Mar 3, 2023

IAB Response to the Office of the High Commissioner for Human Rights Call for Input on "The relationship between human rights and technical standard-setting processes for new and emerging digital technologies"

The Internet Architecture Board (IAB) welcomes the opportunity to provide input to the Office of the High Commissioner for Human Rights on "The relationship between human rights and technical standard-setting processes for new and emerging digital technologies". The IAB advises and provides oversight for protocols and procedures used by the Internet and also handles the liaison management for the Internet Engineering Task Force (IETF), the main engineering organization that works on standards relating to Internet technology.

BRIEF BACKGROUND

The IETF is an open, diverse, and global community of network operators, engineers, researchers and many other stakeholders. The mission of the IETF is to produce "relevant technical documents that influence the way people design, use, and manage the Internet [...] to make the Internet work better" "for communities that share our commitment to openness and fairness" (RFC 3935). The IETF develops, maintains and evolves the Internet protocol suite and many related standards. The Internet Research Task Force (IRTF) is a parallel organization to the IETF with a focus on longer term research issues related to the Internet.

OPEN PARTICIPATION

The IETF is both part of and through its processes fosters the complex, multistakeholder nature of Internet governance. Multistakeholder participation is a precondition to ensure the long term health of a free and open Internet and the inclusion of legal and human rights experts in its process is important to protocol

development. That the IETF operates by consensus lends further credit to its outputs as all viewpoints have been considered.

The IETF and IRTF are open for participation for everybody at no cost. The IETF does not have individual or organizational membership; but instead as stated in the IETF mission, "any interested person can participate in the work, know what is being decided, and make his or her voice heard on the issue" (RFC 3935). This principle provides the basis for the participation for a broad set of stakeholder and wide input. The interconnection of the IETF and IRTF and their open nature for participation has shown to provide a valuable approach to enable input from an increasing set of stakeholders and considerations of broader perspectives in the standards-setting process.

A key tenet of the IETF process is that technical standards benefit when more people can contribute expertise. As such the IETF invests in enhanced remote participation for its meetings and interim meetings such that participants both in-person and remote can equally participate. Further, a variety of activities help realize these ideals by providing a path to sustained engagement for those who would otherwise face difficulties participating in the IETF, both in the IETF's substance such as a move towards more inclusive terminology in RFCs (draft-terminology) and in the IETF's processes. On process, the IETF's Diversity and Inclusion sponsorships support a variety of mechanisms to increase inclusion such as the principle to provide a free registration option for remote participants (draft-ietf-shmoo-remote-fee) and fee waivers to lower economic barriers to meeting participation, as well as support activities such as childcare, or the IETF Systers program which offers women participants the opportunity to connect, share, and learn with each other.

IETF standards development is fully transparent and openly documented. Its discussion lists are open and publicly archived, its meetings are announced in advance, some proceedings stream audio and video, and all IETF meeting attendance is recorded and published along with official meeting minutes. This high level of transparency does not only allow broad participation but also provides a report of the standardization process documenting inputs, discussions, and conclusions for later review.

HUMAN RIGHTS IS A LONG-TERM AREA OF RESEARCH

The IRTF promotes Internet research through focused, long-term Research Groups working on Internet protocols, applications, architecture and technology. Meetings of IRTF research groups are usually co-located with IETF standards meetings, promoting this research within the IETF as input to the standardization process. Further, it also enables participation of a broad set of stakeholders, including from academia and civil society, in the IETF standardization process.

In 2015, the IRTF chartered a research group on Human Rights Protocol Considerations (HRPC) and thereby promotes the interconnection of human rights research and Internet protocol standardization. HRPC research aims to expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly. It has proposed guidelines to protect the Internet as a human-rights-enabling environment in future protocol development with its first publication, that has led to the increase of awareness, in both the human rights community and the technical community, of the importance of the technical workings of the Internet and its impact on human rights (RFC 8280).

Furthermore, since 2018, the Privacy Assessments and Enhancements Research Group (PEARG) considers impacts of Internet protocols on the right to privacy.

The Applied Networking Research Workshop (ANRW) is a collaboration between the IRTF, the Internet Society and the Association for Computing Machinery (ACM) that fosters cross-community collaboration on emerging results in applied research of the Internet. It provides a platform and monetary support for emerging areas of interest that would not otherwise get much exposure or be able to participate in the discussion.

