University of New South Wales Law Research Series

INTERNET ARCHITECTURE AND HUMAN RIGHTS: BEYOND THE HUMAN RIGHTS GAP

MONIKA ZALNIERIUTE AND STEFANIA MILAN

UNSW Law
UNSW Sydney NSW 2052 Australia

Editorial

Internet Architecture and Human Rights: Beyond the Human Rights Gap

Monika Zalnieriute

Allens Hub for Technology, Law & Innovation,
Faculty of Law, UNSW Sydney, Australia
m.zalnieriute@unsw.edu.au

Stefania Milan,

Department of Media Studies,
University of Amsterdam,
The Netherlands
s.milan@uva.nl

Abstract

Internet architecture and infrastructure are generally not at the top of the concerns of end users, and the overlying logical arrangements of root services, domain names, and protocols remain largely invisible to its users. Recent developments, however— including massive user data leakages, hacks targeting social networking service providers, and behavioral micro-targeting—have turned a spotlight on Internet governance defined broadly, and its relationship with civil liberties and human rights. The articles in this special issue examine the policymaking role of influential private intermediaries and private actors such as ICANN in enacting global governance via Internet architecture, exploring the implications of such a mode of governance for human rights. They consider: to what extent are human rights standards mediated and set via technical infrastructure, such as the DNS and platform policies, rather than by governmental structures? What are the implications of governance via Internet architecture for individual human rights? And what frameworks—be they legal, technological or policy-related—are needed to address the contemporary privatization of human rights online, in order to ensure the effective protection of human rights in the digital age?

KEY WORDS: Internet governance, human rights, IGF, ICANN, Internet architecture, DNS, civil liberties

Introduction

"Frequently mundane to the point of boredom" (Star, 1999, 377), Internet architecture and infrastructure are generally not at the top of the concerns of end users. The complex entanglement of hard-wired infrastructure—think of exchange points, cables and satellites, and the very same internet backbone—and overlying "logical" arrangements such as root services, domain names and protocols, remains largely invisible to its user base. It is typically taken for granted. It *might* become an explicit object of reflection and/or concern when its performance is inadequate or when it exposes individuals and groups to tangible, fathomable risks—from privacy infringement to censorship, all the way to online harassment.

Curiously, in the age of maturity for the World Wide Web—it has been thirty years since Tim Berners-Lee's magical intuition—we find ourselves at a crucial turning point. While Internet infrastructure per se is not explicitly "broken," a number of recent scandals of global resonance have exposed the fragility of the Internet ecosystem broadly defined—that is, including not only the internet architecture *strictu sensu*, but also the economic and societal layer of internet governance (cf. Internet Corporation for Assigned Names and Numbers, 2015). The resurgence of propaganda under the guise of so-called "fake news" (Bradshaw and Howard, 2018), with its corollary of draconian legislative fixes (cf. Strossen, 2018); massive user data leakages and hacks targeting social networking service providers like Facebook (e.g., Heaven, 2018); and the infamous behavioral micro-targeting undertaken by Cambridge Analytica (Ward, 2018), have marked the coming of age of the mass of unsuspecting users (Marda and Milan, 2018). Meanwhile, private actors such as platform operators have taken up an unelected role as the "new governors" of online speech (Klonick, 2018), de facto operating as private proxies easing the global application of national regulations (Belli et al., 2017) and promoting "the privatization of human rights" (Taylor, 2016, 763; DeNardis and Hackl, 2015).

All in all, these critical developments pose a serious "threat to our lifestyle online" (Marda and Milan, 2018, 1). Most importantly, they have turned a spotlight on the governance of the internet broadly conceived, including the management of data flows more generally. They have made the underlying infrastructure a tad less invisible. And they have irremediably tied the realm of the "invisible functioning" to very human, down-to-earth concerns such as freedom of expression, privacy, and data ownership. Suddenly, internet infrastructure has moved from the stuff of abstract digits and switches to a matter of civil liberties and human rights—something of concern to those who care about the functioning of liberal democracies and the enjoyment of human rights by individuals and groups.

