Leiden Journal of International Law (2020), **33**, pp. 249–252
doi:10.1017/S092215651900058X

BOOK REVIEW

Molly K. Land and Jay D. Aronson, *New Technologies for Human Rights Law and Practice*, 2018, Cambridge University Press, 330 pp, ISBN 9781107179639
doi:10.1017/S092215651900058X

In this edited volume, a diverse set of perspectives is brought together in a timely examination of human rights law and practice in the digital age. The different contributions are grouped into three sections within the book. The first Part, titled 'Normative Approaches to Technology and Human Rights', illustrates the range of ways in which technology and human rights intersect and interact, including in relation to climate change, assisted reproduction, water metres, and automated weapons. Part two, on 'Technology and Human Rights Enforcement', moves onto topics pertaining to the role that technology can play in human rights fact finding, investigation, and documentation. Finally, in Part three, titled 'Beyond Public/Private: States, Companies, and Citizens', the contributions tackle forward looking questions concerning the presence of non-State actors in the online space and the effects of this on human rights.

At the volume's centre lies the dichotomy that underpins the majority of writing in this area: opportunity vs risk. On the one hand, new technologies offer innovative ways to protect and secure human rights; on the other hand, they can create new harms, new ways in which human rights can be violated, and can entrench existing inequalities. In some instances, the same technology can give rise to both these possibilities, as Chapters 3 and 9 show. In Chapter 3, Shabalala describes innovations that can help mitigate the negative effects of climate change, but also notes how these technologies are often not available to the most vulnerable populations (hence, the author argues, the need for a human rights approach to technology transfer). In Chapter 9, McPherson explains that technologies such as social media allow NGOs to reach a broader audience with their human rights advocacy work, but also notes how the design of social media makes larger, better funded, NGOs more visible than smaller ones.

Importantly, however, the editors note in the introductory chapter that the aim of the volume is also to move the discussion on from this focus on opportunity vs risk. Land and Aronson articulate a 'human rights approach to technology' that is based on two tenets: (i) using international human rights law as a source of normative commitments, and (ii) looking to human rights practice for accountability strategies. The normative underpinnings of international human rights law – identified by Land and Aronson as including universality, indivisibility, interdependence, equality, and accountability – are said to provide insights into how technology should be approached from a human rights perspective. These ideas return in various individual chapters, such as in Chapter 2 where Shaver describes the need for participation, inclusion, and equality when new technologies are introduced into communities (in this case, pre-paid water metres that were introduced in poor townships in South Africa). Land and Aronson, and the respective authors, are not alone in turning to international human rights law standards when searching for a normative framework to govern technology. For example, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has argued in favour of approaching content moderation and artificial intelligence in online spaces through a human rights lens;[1] furthermore, the UN High Commissioner for Human Rights has set out the need for a human rights based approach to bridging the gender digital divide.[2] As the rapidity of technological development outstrips the pace of effective regulation, the normative standards of international human rights law are often turned to as a way to bridge the gap.

The second tenet of Land and Aronson's 'human rights approach to technology' looks to human rights accountability practices in order to understand the role that technology can play in enforcing human rights. This is an important element of the discussion, as it addresses issues surrounding the effectiveness of human rights law, and how technology can both help and hinder human rights enforcement. Part two of the book focuses strongly on this element, with chapters on how user generated content – whether videos, photos, or reports – can help human rights investigators (Chapter 6), and on the use of data visualisation in human rights advocacy (Chapter 8). Indeed, this part of the book more than justifies the inclusion of the term 'practice' in the book's title, with some of the contributions taking on an almost encyclopaedic quality in their description of various practices of using technology for human rights accountability.

In its approach to accountability, the book has a clearly discernible focus on forms of accountability connected with advocacy and civil society work, rather than on institutional forms of accountability. On the one hand, this is to be welcomed; the important work of NGOs is often an overlooked element in the accountability landscape, particularly in the context of legal discussions. Lawyers focus instead on the role of domestic or international courts, or intergovernmental fact-finding bodies. And yet, the awareness raising work that NGOs perform can be an important factor in bringing a situation of human rights violations to the attention of these accountability institutions. On the other hand, in not addressing these more formalised forms of accountability, the book fails to cover an important area of practice for the enforcement of human rights, and one where technology is playing an increasingly important role.

