (@vecirex)
hernani@pep.foundation (3173 3E0C 598D 3A1C F709 55D6 CB57 3865 2768 F7E9)

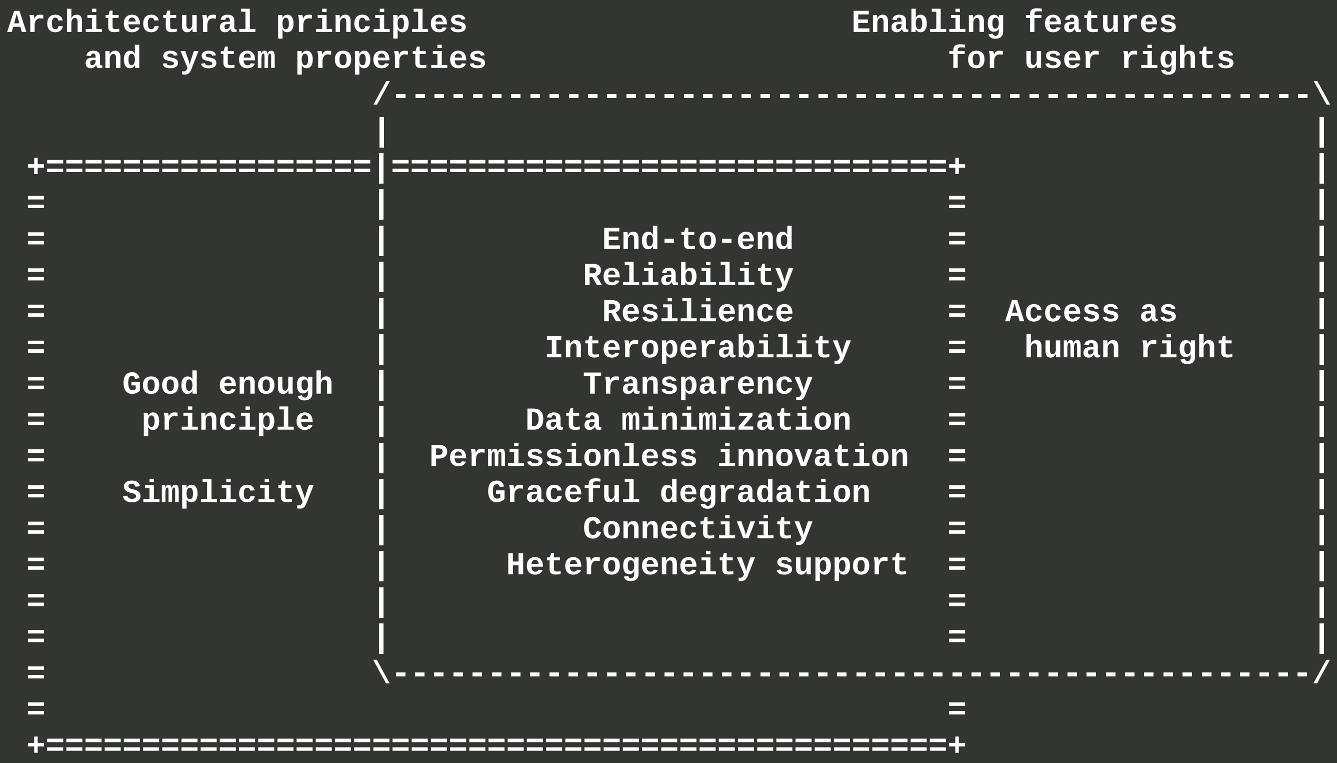
p≡p foundation (@pEpFoundation)

p≡p

Privacy by Default.

Recalling HRPC’s first RFC: 8280

(“Research into Human Rights Protocol Considerations”)



```
Architectural principles                    Enabling features
    and system properties                        for user rights
                   /------------------------------------------------\
                   |                                                |
 +=================|=============================+                  |
 =                 |                             =                  |
 =                 |           End-to-end        =                  |
 =                 |          Reliability        =                  |
 =                 |           Resilience        =  Access as       |
 =                 |        Interoperability     =   human right    |
 =    Good enough  |          Transparency       =                  |
 =     principle   |       Data minimization     =                  |
 =                 |  Permissionless innovation  =                  |
 =    Simplicity   |     Graceful degradation    =                  |
 =                 |          Connectivity       =                  |
 =                 |      Heterogeneity support  =                  |
 =                 |                             =                  |
 =                 |                             =                  |
 =                 \------------------------------------------------/
 =                                               =
 +===============================================+
```

Figure 1: Relationship between Architectural Principles and Enabling Features for User Rights