The Human Rights Gap

Whereas governments are formally tasked with setting regulatory policies and human rights standards, in the digital environment the public sector often delegates this regulatory responsibility to private actors. Thus, public sector participation in the regulation of human rights in the digital sphere is very limited and primarily relies on private sector "notice and takedown procedures" for enforcement of copyright infringement, libel or other content that is considered illegal. Various private actors—such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN)—as well as platform and service providers such as Google and Facebook, do *de facto* govern and mediate human rights on the Internet via their standard contractual clauses and Internet design (e.g., Domain Name System and algorithms, see Zalnieriute, 2017). Yet these actors and Internet architecture are mostly invisible in our everyday life. These characteristics and lack of regulatory intervention and public sector participation have been described as a digital "global default" (Wagner, 2016), whereby private actors establish boundaries to human rights online—most notably freedom of expression, data protection, and privacy—*in accordance with* their respective business models. And in the context of this omnivorous global default, the basic tools of accountability and governance—public and legal pressure—have lost their teeth, with private actors holding most of the power (Buni and Chemaly, 2016).

We argue that there is a vacuum which occurs when human rights are public (at least for now *only* state actors can be sued for not respecting human rights; Deva and Bilchitz 2017) and the Internet architecture—through which human rights online are largely mediated and governed today—is mainly privately owned or privately operated. This vacuum creates what we call a "human rights gap" whereby the delegation of human rights enforcement to private actors circumvents both international human rights law, and often domestic laws and constitutions as well.

These developments hardly find any resonance with the user and developer imaginaries long associated with the World Wide Web, and the utopias and ideology built on them (see Flichy, 2007; Mansell, 2012; Lesage and Rinfret, 2015). To be sure, individual rights such as freedom of speech have played a key role in the design of the internet as we know it (see, for example, Turner, 2006). As the internet mythology goes, the evolution of the inter-network "depends on rough consensus about technical proposals, and on running code" (Carpenter, 1996). For better or for worse, however, values have been wired into the architecture of the network (DeNardis, 2009). But when we look at the kernel of the Internet, so to speak, we see that the battle for connecting the internet architecture to the respect and enjoyment of human rights worldwide is a somewhat recent concern. Even when the organized civil society—historically a proactive actor in the global Internet governance debate (Mueller et al., 2004)—has from time to time lobbied for privacy, fair use, and freedom of expression within, for example,

ICANN; "human rights" as an organic whole have not always served as a frame of reference for advocacy in the hard-core internet governance realm (Milan and ten Oever, 2017).

Recent unprecedented windows of opportunity have caused the tide to turn. Most notably, in March 2014 the US Department of Commerce announced that it would release its stewardship functions over the Domain Name System (DNS) (National Telecommunications and Information Administration, 2014). Shortly afterwards, the Council of Europe published a landmark study on the human rights implications of the DNS (Zalnieriute and Schneider, 2014). A number of nongovernmental organizations became active within ICANN as well as the IETF, lobbying for human rights in these key arenas (see, e.g., Cath and Floridi, 2017).

But while there is a growing recognition among a variety of members of the international Internet (governance) community that particular features of the Internet architecture—such as Internet protocols and domain names, as well as algorithms and standard contractual clauses of platforms—create conditions for setting *de facto* global standards on human rights and lead to privatized human rights governance, the scholarly understanding of these issues is still in the making.

