Human Rights in the Digital Age: Inclusive Policies on Data Privacy

Violette Khammad, Bryn McAuley, Sarah Murray and Naomi Pearson

Issue

States and corporate actors are using new technologies to commit mass human rights violations, and existing international human rights norms, laws and enforcement mechanisms are insufficient to protect vulnerable populations in the digital age.

Background

The ongoing digital transformation is having a profound impact on human rights. While human rights norms and laws recognize the right to privacy, the global human rights regime was not designed to protect people from the advanced surveillance tactics and technologies used today by state and corporate actors (United Nations General Assembly [UNGA] 2014). More specifically, it was not designed to protect against violations that are enabled by the rampant collection of personal data, the abuse of geolocation technologies, the interference into personal communications and other rapidly advancing surveillance techniques, such as targeted acts of violence and other breaches of the security of the person (ibid.).

The protection of privacy — particularly the privacy of marginalized communities — will be the focus of this brief. This briefing note will make recommendations for strengthening the international human rights regime in five areas: advancing new international law protecting the right to privacy; enhancing the capacities of the Universal Periodic Review (UPR) and United Nations Special Procedures to address digitally enabled violations; updating UN Guiding Principles (UNGPs) assessment tools to include violations against vulnerable populations; championing a global certification scheme for the private tech sector; and amending the Rome Statute of the International Criminal Court to include corporate actors.

Each recommendation is informed by the Canadian government's dedication to gender inclusivity via Gender-based Analysis Plus (GBA+) policies and is intended to help Global Affairs Canada advance its top two priorities: strengthening the rules-based international order and furthering a feminist foreign policy.

Human Rights Violations in the Digital Age

There is an urgent need for an inclusive approach to protecting human rights in the digital age. Many states — democratic and non-democratic — are already forging ahead with mass state surveillance systems, some of which specifically target vulnerable minority populations. China's persecution of its Uyghur population is enabled by "wifi sniffers" that search for prohibited images by intercepting communications on personal devices (Zand 2018). Intelligence services in the United States and the United Kingdom have developed technologies providing access to massive quantities of private online communications (UNGA 2014). In addition, corporations are also acting independently in collecting vast troves of user data for advertising purposes while failing to protect user privacy. The US Federal Trade Commission is presently reviewing persistent breaches of user privacy by Facebook (Electronic

Privacy Information Center 2019), whose platform was also used to broadcast the Christchurch massacre (Willsher 2019) and facilitate genocide and mass atrocities in Myanmar (Mozur 2018).

Current Governance Models

There is little consensus among the major players as to which model of data governance should be adopted. While the global community acknowledges the need for the regulation of state and private actors' use of digital technologies, there are differing opinions as what form these regulations should take. In 2018, the European Union implemented the General Data Protection Regulation (GDPR) — a supranational law that governs companies that market online goods or services to EU citizens, regardless of where the company itself is located (De Groot 2019). The United States has traditionally adopted voluntary privacy regulations; however, there is a growing chorus of voices calling for greater regulation. California has recently implemented strict privacy-based legislation and US-based tech giants such as Google and Apple have advocated for comprehensive federal privacy legislation (Pichai 2019; Meyer 2018). China has developed a far-reaching regulation similar to the GDPR that applies only to private actors and is pseudo-voluntary (Sacks 2018). However, the Chinese government has prioritized national security over privacy and human rights and engages in mass state surveillance of its citizens (Dholakia and Wang 2019). One danger is that a model that only regulates private actors while exempting the state from regulation may be attractive to other illiberal and authoritarian states. Such an outcome would not be in Canada's interest; hence, the need to strengthen international human rights laws and norms in order protect the right to privacy.

A prevailing concern among states and businesses is that strong regulation will come at the cost of innovation and profit. Innovation Minister Navdeep Bains and Privacy Commissioner Daniel Therrien reject the narrative that data regulation is a zero-sum game (Soloman 2018). The Canadian public has indicated a desire for greater privacy protections (Office of the Privacy Commissioner of Canada 2016). As such, it is in the corporate interest to provide platforms that guarantee these protections for consumers.

International Law, Enforcement Mechanisms and the Right to Privacy

Currently, there is no comprehensive international treaty regulating state-led surveillance. In 2018, the UN Special Rapporteur on Privacy released a Working Draft Legal Instrument on Government-led Surveillance and Privacy. One possibility is for the legal instrument to take the form of a guiding principle, but the Special Rapporteur and other key stakeholders prefer that it form the foundation for a future international treaty (Office of the High Commissioner for Human Rights [OHCHR] 2018b). The treaty would apply to all law enforcement and intelligence agencies and would expressly prohibit arbitrary or unlawful surveillance. The draft text underscores that states must never target populations for surveillance on the basis of gender, religion, political opinion or other immutable characteristics. Canada's engagement with the treaty-drafting process could ensure that the text makes explicit mention of respect for diversity and inclusivity, and that the text notes the particular risks of state surveillance for women, girls and LGBTQ+ populations. The European Union was the key financial benefactor for the current draft and would be a crucial ally for Canada in promoting the adoption of the text as a treaty through the UN system.

