Proposed RG
Human Rights Protocol Considerations
(hrpc)

IETF 93
Wednesday July 22
17:40 – 19:40

Co-Chairs:
Niels ten Oever – Article19
Avri Doria – APC

Agenda

- Agenda Bashing
- Jabber scribe, note takers
- Notewell
- Introduction
- Status of proposed research group
- Context of research
- Discussion of Methodology draft draft-varon-hrpc-methodology-00
- Discussion of Glossary draft draft-dkg-hrpc-glossary-00
- Research on "Values and Networks"
- Open discussion other drafts, papers, ideas
- Next steps

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Status of proposed research group

- October, 27, 2014 - Publication of Proposal for research on human rights protocol considerations - 00

  ID 00 - www.ietf.org/id/draft-doria-hrpc-proposal-00.txt
- IETF91 - November, 13, 2014: Presentation during saag session

  https://datatracker.ietf.org/meeting/91/agenda/saag/
- March 9, 2015 - Publication of Proposal for research on human rights protocol considerations - 01

  http://www.ietf.org/id/draft-doria-hrpc-proposal-01.txt
- January 2015 - Proposed research group in the IRTF
- March 22 to 27, 2015 IETF92 – Session & Interviews with members from the community
- June 2015 - Interim Meeting
- July 2015 Publication of Methodology and Glossary

  ID 00 - https://tools.ietf.org/html/draft-varon-hrpc-methodology-00

  ID 00 - https://tools.ietf.org/html/draft-dkg-hrpc-glossary-00
- November 2015, IETF93 – Expected screening of film, two or three IDs (01, 01 and 00), paper, session

Context of research

- Internet as tool for freedom of expression and freedom of association
    - By intention or by coincidence?
        - The Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. (RFC1958)
- But as the scale and the industrialization of the Internet has grown greatly, the influence of such world-views started to compete with other values.
- The belief of the RG is that as the Internet continues to grow, the linkage of Internet protocols to human rights needs to become explicit, structured, and intentional

Context of the Research (2)

Working on this problem in the IRTF (in context of IETF), because this is where the protocols and standards that have shaped and are shaping the Internet are being developed

This proposed RG has two major aims:

- to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly, and

- to propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, in a manner similar to the work done for Privacy Considerations in RFC 6973. This research group suggests that similar considerations may apply for other human rights such as freedom of expression or freedom of association.

Methodology ID

- Presented by Corinne Cath

HRPC

methodology

It’s not easy but

- We have developed a method to:

- Map the relation between human rights and protocols and architectures.
- Requires a good amount of interdisciplinary and cross organizational cooperation to develop a consistent methodology.
- Input from the community

Data is gathered from 3 sources

1: Discourse analysis of RFCs

2: Interviews with members of the IETF community during the Dallas meeting of March 2015

3: Participant observation in Working Groups

➡ data was processed and led to creation of the following three consecutive strategies

3 Strategies

1. Translating human rights concepts to technical definitions

2. Map cases of protocols that enable or hinder FoA and FoE

3. Apply human rights technical definitions to the cases mapped

Expected Outcome

1. Identify best (and worst) current practices.

2. Develop procedures to systematically evaluate protocols for potential human rights impact

Preliminary Findings

- See ID

- In conversation with different individuals that experienced different forms of HR violations aided by protocols.

Next Steps

- A first list of concepts, which definitions should be improved and further aligned with existing RFCs, is being publish as [ID draft-dkg-hrpc-glossary-00].
- Next Steps of the Methodology still to be applied
- Map cases of protocols that hinder or help FoA and FoE
- Apply human rights technical definitions to the cases mapped
- Next Steps of the Methodology still to be developed

Future Research Questions

- 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]?

Glossary ID

- Presented by Niels ten Oever

$$freedom\ of\ expression = \begin{pmatrix} content\ agnosticism \\ connectivity \\ privacy \\ security \end{pmatrix}$$