Recent fact-finding missions established by the UN Human Rights Council have demonstrated clearly the role that technology can play in substantiating allegations of human rights violations in an institutional setting. In the 2019 report of the Commission of Inquiry on the protests in the Occupied Palestinian Territory, videos and photos from social media were used to support findings that the targeting of certain individuals by Israeli forces was unlawful.[3] Social media content was also crucial in the 2018 Fact Finding Mission on Myanmar report, to the extent that social media posts were used to support an inference of genocidal intent on the part of members of the Myanmar military with respect to the killing of Rohingya Muslims.[4] While these fact-finding missions issued their reports after the present book was already published, the role of technology in the work of UN fact finding missions has been growing for some time. In 2012, the International Commission of Inquiry on Libya delivered a report that relied on extensive satellite imagery analysis.[5] The images were used, *inter alia*, to assess damage to buildings and to investigate

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HR/38/35 (2018) and Promotion and protection of the right to freedom of opinion and expression, UN Doc. A/73/348 (2018).

[2] Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective: Report of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/35/9 (2017).

[3] Report of the detailed findings of the independent international Commission of inquiry on the protests in the Occupied Palestinian Territory, UN Doc. A/HRC/40/CRP.2 (2019). See, for example, the findings concerning Abed El Fatah Nabi at para 423 and those concerning Mohammad Ayoub at para 515.

[4] Report of the independent international fact-finding mission on Myanmar, UN Doc. A/HRC/39/64 (2018), at paras. 86–7.

[5] Advance Unedited Version, Report of the International Commission of Inquiry on Libya, UN Doc. A/HRC/19/68 (2012).

https://doi.org/10.1017/S092215651900058X Published online by Cambridge University Press

whether bombed areas had been legitimate military targets due to military activity taking place there.[6] The 2014 report of the Gaza Commission of Inquiry refers to two videos posted on an unofficial IDF YouTube channel when assessing whether buildings in a given area had been targeted and damaged.[7] As this short overview shows, there was existing institutional practice at the time of writing that could have been explored as part of the intersection between technology and human rights enforcement and accountability, and which would have added greater breadth to the topics explored in the volume.

An overall aspect of the book that is especially worth noting is the fact that a number of chapters move the discussion on key legal issues concerning human rights and technology into new territory. Two such issues will be commented upon here (although the book offers a number that could be mentioned): privacy and extraterritoriality, and private actors in the online domain.

Discussions on privacy in connection with technology are by no means new, and recent scandals have ensured that privacy has remained a prominent topic in public debate.[8] However, in Chapter 10, Brunner raises a less often considered issue: how the right to privacy operates extraterritorially in the online context. Traditionally, a state's extraterritorial human rights obligations have been tied to the notion of effective control, a concept that was developed for the physical world, rather than the virtual one. Yet such concepts are, according to Brunner, ill-suited for digital communications in the internet age. In the context of modern surveillance operations, a state may access data about an individual in circumstances where neither the data nor the individual are located on its territory or subject to its effective control. An example of this is the United States CLOUD Act, a piece of domestic legislation that empowers US authorities to compel US service providers to disclose data in their possession, even if the data is located abroad and pertains to non-nationals located abroad.[9] In such situations, questions emerge as to whether the surveilling state would be subject to extraterritorial obligations to respect and ensure the privacy of such individuals, with disagreements persisting as to how the law does and should operate under these circumstances. In her chapter, Brunner explores the arguments surrounding this issue, and suggests that the European Union's General Data Protection Regulation may go some way to filling the gap.

Turning to the issue of private actors in the online domain, in Chapter 11 Jørgensen tackles the difficult question of how human rights can be protected online when the online space is owned by private actors. Her statement that 'access to the Internet and participation in discourse through the Internet have become integral parts of modern life',[10] will resonate with many readers, but the challenges that arise from the fact that this discourse takes place on privately-owned platforms are less well known and understood. The problem can be illustrated by the example of content moderation on social media. Social media platforms – such as Facebook, Twitter, YouTube – are now key mediums of communication. As such, they are important spaces for the exercise of free speech, access to information, and freedom of opinion. However, the fact that these platforms are privately

[6] See, for example, ibid., at paras. 640–6 and Annex IV.