Nonetheless, the adoption of new international human rights law is often a lengthy process that can take years, even decades. In the immediate term, Canada possesses the ability to strengthen the right to privacy via the UPR and the Special Procedures. With respect to the former, the protection of privacy has been evaluated in some states' reviews. However, this has not been done consistently. Similarly, digital privacy rights are being incorporated within some UN Special Procedures. For example, in 2018, the Special Rapporteur on violence against women released a report on web-based gender violence (Human Rights Council 2018). The Special Rapporteur on poverty has also made statements about the disproportionate impact of unregulated digital technologies on the poor (OHCHR 2018a). As with the UPR, not every monitoring body considers violations of privacy and its effect on vulnerable populations in their reviews. Granted, there are limits to what the UPR and UN Special Procedures can achieve. Neither represents a panacea that will guarantee the right to privacy. However, they remain important and legitimate vehicles for establishing new norms and improving human rights observance.

Private Actors and Respect for Human Rights: Innovative Approaches

Currently, private actors are governed through voluntary frameworks that attempt to influence their business practices. The UNGPs are used by large companies to report annually on their compliance with human rights norms via the SHIFT reporting framework. Neither the UNGP nor the Shift assessment database includes criteria protecting LGBTQ+ rights in their reporting. No other marginalized communities are included, and specific questions addressing gender equality and women's rights are not incorporated in reporting criteria regarding privacy and the protection of personal data (Shift 2019).

Similarly, certification schemes are a potential avenue to incentivize corporations to adopt human rights norms while encouraging innovation. The European Data Protection Certification (EDPC) is currently being tested among EU member states and is derived from the processes of the GDPR. However, the EDPC only certifies companies within EU member states, creating a gap among the remaining global community. Additionally, the EDPC is an opt-in process that only covers micro, small- and medium-level companies and, thus, does not incentivize larger companies such as Facebook or Google to participate. Still, although the EDPC is yet to be fully tested, it has great potential. Along with European allies, Canada is in an excellent position to champion a global certification scheme supported by the UNGP and a civil society reporting organization like Shift. By doing so, the certification would come with built-in brand recognition and a set standard of human rights observance, discouraging copycats who might wish to cheat the system and create their own certification in order to appear ethical without modifying their behaviour.

While voluntary standards can offer incentives for corporate compliance with human rights, they are ultimately insufficient for addressing corporate complicity in mass atrocities. There is a strong need to expand the purview of the Rome Statute of the International Criminal Court to include private actors. This would allow for the prosecution of senior business leaders whose companies perpetrate and enable mass atrocity crimes. Of course, expanding the scope of international criminal justice is a long-term objective and would undoubtedly face fierce resistance. However, the ease with which hate can be spread over social media — sometimes with fatal consequences — requires a bold response. Twenty years ago, Canada, along with like-minded allies and the Coalition for an International Criminal Court, led the charge to establish the International Criminal Court (ICC). Given this legacy, Canada is uniquely placed to lead efforts to expand the ICC's jurisdiction to include corporate actors.

Next Steps

There is an opportunity for Canada to mobilize support for inclusive, human rights-based international data and privacy regulation. Outside of the recommendations below there are further areas of interest for Global Affairs to consider in pursuit of global data governance. International forums such as the Group of Seven and the Organisation for Economic Co-operation and Development are additional avenues for Canada to lead and promote a GBA+ approach to data protection. To that effect, Canada recently attended a summit hosted by France and New Zealand on combatting online hate (Willsher 2019). To realize its priorities of strengthening the rules-based international order and supporting feminist foreign policy, it is crucial that Canada continues to participate and even take the lead in these discussions.

Recommendations

1. **Lead in the adoption of the UN Draft Legal Instrument on Government-led Surveillance and Privacy.** Canada is well-positioned to ensure the incorporation of gender inclusive language within the treaty text and champion the adoption of the treaty within the UN system. Recommending a low threshold for ratification — such as 20 states (the threshold for the Convention on the Rights of the Child) — would help prevent opposing states from delaying the treaty's adoption.