A Gap in the Literature

The management of key Internet resources, the structure and dynamics of the global Internet Governance regime, as well as the legitimacy and accountability of its structures, and various other aspects related to Internet policymaking have been the topic of intense academic debate (see, among others, Bygrave, 2015; DeNardis, 2009, 2014; Goldsmith and Wu, 2008; Mueller, 2010a). Much of the legal, sociological and political science scholarship exploring the intersection of technology and human rights has focused primarily on Internet *content* and its implications for human rights (e.g, Lucchi, 2014; Jørgensen et al., 2006; Venturini et al., 2016; Jørgensen, 2017), at the expense of the less visible area of the *technical (infra)structure* supporting that very same digital content. Legal scholarship has for a long time focused primarily on the role of states and policies in governing (or not governing) the Internet (Goldsmith and Wu, 2008; Bygrave and Bing, 2009; Radu et al., 2014). Similarly, political science has paid much attention to the role of state institutions, multilateral relations and the overall geopolitics of power as it is mediated by the digital (e.g., Deibert, 2009; Nye, 2011; Zittrain, 2008). Ambitious literature has however emerged with a focus on technical structures of information technologies, with the aim of advancing our conceptual understanding of the dynamics at play within the most technical aspects of Internet governance. This embraces classical claims that "code is law" (Lessig, 2006), grand systemic views on the intertwining of information, law, and infrastructure (Braman, 2009), and more recent articulations of an infrastructure-based theory of Internet governance (DeNardis, 2014, 2012; Musiani et al., 2016). Innovative case studies have scrutinized, for instance, how the DNS's

technical infrastructure has been occasionally coopted as a tool of global power (Bradshaw and DeNardis, 2016), and how, conversely, infrastructure comes to constitute institutions (Musiani, 2016). Yet this debate has not been explicitly framed in terms of human rights until very recently (e.g., Zalnieriute and Schneider, 2014; Cath and Floridi, 2017; ten Oever and Cath, 2017; Zalnieriute 2017, 2019).

Amid this background, this special issue attempts to move beyond those legal scholarship narratives exaggerating the "technological neutrality" of the Internet, and that political science literature focused on observing merely the role of the state and associated multilateral relations. Rather, this collection intends to give an adequate consideration to the policymaking role of influential private intermediaries and private actors, such as ICANN, in enacting global governance via Internet architecture, exploring the implications of such a "mode" of governance for human rights. To broaden our understanding of the complex relation between fundamental rights online and internet architecture broadly defined, this special issue thus asks to what extent public interest concerns, and human rights in particular, are (re-)mediated by relying on particular qualities of the Internet architecture broadly defined. To what extent are human rights standards mediated and set via technical infrastructure, such as the DNS and platform policies, rather than by governmental structures? What are the implications of *governance via Internet architecture* for individual human rights? And last, but not least, what frameworks—be they legal, technological or policy-related—are needed to address the contemporary privatization of human rights online, with a view to ensuring the effective protection of human rights in the digital age?

Governance via Internet Infrastructure: An Interdisciplinary Conversation

To tackle these questions and fill the gap in the literature, the five contributions to this special issue leverage a variety of disciplinary and conceptual lenses. They draw upon the work of, among others, DeNardis (2009, 2012, 2014), Lessig (2006), Mueller (2010b), Wu and Goldsmith (2008), Wu (2010) and Balkin (2014) on *governance through architecture*. They dialogue with a variety of disciplinary approaches, such as critical political economy and/or Science and Technology Studies (STS). STS is particularly relevant for this collection, as it pays attention to how our digital communications are not merely defined by their *content*, but also by the institutional and technological *structures* underpinning said content. In other words, STS aims to bring technology itself into the game, and approach it not merely as a target for regulation, but as part of the complex arrangements of communication environments (cf. Epstein et al., 2016). Finally, the articles rely on a variety of empirical sources and methods, from qualitative to automated analysis. Interestingly, the authors include both distant observers and individuals who have played—or still play—key roles as advocates within Internet governance arenas, such as ICANN and the IETF.

Ranging from the role of private actors in policy development to civil society advocacy within private corporations, the contributions in the special issue form a solid point of departure to explore the present and future of Internet architecture in relation to human rights. The articles offer empirically informed case studies on how various private bodies have developed policies related to Internet architecture which support or have led to violations of human right principles such as to rights to privacy, data protection, freedom of expression and assembly, among others.