This is roughly where we left off at IETF92

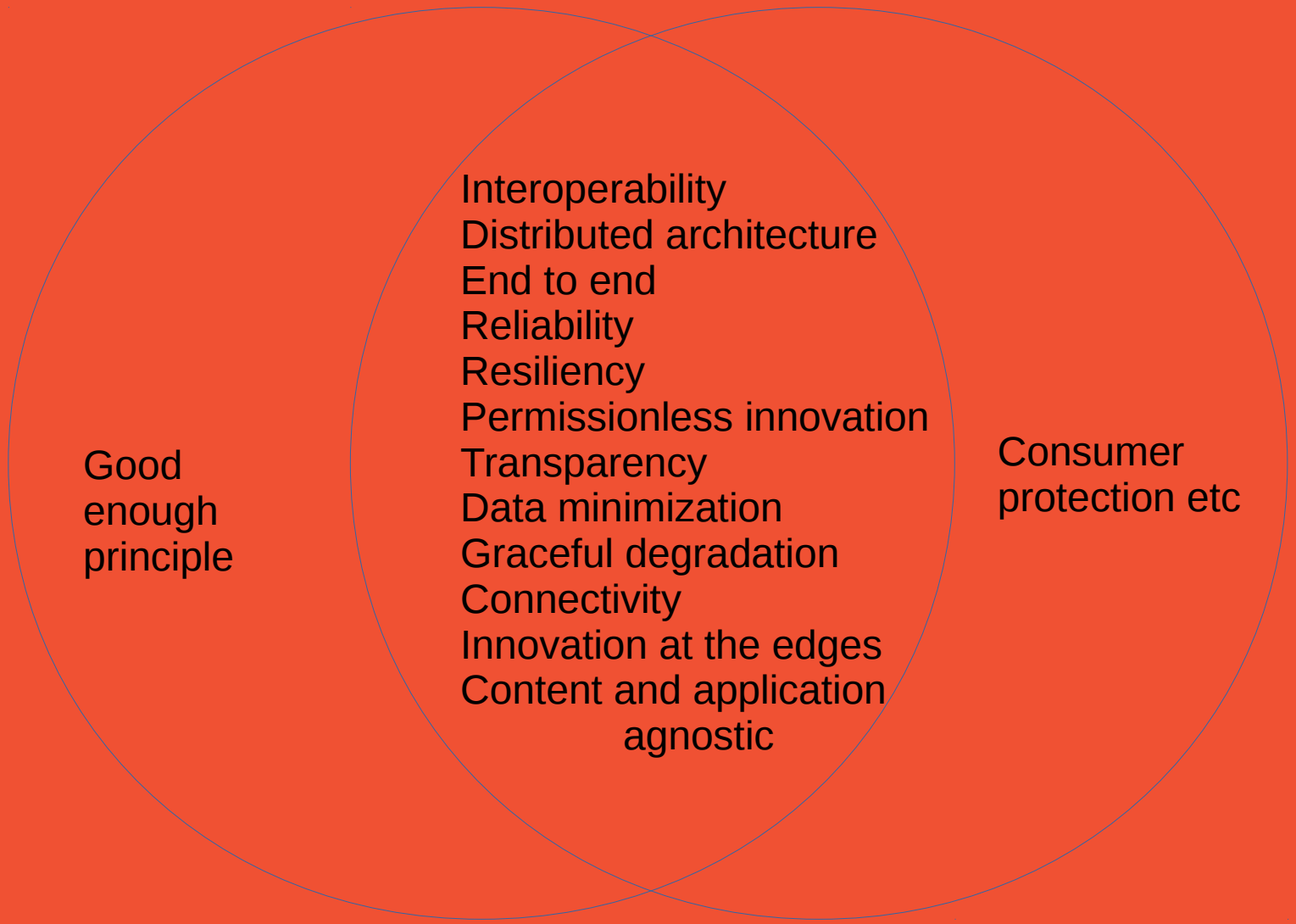
We need better defintions

$$security = \begin{pmatrix} resilience \\ reliability \\ confidentiality \\ anonymity \\ authenticity \end{pmatrix}$$

$$connectivity = \begin{pmatrix} interoperability \\ resilience \\ reliability \\ robustness \end{pmatrix}$$

Architectural principles / characteristics

Enabling features for user rights



Define more

- OK – we'll make a glossary
  - Not dissimilar to RFC4949 Internet Security Glossary

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 fact of not being identified

Authenticity

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

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 (1)

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. (Wordpress)

Debugging (2)

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 a single point of control.

- Too vague? Example? Different understandings of decentralized

Distributed

A distributed architecture is a system in which not all processes reside in a single computer.

End-to-End (1)

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.

End-to-End (2)

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}}

Federation

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

Integrity

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

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.

Internationalization

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

Please see {{ RFC6973 }}

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.

Robust

The resistance of protocols and their implementations to errors, and to involuntary, legal or malicious attempts to disrupt its mode of operations.

