Are Internet Protocols the New Human Rights Protocols? Understanding 'RFC 8280 – Research into Human Rights Protocol Considerations'

Vivek KRISHNAMURTHY*

Keywords: human rights by design, internet governance, technology and human rights

I. Introduction

'Guns don't kill people; people do.' This favourite phrase of firearms enthusiasts in the United States is emblematic of the view that technologies are morally neutral, and that the responsibility for the adverse consequences of any particular use of a technology should be borne by the user.

It is against the backdrop of this mentality, which has long been commonplace in Silicon Valley,[1] that the significance of a new publication by the Internet Research Task Force (IRTF) is best understood.[2] The title of the publication ('RFC 8280 – Research into Human Rights Protocol Considerations') could not be more obscure. Yet beneath the impenetrable title and the often dry and technical content than follows is a landmark for the burgeoning technology and human rights movement. The publication of RFC 8280 represents one of the first acts of recognition by the institutions that govern and develop the internet's technical architecture of the human rights impacts of their engineering decisions. Whether the tools that RFC 8280 attempts to provide the internet engineering community with to consider the human rights impacts of their standard-setting work will prove effective remains to be seen, yet the very attempt at doing so is worthy of praise, note, and analysis, too.

II. Background

Understanding the significance of RFC 8280 requires delving into the process through which the technical standards that underpin the internet come into being. Although we

* B.A., Toronto; M.Phil, Oxon; J.D., Yale. Counsel, Foley Hoag LLP; Lecturer on Law, Harvard Law School; Fellow, Carr Center for Human Rights Policy, Harvard Kennedy School of Government; Affiliate, Berkman Klein Center for Internet & Society, Harvard University.

[1] Anupam Chander and Vivek Krishnamurthy, 'The Myth of Platform Neutrality' (2018) 2 *Georgetown Law Technology Review* 400.

[2] N ten Over and C Cath, 'RFC 8280 – Research into Human Rights Protocol Considerations' (October 2017), https://tools.ietf.org/html/rfc8280 (accessed 9 November 2018).

Business and Human Rights Journal, 4 (2019), pp. 163–169
doi:10.1017/bhj.2018.30
© Cambridge University Press

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

now take the existence and the efficient functioning of the internet for granted (as we do most forms of infrastructure until they stop working), the development of a set of open standards that allows anyone with the requisite skills to build a device that can communicate with any other internet-connected device is a remarkable achievement.

Much of the credit for this achievement belongs to the Internet Engineering Task Force (IETF), a consensus-driven organization that, since the mid-1970s, has spearheaded the development of open protocols for internet-based communications. In technical parlance, protocols are sets of agreed standards that allow two or more devices to communicate and exchange information with each other. Some protocols developed by the IETF have become part of the vernacular, such as the Hypertext Transfer Protocol, whose four-letter abbreviation (HTTP) prefaces every address on the World Wide Web. From a technical perspective, however, HTTP is a set of rules that governs how web browsers exchange information with a variety of different web servers to render and display web pages on a diversity of devices.[3]

Similarly, we are able to seamlessly and efficiently exchange billions upon billions of emails per day because every email system in existence follows the specifications laid out in the Simple Mail Transfer Protocol (SMTP).[4] Other protocols developed through the IETF's processes are less widely known but much more important. Most notable among these is the Internet Protocol (IP), which establishes the internet as we know it by giving every device connected to the global network a unique address, and laying down rules on how to route information through the network to allow any pair of devices to communicate with each other.[5]

Like most other institutions of internet governance, the IETF is not a membership organization. Rather, anyone with the interest and ability to participate in the IETF's standards-development work is welcome to do so. Engineers from government laboratories, private companies, and academic institutions, along with a notable number of solo tinkerers, can and have proposed the development of new internet protocols by circulating documents called 'Requests for Comment' – or RFCs. More commonly, however, members of the IETF's numerous working groups on different issue-areas will work together to develop a proposal for a new protocol or standard that is then circulated as an RFC. Some of these RFCs will eventually be formally adopted by the IETF and published as official 'internet standards'. Other RFCs will never get beyond the proposal stage, while others still are submitted to document best practices or for informational purposes.