2. **Introduce a resolution at the Human Rights Council to mainstream the right to privacy in the Universal Periodic Review and the UN Special Procedures.** Canada should call for having every state's Universal Periodic Review assess data privacy protections. It should also lead efforts to expand the mandates of all Special Procedures in order to ensure that digital privacy rights are considered from multiple lenses, for example, acknowledging the effect of technology on gender-based violence.

3. **Lead an international effort to update the reporting mechanism for the UNGPs Assessment Framework to require inclusivity and intersectionality via the Shift disclosure database.** Shift currently works with over 130 companies worldwide in order to facilitate human rights reporting within the private sector. Canada should work with Shift to incorporate intersectional reporting on gender and LGBTQ+ perspectives in the private sector.

4. **Champion a global certification scheme modelled from the EU's European Data Protection Certification.** It is in the best interest of Canadians to support further cooperation between the private sector, civil society and government in order to better protect their privacy. Endorsing a global certification scheme, facilitated by the UNGP and a civil society organization such as Shift, would incentivize private actors to be active and enthusiastic participants in protecting human rights.

5. **Advocate for an expansion of the jurisdiction of the ICC to include private actors.** Considering the expansive capability of social media platforms to violate privacy, spread hate speech and incite violence, as seen in the recent mass atrocities in Myanmar, the persons responsible for these violations must be held to account. Expanding the purview of the ICC to include corporate actors would provide a mechanism for redress for victims of mass atrocities facilitated by tech companies.

About the Authors

Violette Khammad is a student in the University of Waterloo's Master of Arts in Global Governance based at the BSIA.

Bryn McAuley is a student in the University of Waterloo's Master of Arts in Global Governance based at the BSIA.

Sarah Murray is a student in the joint-Wilfrid Laurier University/University of Waterloo PhD Global Governance program based at the BSIA.

Naomi Pearson is a student in Wilfrid Laurier University's Master of International Public Policy Program based at the BSIA.

Acknowledgements

The authors would like to thank Andrew Thompson for his guidance and mentorship throughout the development of this briefing note. Special thanks to Global Affairs Canada for their knowledgeable feedback and support throughout the course of this project.

Works Cited

De Groot, J. 2019. "What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019." https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

Dholakia N. and M. Wang. 2019. "Interview: China's 'Big Brother' App Unprecedented View into Mass Surveillance of Xinjiang's Muslims." *Human Rights Watch.* https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

Electronic Privacy Information Center. 2019. "Facebook Privacy." https://epic.org/privacy/facebook/.

Human Rights Council. 2018. *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/47.

Meyer, D. 2018. "In the Wake of the GDPR, Will the U.S. Embrace Data Privacy?" *Fortune,* November 29. http://fortune.com/2018/11/29/federal-data-privacy-law/.

Mozur, P. 2018. "A Genocide Incited on Facebook, With Posts From Myanmar's Military." *New York Times*, October 15. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

OHCHR. 2018a. *Call for submissions: thematic report to the UN General Assembly on digital technology, social protection and human rights.* https://www.ohchr.org/EN/Issues/Poverty/Pages/CallforinputGADigitalTechnology.aspx.

OHCHR. 2018b. *Working Draft Legal Instrument on Government-Led Surveillance and Privacy*. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

Office of the Privacy Commissioner of Canada. 2016. *2016 Survey of Canadians on Privacy.* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/.

Pichai, S. 2019. "Google's Sundar Pichai: Privacy Should Not Be a Luxury Good." *The New York Times,* May 7. https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

Sacks, S. 2018. "New China Data Privacy Standard Looks More Far-Reaching than GDPR." January 29. https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr.

Shift. 2019. "Our Story." https://www.shiftproject.org/who-we-are/?fbclid=IwAR03XRtuU7kBh5y2vz8f4sWbRLxhDRGt2dyoKEda4DlDrTVNbgGUub7Mn8g.

Soloman, H. 2018. "Give public more privacy rights, says Canadian commissioner." *IT World Canada,* December 5. https://www.itworldcanada.com/article/give-public-more-privacy-rights-says-canadian-commissioner/412662.

UNGA. 2014. "The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights (A/HRC/27/37)."https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.

Willsher, K. 2019. "Leaders and tech firms pledge to tackle extremist violence online." *The Guardian,* May 15. https://www.theguardian.com/world/2019/may/15/jacinda-ardern-emmanuel-macron-christchurch-call-summit-extremist-violence-online.

Zand, B. 2018. "China's Xinjiang Region: A Surveillance State Unlike Any the World Has Ever Seen." *Spiegel Online,* July 26. https://www.spiegel.de/international/world/china-s-xinjiang-province-a-surveillance-state-unlike-any-the-world-has-ever-seen-a-1220174.html.