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. (Wikipedia)

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}}

With this in mind: Security?

$$security = \left(\begin{array}{c} resilience \\ reliability \\ confidentiality \\ anonymity \\ authenticity \end{array} \right)$$

Connectivity

$$connectivity = \begin{pmatrix} interoperability \\ resilience \\ reliability \\ robustness \end{pmatrix}$$

Can we say that:

$$\left\langle \begin{array}{c} \textit{content agnosticism} \\ \textit{connectivity} \\ \textit{privacy} \\ \textit{security} \\ \textit{open standards} \end{array} \right\rangle = \textit{freedom of expression}$$

Or should it be:

$$freedom\ of\ expression = \left(\begin{array}{c} content\ agnosticism \\ connectivity \\ privacy \\ security \\ open\ standards \end{array} \right)$$

The full picture

$$\left(\begin{array}{c} \left(\begin{array}{c} interoperability \\ resilience \\ reliability \\ robustness \end{array} \right) = connectivity \\ \left(\begin{array}{c} resilience \\ reliability \\ confidentiality \\ anonymity \\ authenticity \end{array} \right) = security \\ privacy \\ content\ agnosticism \end{array} \right) = freedom\ of\ expression$$

What Snowden said at IETF93

Universal declarationof HUman Rights , US constitution, UCCPR, they all say that rights should be protected against arbitrary interference. [...] Unfortunately the Internet has provided a very cheap and effective means to interfere with it.

[...]

Human rights are difficult to enforce all around the world [..] The Internet you access in France should be the same as the Internet you access in China.

[...]

When you think about access, you should think about non-discrimination, how do you enforce non-discrimination *on the network. [..] What are the mechanism through which discrimination works? It's by identification, by association. By anonymizing people, by allowing themselves to divorce themselves from being visible members of a minority group, religious group, political affiliation that could get them jailed, if you allow them to divorce themselves for this identity through technology, you're providing human rights.*

Universal Declaration of Human Rights

Article 1

All human beings are born free and **equal** in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 2

Everyone is entitled to all the rights and freedoms set forth in this Declaration, **without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.**

Article19

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.

Non-discrimination

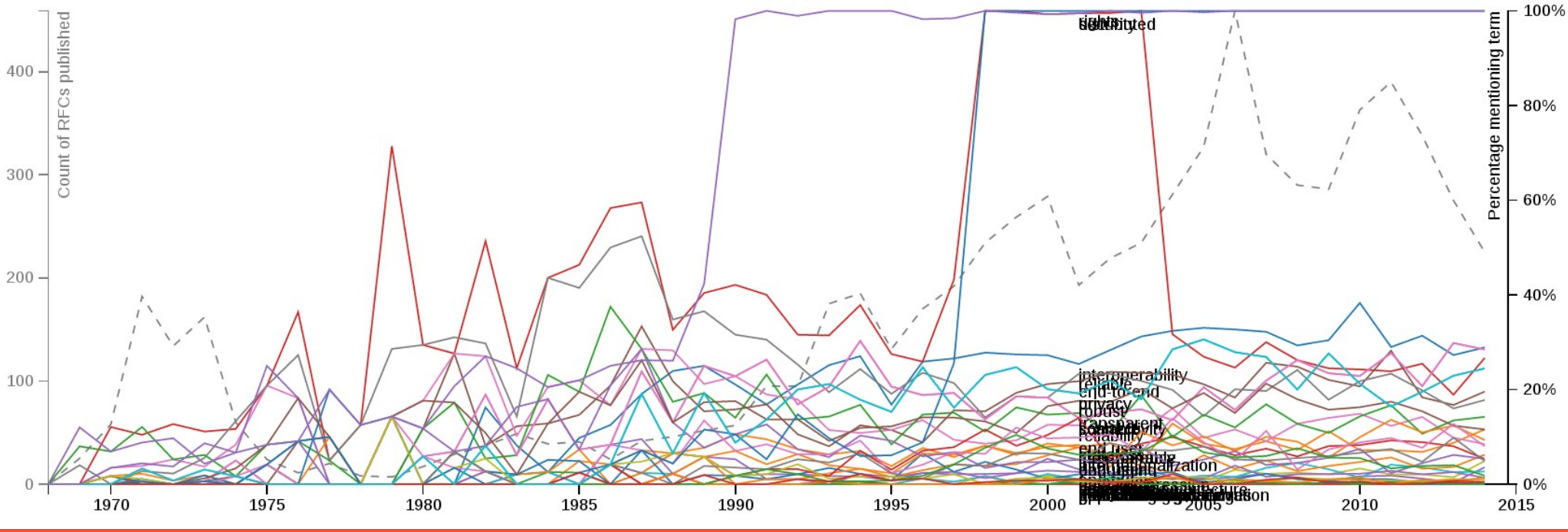
- Function / part of:
  - Privacy?
  - Content agnosticism?
  - Anonimity?
- Or could this have its own 'formula'?