As the challenge and complexity of the technical aspects of internet governance grew more complex, a separate Internet Research Task Force (IRTF) was created in the late 1980s to focus on longer-term research tasks, so that the IETF could concentrate on the development of protocols and standards to be implemented in the short to medium term.

[3] T Berners-Lee et al, 'RFC 1945 – Hypertext Transfer Protocol – HTTP/1.0' (May 1996), https://tools.ietf.org/html/rfc1945 (accessed 9 November 2018).

[4] Jonathan Postrel, 'RFC 821 – Simple Mail Transfer Protocol' (August 1982), https://tools.ietf.org/html/rfc821.html (accessed 9 November 2018).

[5] 'RFC 791 – Internet Protocol: DARPA Internet Program Protocol Specification' (September 1981), https://tools.ietf.org/html/rfc791 (accessed 9 November 2018).

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

Mirroring the structure of the IETF, the IRTF is composed of a number of research groups, of which there are currently 13.[6] In the early days, the IRTF's research groups were focused almost exclusively on technical issues, such as developing new anti-spam tools and techniques.[7] In 2015, however, a new research group into 'Human Rights Protocol Considerations' was established under the auspices of the IRTF with three stated aims:

- To expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly.
- 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.
- To increase the awareness in both the human rights community and the technical community on the importance of the technical workings of the internet and its impact on human rights.[8]

From a structural perspective, therefore, RFC 8280 can be understood as the first output by the human rights-focused component of a larger technical research endeavour that considers the human rights implications of the IETF and IRTF's standards-development work. In view of the long-standing tendency of engineers to view the social repercussions of their creations as someone else's problem,[9] the publication of RFC 8280 is a sign of how far the internet engineering community has come from the notion that their work is morally neutral. Indeed, it is noteworthy that the very process that has historically been used to develop new technical protocols and standards (i.e., issuing RFCs), is now being used to explore the human rights impacts of those standards.

In this vein, RFC 8280 is part of a larger trend towards engineering standards development bodies concerning themselves with human rights. In 2016, for example, the Institute of Electrical and Electronic Engineers – a professional association for engineers that has developed standards for everything from synchronizing clocks (IEEE 1588) to Wi-Fi networking (IEEE 802.11) – announced the launch of a new 'Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems'.[10] In the last two years, this Initiative has published two versions of a guidance document called 'Ethically Aligned Design' that provides advice on how artificial intelligence systems can be designed to promote human well-being.[11]

In a similar vein, individual engineers have been becoming more active in considering and sometimes protesting against the social impacts of their creations. Consider, for

[6] Internet Research Task Force, 'IRTF Research Groups', https://irtf.org/groups (accessed 7 October 2018).

[7] Ibid.

[8] Internet Research Task Force, 'Human Rights Protocol Considerations', https://datatracker.ietf.org/rg/hrpc/about/ (accessed 7 October 2018).

[9] This traditional mindset is explored in Langdon Winter, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: University of Chicago Press, 1986).

[10] Raja Chatila et al, 'IEEE Global Initiative Aims to Advance Ethical Design of AI and Autonomous Systems', *IEEE Spectrum* (29 March 2017), https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/ieee-global-initiative-ethical-design-ai-and-autonomous-systems (accessed 5 October 2018).

[11] These documents are available at https://ethicsinaction.ieee.org (accessed 9 November 2018).

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

example, the recent resignation of a senior Google researcher following disclosures of the company's plans to offer a censored version of its search engine in China.[12] Or consider the employee backlash at Microsoft after a company blog highlighted its sale of deep learning and facial recognition technologies to US Immigration and Customs Enforcement (ICE), just as the agency's policy of separating children from their parents at the border was becoming a roiling public controversy.[13] The publication of RFC 8280 could not be more timely, therefore, nor could the work of identifying the human rights impacts of seemingly technical decisions be more pressing than at this crucial moment.