In the first contribution, Samantha Bradshaw and Laura DeNardis dive into the privacy implications wired in the technical architecture of the DNS managed by ICANN. Looking at the WHOIS system (the global database of domain registrants) and privacy in domain name queries the authors observe how cross-border technologies like the DNS often collide with the law and government regulations. Because "privacy is often not just about personal safety and reputation," domain name policy contributes to "shap[e] what counts as freedom of expression online" (Bradshaw and DeNardis, 2019). It is thus imperative, they argue, to find solutions that consider both privacy and security values, such as confidentiality, data integrity, and verification.

In the second contribution, Niels ten Oever builds on his experience as a human rights advocate within ICANN to reflect on what the organized civil society rightly considers a success story: in 2016, ICANN included a respect for "internationally recognized human rights" as one of its Core Values enshrined in the organization's Bylaws. Combining ethnographic observations with document analysis, ten Oever shows how human rights functioned a "boundary object", an "arrangement which allows people to achieve some form of coordination without necessarily requiring consensus" (ten Oever 2018, 3). Thanks to its interpretive flexibility, the notion of human rights could be embraced by distinct stakeholders with diverging agendas.

Ten Oever's (widely shared) optimism is questioned by Internet governance scholars and policy advocates Milton Mueller and Farzaneh Badiei (2018, 3), whose normative article offers a cautionary tale on—and, they argue, a "more realistic approach" to—the relation between Internet architecture and human rights. Investigating the efforts of human rights advocates within the IETF and bringing their arguments to bear on existing Internet governance and STS scholarship, the authors critically examine the claim that standards and protocols can advance human rights and that "engineers have an ethical responsibility to be aware of the human rights implications of their design decisions."

In the fourth contribution, Nicolas Suzor, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen (2018) move away from the institutional focus on ICANN and DNS-mediated governance to instead explore the responsibilities of social media platforms in tackling gender-based violence and harassment online. They explore the potential of non-legal standards as instruments able to identify the responsibilities of Internet intermediaries, which have been reluctant to tackle the problem on the basis of their supposed neutrality. Thanks to its "multivalent approaches to developing effective remedies" (2018, 15), the human rights framework,

they argue, "can provide a specific set of demands for concrete change" in the hands of states and civil society groups" (2018, 5).

Finally, Ben Wagner brings the special issue to a close by taking us one step further and analyzing the role of human agency in automation and non-automation in Internet architecture, contributing to future-proofing this debate. Arguing that "human decision making is an important part of what could be considered to be a human right-based Internet Architecture" (2019, p. XX), Wagner's work explicitly questions the technical neutrality claim, looking at the invisible human labor that goes into the functioning of, respectively, self-driving cars, police border searches based on passenger name search, and content moderation on social media. The article also elaborates a set of criteria needed to ensure meaningful decision-making in automated technical systems.

Conclusion

This special issue supports the idea that human rights issues and governance online are not only dependent on Internet *content* or *usage*—rather they also rest on the complex, underlying system of technological *architecture* that supports the Internet as we know it. Various features enabling or constraining the exercise of our fundamental rights online are wired into the technical architecture of the Internet and incorporated into various policies and *modus operandi* of actors creating and/or managing that architecture. While end users commonly assume that the Internet technology is neutral, the implications of the ever-growing privatization of human rights enforcement via Internet architecture and private policies by actors, such as social media platforms and ICANN, are huge and profound, not least because such privatization in essence circumvents the protections afforded to individuals by the international human rights framework. The political and civic power held by these various private actors exercising influence on the Internet architecture does not seem to be diminishing—quite to the opposite, it appears to be expanding at a fast pace.

This expanding power of private actors means an ever-widening human rights gap, which could only be inhibited or at least paused by imposing legally binding human rights obligations on these private actors. It is obvious by now that the human rights discourse alone is insufficient to address the wider problems of the globalized economy and of the regulatory capitalism from which many of the private human rights governance issues arise. Nonetheless, it is clear that in the context of the Internet architecture broadly conceived, it is private actors who very often determine and establish *de facto* human rights standards; and there is no reason why they should not be treated as agents bearing some of the obligations flowing from these very rights. Otherwise the human rights gap will keep widening, and our fundamental rights online will keep retreating. But there is more work to do—in the long run, we need to reimagine human rights too, if we are to address the challenges of our increasingly complex digital present.