[7] Report of the detailed findings of the independent commission of inquiry established pursuant to Human Rights Council resolution S-21/1, UN Doc. A/HRC/29/CRP.4 (2015), at para. 281.

[8] In the course of 2018 alone, we saw a number of stories about data breaches: M. Isaac and S. Frenkel, 'Facebook Security Breach Exposes Accounts of 50 Million Users', *New York Times*, 28 September 2018, available at www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html; D. MacMillan and R. McMillan, 'Google Exposed User Data, Feared Repercussions of Disclosing to Public', *Wall Street Journal*, 8 October 2018, available at www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194; B. Logan, 'Facebook suspends Cambridge Analytica, a controversial data-analysis firm linked to the Trump campaign', *Business Insider*, 17 March 2018, available at www.businessinsider.in/facebook-suspends-controversial-data-analysis-firm-cambridge-analytica-from-its-platform/articleshow/63340337.cms.

[9] D. Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0', (2018) 71 *Stanford Law Review Online* 9, at 11.

[10] R. F. Jørgensen, 'Human Rights and Private Actors in the Online Domain', in M. K. Land and J. D. Aronson (eds.), *New Technologies for Human Rights Law and Practice* (2018), 243, at 253

https://doi.org/10.1017/S092215651900058X Published online by Cambridge University Press

owned means that the companies that own them also control who has access to them and what can be shared there. In recent years this has been a challenging issue, as governments have exerted pressure on social media companies to take down certain types of content, in particular content connected to terrorism and hate speech.[11] There are strong justifications for this, but the ambiguity surrounding the meaning of the terms 'terrorism' and 'hate speech' can lead to social media companies being overly broad in their removals, thereby negatively affecting free speech and leaving those affected with no recourse or remedy. In the chapter Jørgensen sets out different frameworks, of both the soft law and hard law varieties, that may be applicable to this type of situation, and addresses both responsibilities that may exist for the private companies themselves and obligations that exist for States with respect to those companies. While this field is still developing and many issues remain unsettled, Jørgensen's chapter takes important steps in laying the groundwork for future discussions.

In their introductory chapter, the editors reiterate that one of the aims of the book is to spark conversations: conversations between human rights practitioners and technologists, conversations about the potential and the dangers of technology in protecting human rights, and conversations between those working in different areas of human rights and technology. In this respect, the volume certainly succeeds. And yet, to some degree, the book falls into the trap that affects a great many edited volumes; namely, a certain lack of cohesion between the individual chapters. The editors set out cross cutting themes at the outset of the book, and on close inspection the individual chapters do tie in with the two tenets of the 'human rights approach to technology' articulated in the introduction. However, the varying approaches taken by the respective authors – ranging from singular case studies, to overviews of practice, to analyses of both particular and general legal issues – means that it is hard to identify just one core message at the heart of the volume. That being said, the plethora of messages that is does convey makes it a great platform from which to launch new research, and the book is an important and timely contribution to the growing field of human rights and technology.

Emma Irving[*]

[11] The EU has been a strong player in exerting this pressure, with the European Commission issuing a code of conduct and inviting social media companies to sign up ('European Commission and IT Companies announce Code of Conduct on illegal online hate speech', European Commission Press Release, 31 May 2016, available at www.europa.eu/rapid/press-release_IP-16-1937_en.htm. More recently, the EU has initiated efforts to impose legal obligations on social media companies to take down problematic content within short timeframes ('Terrorist content online: Council adopts negotiating position on new rules to prevent dissemination', European Council Press Release, 6 December 2018, available at www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/. Legal measures of this type have already been taken by Germany in its 2017 Network Enforcement Act.

[*] Assistant Professor of Public International Law, Grotius Centre for International Legal Studies, Leiden Law School, Leiden University [e.irving@law.leidenuniv.nl].

https://doi.org/10.1017/S092215651900058X Published online by Cambridge University Press