Recalling HRPC’s first RFC: 8280

(“Research into Human Rights Protocol Considerations”)

```
+-----------------------+-----------------------------------------+
| Technical Concepts    | Rights Potentially Impacted             |
+-----------------------+-----------------------------------------+
| Connectivity          |                                         |
| Privacy               |                                         |
| Security              |                                         |
| Content agnosticism   | Right to freedom of expression          |
| Internationalization  |                                         |
| Censorship resistance |                                         |
| Open standards        |                                         |
| Heterogeneity support |                                         |
+-----------------------+-----------------------------------------+
| Anonymity             |                                         |
| Privacy               |                                         |
| Pseudonymity          | Right to non-discrimination             |
| Accessibility         |                                         |
+-----------------------+-----------------------------------------+
| Content agnosticism   |                                         |
| Security              | Right to equal protection               |
+-----------------------+-----------------------------------------+
| Accessibility         |                                         |
| Internationalization  | Right to political participation        |
| Censorship resistance |                                         |
| Connectivity          |                                         |
+-----------------------+-----------------------------------------+
| ...
```

Recalling HRPC’s first RFC: 8280

(“Research into Human Rights Protocol Considerations”)

Open standards Localization Internationalization Censorship resistance Accessibility	Right to participate in cultural life, arts, and science, and Right to education
Connectivity Decentralization Censorship resistance Pseudonymity Anonymity Security	Right to freedom of assembly and association
Reliability Confidentiality Integrity Authenticity Anonymity	Right to security

Figure 2: Relationship between Specific Technical Concepts
with Regard to Their Contribution to an Enabling Environment
for People to Exercise Their Human Rights

RFC8280: Connectivity

(Freedom of Expression / Freedom of Assembly and Association)

Definition:
“The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958]. Different types of connectivity are further specified in [RFC4084].”

Questions:

- Protocol end-to-end or relying on intermediaries?
- Optimization for low bandwith and high latency?

Examples:

- Middleboxes (e.g., Firewalls, NATs)

RFC8280: Privacy

(Freedom of Expression / Non-Discrimination)

Definition:
”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].”

Questions:

- Any privacy considerations in the protocol, cf. RFC6973?
- Countering traffic analysis?
- Improvement of data minimization?

Examples:

- E-Mail formats and SMTP without added encryption / HTTP / Tor

RFC8280: Content Agnosticism

(Freedom of Expression / Non-Discrimination / Equal Protection)

Definition:
”Treating network traffic identically regardless of content.”

Questions:

- Protocol decisions based on payload / actual content?
- Prioritization of content or services in routing?
- Transparency in the prioritization?

Examples:
ISP plans / HTTPS / VPN / Tor

RFC8280: Security

(Freedom of Expression / Freedom of Assembly and Association / Non-Discrimination / Security)

Questions:

- Any security considerations in the protocol, cf. RFC3552 (BCP72)?
- Are there attacks which could be related to the protocol?
- Are possible attacks pertinent to the features of the Internet enabling Human Rights?

Examples:

Denial of Service / Cryptography (Strength) / MITM

RFC8280: Internationalization

(Freedom of Expression / Political Participation / Participate in Cultural life, Arts, and Science)

Definition:
“The practice of making protocols, standards, and implementations usable in different languages and scripts [...]” (also known as I18N).

Questions:

- Any text strings humans need to understand / enter?
- Unicode support (e.g., with UTF-8 encoding)?
- If anything other than UTF-8 supported, any proper tagging?

Examples:

- Domains / URLs / URIs

RFC8280: Censorship Resistance

(Freedom of Expression / Political Participation / Participate in Cultural life, Arts, and Science / Assembly and Association)

Definition:
”Methods and measures to mitigate Internet censorship.”

Questions:

- Any identifiers in use which can be associated with users or content?
- Any signaling / transparency when access to resource restricted?
- Protocol designed in a way that filtering of data / services possible?

Examples:

- DNS / HTTP / Tor

RFC8280: Open Standards

(Freedom of Expression / Participate in Cultural life, Arts, and Science)

Questions:

- Protocol fully documented to be changed / implemented?
- Use of proprietary code?
- Use of standards not available without cost?
- Use of patents preventing full implementation?

Examples:

- Most RFCs vs. centralized instant messaging silos

RFC8280: Anonymity

(Non-Discrimination / Political Participation / Freedom of Assembly and Association / Security)

Definition:
“The condition of an identity being unknown or concealed [RFC4949].”

Questions:

- Similar questions as to Privacy
- Any ways to not / less expose personal data?

Examples:
Hide IP, User Agent data / VPN / Tor

RFC8280: Decentralization

(Non-Discrimination / Political Participation / Freedom of Assembly and Association / Security)

Definition:
”Implementation or deployment of standards, protocols, or systems without one single point of control.”

Questions:

- No single point of control?
- Which potential discrimination is possible?
- Are centralized points of control created?

Support for federation?

Examples:

XMPP / E-Mail / DHT-based networks vs. centralized services

Links & Questions & Discussions

- Learn about the IETF: https://ietf.org/
- Learn about the IRTF: https://irtf.org/
- Learn about the HRPC: https://datatracker.ietf.org/rg/hrpc/about/
- Work and meet HRPC group members
  - IETF meetings
  - hrpc@irtf.org mailing list: https://www.irtf.org/mailman/listinfo/hrpc
- ...
- Ask & Discuss!