SECURITY AND PRIVACY STANDARDS

The IAB and the IETF have a long history of working on privacy improvements for Internet technology and applications. As one of the key early principles in this space, the IAB and the IETF decided to not consider wiretapping requirements into Internet protocols (RFC 2804). Providing secure and private communication is a precondition to support human rights. A requirement of all IETF work is to include a discussion of the security and privacy implications of our protocols (RFC 6973), and the IETF has explicitly aimed to thwart any attempts to pervasively monitor Internet users (RFC 7258).

Identifying pervasive monitoring as a technical attack was the result of a joint workshop between the IETF and the World Wide Web Consortium (W3C) that aimed to strengthen the Internet against surveillance, setting a good example for divisive action based on the integration and consideration of human rights goals through standard setting.

Established IETF standards in areas such as ensuring confidentiality for Internet communications, including TLS (RFC 8446), are very widely used. They continue to be enhanced and used in new contexts, such as with new transport protocols like QUIC (RFC 9000) or application protocols like DNS over HTTPS (RFC 8484). Securing communication and designing an Internet that is foremost addressing the interest of the users (RFC 8890) are goals that align the mission of the IETF standards process

to develop high qualitative specifications that make the Internet work better for human rights.

Confidential and authenticated Internet communications between people are a growing need in an increasingly Internet-intermediated world. Messaging Layer Security (MLS) and OpenPGP Message Format (OpenPGP) describe standards with which a service provider does not have access to the content of users' communications by design. End-to-end encrypted systems are exceptional in providing both security and privacy properties through confidentiality, integrity and authenticity features for users (draft-knodel-e2ee-definition).

As mentioned previously, in addition to IETF work on standards that improve privacy, privacy technologies are considered and researched in the IRTF in the PEARG.

STANDARDIZATION AND THE INTEROPERABLE, INTERCONNECTED INTERNET

Technical standards describe designs for services and tools such that different providers can build services and tools that interoperate. A standard is not code. Services and tools using the same standard might be implemented between layers of the technical stack, across platforms, using different programming languages, and offered and used by actors subject to specific constraints such as legal jurisdiction and regulatory environments.

Beyond interoperable and interconnected service and tool development, standardization can also support requirements for transparency, certification, attestation, safety and compliance.

The main goal of the networking standards process is to enable the long term interoperability of protocols (draft-iab-protocol-maintenance). Therefore the pace of standardization is necessarily slower than the pace of innovation. In order to standardize emerging technologies a standards body must first develop the expertise required to build consensus through peer review. And the standardization process itself is best informed by "running code", eg "the combined engineering judgment of our participants and our real-world experience in implementing and deploying our specifications" (RFC 3935).

Technologies that can be designed and implemented unilaterally such as data-driven methods,[1] data analysis, machine learning, and others, have major human rights implications. However the voluntary standardization of these technologies is unlikely when not motivated by interoperability. So far there is little IETF work in these areas. Work on this category of emerging technology in the

[1] Often referred to more capaciously as "artificial intelligence (AI)".

IETF/IRTF is limited to documenting operations challenges when computing is done in a networked environment. Some aspects of data-driven methods could potentially provide benefits to end users if there were more interoperability-related standardization, though incentives hardly exist.[2] It is more likely that there will be regulatory or compliance motivations, thus AI standardization is unlikely to be voluntary.

BEYOND STANDARDS DEVELOPMENT

For voluntary standards, it is important to acknowledge the intentional gap between their development, implementation, and deployment.

Consideration on human rights in digital technologies need to go beyond the standards-setting process. Even though goals in standard-setting and document quality are aligned with human rights, the work of the IETF and the design of the Internet architecture is based on technology building blocks that allow for evolution and innovation of the Internet and technologies that use the Internet as a communication platform. The basic need for standardization of these building blocks is driven by the requirement for a global communication platform to interoperate. Therefore interoperability is often the main incentive for companies and other stakeholders to participate in the standards-setting process. As such, standards-setting organizations foremost must ensure high quality standards in order to provide incentives for deployment.

Considering deployment scenarios and implication including those on human rights is important for the standard-setting process but cannot cover and should not limit all future uses of these protocol building blocks. The success of standard-setting organizations is measured in high quality standards that are adopted and deployed. As such creating deployment incentives that align with human rights consideration is of high importance when considering human rights in digital technologies. Such incentives can be only partially provided by the standards-setting process itself by e.g. offering only options that support human rights, however, it is generally difficult for and not intended by standards-setting organizations to control or limit deployment options.