III. Examining RFC 8280 in Detail

This brings us to briefly consider the contents of RFC 8280, which has three main components. The first is a literature review on the limited body of writing that examines the relationship between the architecture of technical systems and internationally recognized human rights. The second attempts to map the relationship between human rights and the 'architectural' principles that underlie the protocols that the IETF and other similar bodies have devised to facilitate the exchange of information over electronic networks. The third and final part devises a questionnaire that developers of new protocols can use to explore and evaluate the human rights impacts of their creations before they are deployed in the wild.

The latter two-thirds of RFC 8280 are quite technical and do not make for light reading. For example, to identify the key architectural principles that underlie the most important protocols, the authors of the RFC describe how they ran the entire corpus of IETF RFCs through a text analyser, the outputs of which they further processed to identify 19 key concepts.[14] Some of these concepts will be familiar to the human rights community, such as privacy, anonymity and accessibility, while others are more technical in nature, such as heterogeneity support.

After mapping these architectural concepts to relevant rights enshrined in the Universal Declaration, the authors of RFC 8280 then proceed to examine the human rights impacts of eight common protocols and common 'networking paradigms'.[15] Some of the protocols they consider are household names, such as HTTP (described in more detail above), while others are not as widely known (such as XMPP – the eXtensible Messaging and Presence Protocol) yet important in their own right.

Those without a technical background might find the analysis that follows hard going, but the key theme that emerges is that technical trade-offs that were made in designing numerous key protocols create significant human rights risks – especially when

[12] Ryan Gallagher, 'Senior Google Scientist Resigns over "Forfeiture of our Values" in China', *The Intercept* (13 September 2018), https://theintercept.com/2018/09/13/google-china-search-engine-employee-resigns/ (accessed 6 October 2018).

[13] Sheera Frenkel, 'Microsoft Employees Protest Work with ICE, as Tech Industry Mobilizes Over Immigration', *New York Times* (19 June 2018), https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html (accessed 5 October 2018).

[14] ten Over and Cath, note 2, at 15–21.

[15] Ibid, 21–40.

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

compared with available alternatives that can achieve the same technical functions without posing the same human rights risks.

The HTTP protocol that underlies the World Wide Web provides an apt illustration of this phenomenon. As the HTTP protocol itself does not support encryption, communications sent using this protocol can be subject to various kinds of attacks that adversely impact the human rights of users.[16] For example, HTTP transmissions can be easily intercepted by third parties, or manipulated in any number of clever and inventive ways that impact the rights to privacy, free expression, and access to information – among others. These problems were amply demonstrated when the National Security Agency (NSA) and other intelligence agencies leveraged the security flaws in HTTP to engage in bulk surveillance of internet traffic.[17] Subsequent improvements to the HTTP protocol, including the development of the successor HTTPS protocol, have made things better by adding support for encryption, yet the situation is still far from ideal.

Certainly, developers of protocols like HTTP could not foresee the ways in which various actors would take advantage of its limitations to advance their own motives. Indeed, the very idea of conducting human rights due diligence before undertaking an activity that is likely to have significant human rights impacts did not become mainstream until the release of the United Nations Guiding Principles on Business and Human Rights in 2011. Moreover, at the time that key protocols such as HTTP were developed, the state of technology did not permit them to be designed in a manner that would make them more resistant to various forms of manipulation and interference.