$$\begin{pmatrix} privacy \\ anonymity \\ content\ agnosticism \end{pmatrix} = non\ discrimination$$

Interdependence

- Many concepts are building blocks of other concepts. How to deal with interrelation?
  - Create (inter)dependency tree?

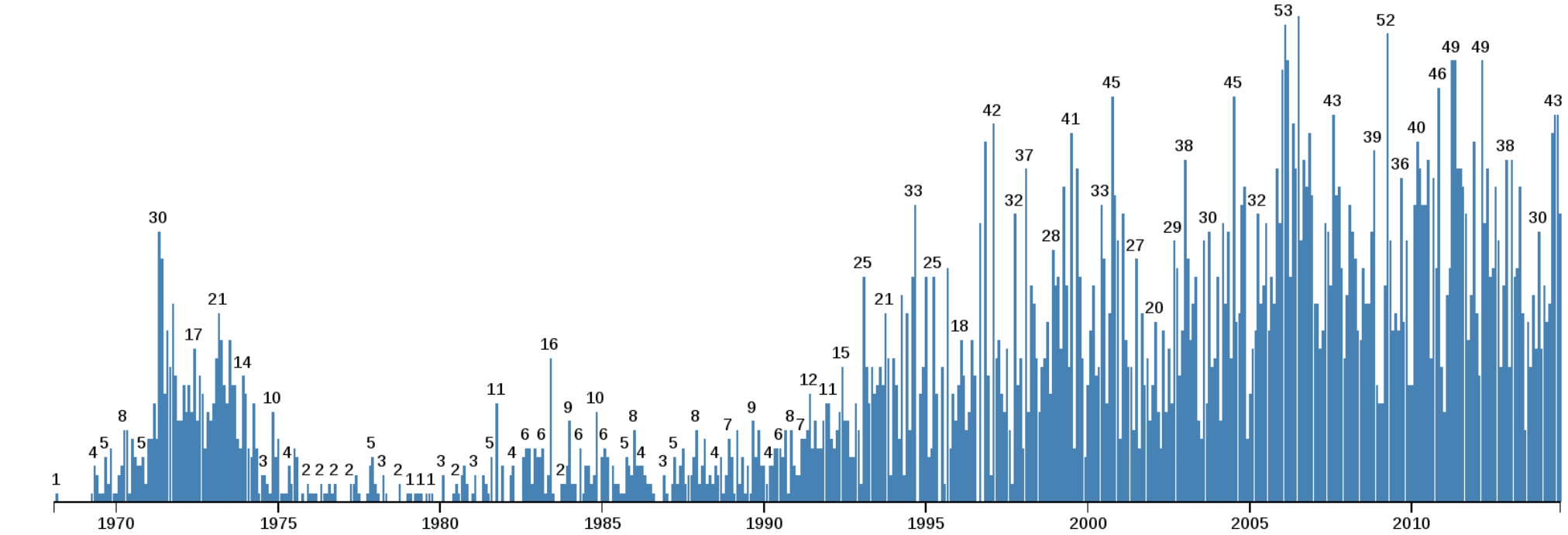
Early outcomes analysis RFCs



Achieved with tools produced by Nicholas Doty

https://github.com/npdoty/rfc-analysis

Still needs to be corrected for



RFCs published, by month

Produced by Nicholas Doty

https://github.com/npdoty/rfc-analysis

Values and Networks

- Presented by Roland Bless

Next steps

- Finalizing film before IETF94
- Improving Glossary ID
- Map more cases of protocol HR violations
- Apply human rights technical definitions to the cases mapped
- Potentially start with an ID for Guidelines for Human Rights Considerations

Join the discussion

- Mailinglist
  https://www.irtf.org/mailman/listinfo/hrpc
- Github

  https://github.com/nllz/IRTF-HRPC