Acknowledgments

References

Balkin, J.M., 2014. Old-School-New-School Speech Regulation. Harward Law Rev. 127, 2296–2342.

Belli, L., Francisco, P.A., Zingales, N., 2017. Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police, in: Platform Regulation. How Platforms Are Regulated and How They Regulate Us. FGV Direito, Rio de Janeiro, pp. 41–64.

Bradshaw, S., DeNardis, L., 2019. Privacy by Infrastructure: The Unresolved Case of the Domain Name System. Policy Internet.

Bradshaw, S., DeNardis, L., 2016. The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. New Media Soc. 20, 332–350. https://doi.org/10.1177/1461444816662932

Braman, S., 2009. Change of state: Information, policy, and power. MIT Press.

Brandshaw, S., Howard, P.N., 2018. The global oragnization of social media disinformation campaigns. J. Int. Aff. 71, 23–32.

Buni, C., Chemaly, S., 2016. The secret rules of the internet. The murky history of moderation, and how it's shaping the future of free speech. The Verge.

Bygrave, L., 2015. Internet Governance by Contract. Oxford University Press, Oxford.

Bygrave, L.A., Bing, J., 2009. Internet Governance. Infrastructure and Institutions. Oxford University Press, Oxford.

Carpenter, B.E. (Ed.), 1996. Architectural Principles of the Internet (RFC 1958).

Cath, C., Floridi, L., 2017. The design of the internet's architecture by the Internet Engineering Task Force (IETF) and Human Rights. Sci. Eng. Ethics 23, 449–468.

Deibert, R.J., 2009. The geopolitics of internet control: censorship, sovereignty, and cyberspace, in: Chadwick, A., Howard, P.N. (Eds.), The Routledge Handbook of Internet Politics. Routledge, London, pp. 323–336.

DeNardis, L., 2014. The Global War For Internet Governance. Yale University Press.

DeNardis, L., 2012. Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance. Inf. Commun. Soc. 15, 720–738.

DeNardis, L., 2009. Protocol Politics: The Globalization of Internet Governance. MIT Press, Cambridge, MA.

DeNardis, L., Hackl, A.M., 2015. Internet Governance by Social Media Platforms. Telecommun. Policy 39, 761–770.

Deva, S., and Bilchitz, D., eds. *Building a Treaty on Business and Human Rights: Context and Contours.* Cambridge University Press, 2017.

Epstein, D., Katzenbach, C., Musiani, F., 2016. Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions. Internet Policy Rev.

Flichy, P., 2007. The Internet imaginaire. MIT Press, Cambridge, MA.

Goldsmith, J., Wu, T., 2008. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, Oxford.

Heaven, D., 2018. Massive Facebook data breach left 50 million accounts exposed. NewScientist.

Internet Corporation for Assigned Names and Numbers, 2015. The logical layer of Digital Governance [WWW Document]. URL https://www.icann.org/news/multimedia/1993

Jørgensen, R.F., 2017. What Platforms Mean When They Talk About Human Rights. Policy Internet 9, 280–296. https://doi.org/10.1002/poi3.152

Jørgensen, R.F., Drake, W.J., Wilson, E.J., 2006. Human rights in the global information society. MIT Press, Cambridge, MA.

Klonick, K., 2018. The new governors: The people, rules, and processes governning online speech. Harv. Law Rev. 131, 1559–1670.

Lesage, F., Rinfret, L., 2015. Shifting imaginaries of the web. First Monday 20.

Lessig, L., 2006. Code 2.0. Basic Books, New York.

Lucchi, N., 2014. Internet Content Governance and Human Rights. Vanderbilt J. Entertain. Technol. Law 809–856.

Mansell, R., 2012. Imagining the Internet: Communication, innovation, and governance. Oxford University Press, Oxford.