This analysis of the human rights impacts of existing protocols and 'networking paradigms' begs the question of how engineers developing new protocols should approach their work. At first, the authors of RFC 8280 seemed to equivocate on this question, stating that:

> *The research group's position is that hard-coding human rights into protocols is complicated and changes with the context. At this point, it is difficult to say whether or not hard-coding human rights into protocols is wise or feasible.*[18]

Yet when the time comes for the authors of RFC 8280 to devise a questionnaire to help developers evaluate if new protocols 'adequately take […] specific human rights threats into account',[19] the authors come awfully close to advocating for the 'hard-coding' of human rights considerations into new protocols. This questionnaire, which is organized around each of 19 key 'architectural principles' that the HRPC Research Group identified through the text processing analysis described above, guides developers through a number of detailed technical questions that reflect hard lessons about how the presence or absence of certain features can result in poor human rights outcomes.

The authors clearly state that the considerations raised in the questionnaire are not exhaustive, and that there is likely to be a range of human rights considerations that the

[16] Ibid, 26–27.
[17] Ibid, 27–30.
[18] Ibid, 14.
[19] Ibid, 42.

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

questionnaire will fail to identify for protocols that are currently under development.[20] Even so, there is at least one instance where the structure and content of the questionnaire presupposes that 'hard-coding' human rights into protocols is a good thing.

Consider, for example, the identification of 'censorship resistance' as a key internet architectural concept, which in turn leads the authors of RFC 8280 to include a question asking developers if their creation can 'contribute to filtering in such a way that it could be implemented to censor data or services?'[21] If so, the authors of RFC 8280 go on to ask if 'your protocol [could] be designed to ensure that this doesn't happen?'[22]

This all seems well and good, but a difficulty arises from the manner in which the authors use the term 'censorship'. The term is, of course, a pejorative to refer to restrictions on free expression that are incompatible with international human rights law (notably Article 19 of the ICCPR). While every act of censorship implies a content restriction, not every content restriction constitutes censorship. Yet 'censorship resistance' as an architectural concept refers to developing network protocols in a manner that prevents third parties from interfering with the exchange of information online based on the content thereof. Therefore, asking engineers to design new protocols so that they cannot be implemented 'to censor data or services' would prevent rights-respecting governments from undertaking certain technical measures to block content that may be restricted pursuant to Article 19, at the same time as it bars non-rights-respecting governments from using the same technical measures to 'censor' content in violation of Article 19.

There is widespread agreement in the technical and policy communities that protocols should be designed to be 'censorship resistant' as the authors use the term, because there are alternative technical means available to rights-respecting governments for restricting online content consistent with Article 19. That said, both the identification of 'censorship resistance' as an architectural feature of modern communications protocols, and the guidance that RFC 8280 provides on designing censorship-resistant protocols, seems to recognize that human rights should at least sometimes be 'hard coded' into new protocols. If that is the case, the authors would do better to make their views explicit and clearly state that there are indeed circumstances where hard-coding human rights into protocols is necessary and appropriate.

IV. Conclusion

The publication of RFC 8280 is an important event that, along with other recent developments, signals how far the engineering community has come from the once-common view that human rights considerations are none of their concern. The document represents a valiant effort to systematically consider how the deep technical architecture of the communications network that has transformed every aspect of our lives impacts the enjoyment of our human rights in ways that range from obvious to obscure.

[20] Ibid, 41–42.

[21] Ibid, 47.

[22] Ibid.

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press

The analysis is not without its limitations, to be sure, but what is most heartening about RFC 8280 is that it represents the first output of a programme of work by the IRTF's HRPC Research Group to both examine the human rights impacts of existing protocols and develop meaningful guidance to ensure that the next generation of protocols is designed with human rights in mind. As of this writing, the HPRC has released three further draft documents that build upon the framework established in RFC 8280.[23] This is a worthy and worthwhile project that not only merits the support and involvement of the larger business and human rights community, but offers a compelling model for the development of human rights guidance in other sectors through the open and collaborative approach that has long been a hallmark of internet governance efforts.

[23] These documents are available at https://datatracker.ietf.org/rg/hrpc/documents/ (accessed 9 November 2018).

https://doi.org/10.1017/bhj.2018.30 Published online by Cambridge University Press