Human rights in technical standards: our practical approach

Date: 2018-01-19
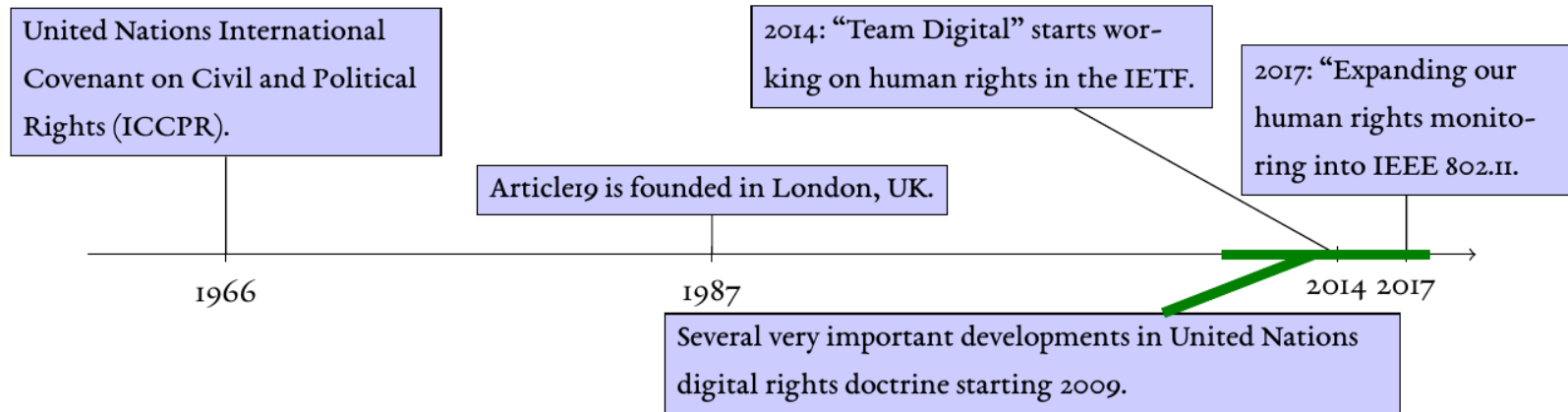
Authors:

Name	Affiliation	E-mail address
Amelia Andersdotter	ARTICLE19	amelia@article19.org

Abstract

ARTICLE19 is a freedom of speech organisation founded in London in 1987. Since 2014, ARTICLE19 operates a digital program to look at human rights implications of design choices in technical standards and specifications, and to promote conciousness about such implications in standard development organisations. This hands-on approach has enjoyed success in other forums, such as the IETF, but is relevant beyond protocols – including in several ongoing projects at the bottom-most plumbing of wireless communications.

What? Who? Why?

United Nations International Covenant on Civil and Political Rights (ICCPR).

2014: "Team Digital" starts working on human rights in the IETF.

2017: "Expanding our human rights monitoring into IEEE 802.11.

Article19 is founded in London, UK.

1966

1987

2014 2017

Several very important developments in United Nations digital rights doctrine starting 2009.

- Founded in 1987. Global focus, regional teams all over the world.
- Digital Program: focussing on human rights implications of the design of technical infrastructures.
- Previous work: IETF, ICANN, ITU, &c. Human rights impact assessments (HRIAs), capacity building, etc.

Some examples of our work until now:

RFC 8280, Research into Human Rights Protocol Considerations (HRPC)

ICANN's Corporate Responsibility to respect Human Rights: Recommendations for developing Human Rights Review Process and Reporting by CCWP-HR, ARTICLE 19 and IHRB.

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems

Why does this matter?

- 802.11 technologies are used by lots of people around the world, for social, political and economic empowerment.

- Helping the "good guys do good" (security practices or privacy enhancements under way?)

- 802.11 standards <u>have an impact</u> on downstream markets: whatever is made easy through the standard, is likely to be implemented down the line.

- 802.1 SEC TG project "802E" already made headway with mapping out risks and mitigations, until 2016.

Some examples of design choices

- Censorship: Is communication dependent on a central point? Can that central point influence what communications are made by end-users?

- End-user power: Can an end-user choose how, why and when he or she accesses information and features, or not?

- Accessibility: Does the standard, specification and the technologies it specifies include support for many languages, especially non-Latin alphabets?

- Privacy: Data minimization, storage minimization, etc.

- Security: Counteract unintended uses (information leakage, reliabile authentication, etc)

- Enables collaborative networking/presupposes dominant network providers?

Some examples of design choices

- Censorship: Is communication dependent on a central point? Can that central point influence what communications are made by end-users?

- End-user power: Can an end-user choose how, why and when he or she accesses information and features, or not?

- Accessibility: Does the standard, specification and the technologies it specifies include support for many languages, especially non-Latin alphabets?

- Privacy: Data minimization, storage minimization, etc.

- Security: Counteract unintended uses (information leakage, reliabile authentication, etc)

- Enables collaborative networking/presupposes dominant network providers?

Network and communication technologies have an impact on freedom of speech, opinion, freedom of assembly, thought, privacy and the right to security – and that's just within the civic and political rights!

Puzzling things in the IEEE 802.11, part 1

- Conditional statements in the standard text are not always expressed as **"if** X [is true] **then** Y".** Frequently alternative construction **"when** X [is true]**, Y"** is used for clearly conditional statements(!)

Examples:

- Section 4.3.16 (dot11OCBActivated), 4.4.2 SS, 5.1.1.3 (priority parameter in MAC Service primitives), etc.

Puzzling things in the 802.11 , part 2

- <u>No mandatory security and privacy considerations in CSD in the Operations Manual section 13!</u>

- Security considerations are mandatory for all IETF standards, and a Privacy Considerations document (RFC 6973) exists since 2013.

- Better procedures pre-empt security and privacy concerns.

- De-antagonises security and privacy concerns imposed from external organisations, such as governments.

- Cf. co-existence assessments: they're alright?

Reflections

"Really, under which normative framework?" Generally high awareness of human rights among participants!

Lack of default framework for privacy and security enhancement, causes proposals/findings in this area to take more time, or face more resistance, than is necessary.

Some procedures makes it easier to find problems, than to be "part of the solution".

In task groups, development imperative is often targetting client (or end-user) centric features, meaning that features seem to be introduced in a way considerate of end-users' preferences most the time.

References

- IETF, RFC 8280: https://tools.ietf.org/html/rfc8280

- IETF, RFC 6973: https://tools.ietf.org/html/rfc6973

- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE 802.11-2016)

- IEEE 802, LAN/MAN STANDARDS COMMITTEE (LMSC), Operations manual (last approved: 17 March 2017)

- ARTICLE19, What we do, https://www.article19.org/what-we-do/

- ICANN's Corporate Responsibility to respect Human Rights: Recommendations for developing Human Rights Review Process and Reporting by CCWP-HR, ARTICLE 19 and IHRB. https://community.icann.org/download/attachments/56132135/ICANN_CS_to_respect_HR_report_ALL_FINAL-PDF.pdf