Marda, V., Milan, S., 2018. Wisdom of the Crowd: Multistakeholder perspectives on the fake news debate. Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA.

Milan, S., ten Oever, N., 2017. Coding and encoding rights in internet infrastructure. Internet Policy Rev. 6. https://doi.org/10.14763/2017.1.442

Mueller, M.L., 2010a. Networks and States: The Global Politics of Internet Governance. MIT Press, Cambridge, MA.

Mueller, M.L., 2010b. Networks and States. The Global Politics of Internet Governance, Information Revolution and Global Politics. MIT Press, Cambridge, MA and London, England.

Mueller, M.L., Badiei, F., 2018. Requiem for a Dream: On Advancing Human Rights via Internet Architecture. Policy Internet 0. https://doi.org/10.1002/poi3.190

Mueller, M.L., Page, C., Kuerbis, B.N., 2004. Civil Society and the Shaping of Information-communication Policy: Four Decades of Advocacy. Inf. Soc. 20, 169–185.

Musiani, F., 2016. Alternative Technologies as Alternative Institutions: The Case of the Domain Name System, in: Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S. (Eds.), The Turn to Infrastructure in Internet Governance. Palgrave Macmillan, Basingstoke, UK, pp. 73–86.

Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S., 2016. The Turn to Infrastructure in Internet Governance. Palgrave Macmillan, Basingstoke, UK.

National Telecommunications and Information Administration, 2014. NTIA Announces Intent to Transition Key Internet Domain Name Functions [WWW Document]. URL https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Nye, J.S., Jr., 2011. The Future of Power. PublicAffairs, New York.

Radu, R., Chenou, J.-M., Weber, R.H. (Eds.), 2014. The Evolution of Global Internet Governance Principles and Policies in the Making. Springer, Cham.

Star, S.L., 1999. The Ethnography of Infrastructure. Am. Behav. Sci. 43, 377–391.

Strossen, N., 2018. Hate: Why We Should Resist It with Free Speech, Not Censorship. Oxford University Press, Oxford.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., Van Geelen, T., 2018. Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online. Policy Internet 0. https://doi.org/10.1002/poi3.185

Taylor, E., 2016. The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality.

ten Oever, N., 2018. Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN. Policy Internet. https://doi.org/10.1002/poi3.172

ten Oever, N., Cath, C., 2017. Research into Human Rights Protocol Considerations (RFC 8280).

Turner, F., 2006. From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. University of Chicago Press, Chicago.

Venturini, J., Louzada, L., Maciel, M.F., Zingales, N., Stylianou, K., Belli, L., Magrani, E., 2016. Terms of service and human rights: An analysis of online platform contracts. Revan.

Wagner, B., 2019. Algorithms, Automation and Human Agency: Can avoiding Quasi-Automation enable Human Rights in Internet Infrastructure? Policy Internet.

Wagner, B., 2016. Governing Internet Expression: Sketching Out the Borders of a Global Default of Freedom of Expression, in: Wagner, B. (Ed.), Global Free Expression - Governing the Boundaries of Internet Content. Law, Governance and Technology Series. Springer, Cham, pp. 121–136.

Ward, K., 2018. Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. J. Media Ethics 33, 133–148. https://doi.org/10.1080/23736992.2018.1477047

Wu, T., 2010. The master switch: The rise and fall of information empires. Random House, New York.

Zalnieriute, M., "The anatomy of neoliberal Internet governance: A queer critical political economy perspective." in Otto, D. (ed) *Queering International Law*. Routledge, 2017. 53-73.

Monika Zalnieriute, 'Digital Rights of LGBTI Communities: A Roadmap for Dual Human Rights Framework, in Wagner, B. *et al* (eds), *Research Handbook on Human Rights and Digital Technologies*, Edward Elgar, 2019.

Zalnieriute, M., Schneider, T., 2014. A Council of Europe analysis on ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values. Council of Europe, Strasbourg.

Zittrain, J.L., 2008. The Future of the Internet - And How to Stop It. Yale University Press.