Standards-setting aims to support innovation but often standards-setting happens after the innovation has started. As such new and emerging technologies that evolve on top of the Internet's communication platform may not be instructed by standards-setting organizations or might not even have a platform for discussion of

[2] "OpenAI Is Now Everything It Promised Not to Be: Corporate, Closed-Source, and For-Profit." *OpenAI Is Now Everything It Promised Not to Be: Corporate, Closed-Source, and For-Profit*, www.vice.com/en/article/5d3naz/openai-is-now-everything-it-promised-not-to-be-corporate-closed-source-and-for-profit.

its impact on human rights at this initial development phase. Most standards-setting organizations aim to provide a platform for such innovation and discussion, and especially the IETF with its open participation model welcomes new areas of working within its scope of protocols development for Internet communication. Innovations in emerging technologies that impact human rights and go beyond this scope, however, may need new organizational structures.

THE INTERNET PROTECTS HUMAN RIGHTS

The Internet has evolved an important part of the infrastructure and specifically a tool to help protect human rights, specifically the rights of freedom of opinion and expression as well as the right to work and education.

Environmental concerns are also a key issue facing humankind. The Internet and Internet technology relates to these concerns in a number of ways, from the point of view of the Internet itself consuming some resources but also being a tool that can enable processes in the rest of the society that have the power to influence the environment. The IAB has recently held a workshop on understanding these implications, and the IETF is looking for ways to continuously improve the impact of the Internet on the environment (draft-iab-ws-environmental-impacts-report).

The flexibility of the Internet architecture based on modular building blocks enables evolvability to support a large set of traffic requirements and even rapid changes in traffic demands as it was observed during the COVID-19 pandemic. This flexibility is also the basis for the Internet as a tool to protect human rights. Respectively, in order to sustain the Internet as a tool for protection of human rights, we need to protect the flexibility and interworking of a global Internet.

While it can be observed that the Internet, by providing a general purpose communication platform, also gets used for efforts that can impact human rights negatively, like censorship or propaganda, limiting the use of the Internet may also impact human rights. Furthermore, implementing tighter control also limits the Internet's ability to evolve and circumnavigate interference with the Internet architecture in its mission to connect people and share information.

Care must be taken in order to achieve the right balance in protocol evolution, standards setting, as well as regulatory actions that impact the evolvability of the Internet in order to retain the Internet as a universal and resilient tool to protect human rights.

ANNOTATED REFERENCES

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>.

The goal of the IETF is to make the Internet work better. Its cardinal principles are: Open process, technical competence, volunteer core, “rough consensus and running code,” and protocol ownership.

Kühlewind, M., Reed, J., and R. Salz, “Open Participation Principle regarding Remote Registration Fee”, draft, <https://datatracker.ietf.org/doc/html/draft-ietf-shmoo-remote-fee-05>.

This draft document proposes a principle for open participation that extends the open process principle defined in RFC3935 by stating that there must always be a free option for online participation to IETF meetings and, if possible, related IETF-hosted events over the Internet.

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>.

Guidelines to protect the Internet as a human-rights-enabling environment in future protocol development have led to the increase the awareness, in both the human rights community and the technical community, of the importance of the technical workings of the Internet and its impact on human rights

IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, DOI 10.17487/RFC2804, May 2000, <https://www.rfc-editor.org/info/rfc2804>.

The IETF developed a policy not to include standards-track documents of functionality designed protocols that facilitate wiretapping. This memo explains what the IETF thinks the question means, why its answer is "no", and what that answer means.

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>.

This document brought privacy considerations into the IETF by aligning the needs of designers, implementers, and users of Internet protocols. It defined a thorough taxonomy and raised awareness of privacy-related design choices.

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>.

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible. Following the Snowden revelations, there became widespread recognition in the IETF that surveillance was an attack on privacy that Internet protocols must mitigate by design.

Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

TLS provides a secure channel between two communicating peers. It encrypts most user-to-web-server traffic today in two parts: the authentication handshake in which cryptographic security is established between parties, and the secure sharing of content between parties.

Iyengar, J., Ed., and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

QUIC is a transport protocol that provides security measures that uses encryption to ensure confidentiality, integrity, and availability in a range of deployment circumstances, but specifically traffic that must be transported in low-latency environments.

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>.

DOH provides a way to send and receive DNS queries in a secure way. Leveraging the encryption in TLS, DNS sends and responds over HTTPS, where previously privacy- and confidentiality-sensitive DNS queries– the IP location of a service a user is requesting by providing a domain– were sent as plaintext.