Surveillance & Society

The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy

Tamara Shepherd

Volume 22, numéro 2, 2024

Open Issue

URI : https://id.erudit.org/iderudit/1112226ar
DOI : https://doi.org/10.24908/ss.v22i2.16300

Aller au sommaire du numéro

Éditeur(s)

Surveillance Studies Network

ISSN

1477-7487 (numérique)

Découvrir la revue

Citer cet article

Shepherd, T. (2024). The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy. *Surveillance & Society*, *22*(2), 179–191. https://doi.org/10.24908/ss.v22i2.16300

Résumé de l'article

In 2020, the Office of the Privacy Commissioner of Canada (OPCC) led a joint federal-provincial investigation into privacy violations stemming from the use of facial recognition technologies. The investigation was prompted specifically by the mobilization of Clearview AI's facial recognition software in law enforcement, including by regional police services as well as the Royal Canadian Mounted Police. Clearview AI's technology is based on scraping social media images, which, as the investigation found, constitutes a privacy law violation according to provincial and federal private sector legislation. In response to the investigation, Clearview AI claimed that consent for scraping social media images was not required from users because the information is already public. This common fallacy of social media privacy serves as a pivot point for the integration of digital policy literacy into the OPCC's digital literacy materials in order to consider the regulatory environment around digital media, alongside their political-economic and infrastructural components. Digital policy literacy is a model that expands what is typically an individual- or organization-level responsibility for privacy protection by considering the wider socio-technical context in which a company like Clearview can emerge.

Surveillance & Society

Article

The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy

Tamara Shepherd

University of Calgary, Canada
tamara.shepherd@ucalgary.ca

Abstract

In 2020, the Office of the Privacy Commissioner of Canada (OPCC) led a joint federal-provincial investigation into privacy violations stemming from the use of facial recognition technologies. The investigation was prompted specifically by the mobilization of Clearview AI's facial recognition software in law enforcement, including by regional police services as well as the Royal Canadian Mounted Police. Clearview AI's technology is based on scraping social media images, which, as the investigation found, constitutes a privacy law violation according to provincial and federal private sector legislation. In response to the investigation, Clearview AI claimed that consent for scraping social media images was not required from users because the information is already public. This common fallacy of social media privacy serves as a pivot point for the integration of digital policy literacy into the OPCC's digital literacy materials in order to consider the regulatory environment around digital media, alongside their political-economic and infrastructural components. Digital policy literacy is a model that expands what is typically an individual- or organization-level responsibility for privacy protection by considering the wider socio-technical context in which a company like Clearview can emerge.

Introduction

Digital policy literacy (DPL) is a critical framework that promotes broader understanding of how digital technologies are shaped by policy processes, political economic power, and infrastructural affordances (Shade 2012). The DPL approach addresses the aim of critical versions of digital literacy to foreground the cultivation of digital citizenship (e.g., Buckingham 2007; Choi 2016; O'Neill 2010). With respect to surveillance and privacy as key internet policy issues, the DPL framework suggests that commercial surveillance predicated on platform infrastructure requires regulatory frameworks informed by broader rights-based approaches to privacy (Smith, Shade, and Shepherd 2017: 2795). These imperatives become particularly important in the context of facial recognition technologies that contribute to networked surveillance infrastructure that includes social media platforms, algorithmic sorting, and predictive policing (e.g., Kosta 2022; Shore 2022). Moreover, when dealing with the Canadian context as I do here, digital policy issues become further mired in the geopolitical dynamics of how large US tech firms come up against Canadian regulatory frameworks.

This paper argues that Canadian Privacy Commissioners' identification of the societal-level threats posed by facial recognition nonetheless maintain an overall individualist stance on how such threats can be mitigated on a case-by-case basis and with increased user responsibility. I ground this claim in a critique of the recent legal investigation into the use of Clearview AI's (hereafter "Clearview") identification services

Shepherd, Tamara. 2024. The Canadian Clearview AI Investigation as a Call for Digital Policy Literacy. *Surveillance & Society* 22 (2): 179-191.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

in Canada alongside an inventory of the Office of the Privacy Commissioner of Canada's digital literacy resources. An analysis of the incongruities between these materials according to the more critical concerns of the DPL model—policy processes, political-economic power, and infrastructural affordances—highlights how the Clearview case challenges regulatory frameworks as well as digital privacy literacy around facial recognition.

Clearview's facial recognition technology works by scraping images of people's faces from publicly accessible websites, including social media platforms like Facebook, Twitter, and YouTube, organizing them in a database using biometric identifiers, enabling clients to upload an image, and using the identifiers to algorithmically produce a list of matching images and metadata that link back to people's online profiles. In these ways, Clearview's technology poses several threats to privacy; as Tim McSorley (2021) argues, the inaccuracy and bias in Clearview's facial recognition technology threatens civil liberties in a way that is compounded by its unregulated use by law enforcement.

While Clearview's service has been used all over the world, Canada represented the largest market for its services outside the US (Allen, Gillis, and Boutilier 2020). The software's use in Canada is particularly instructive in the context of federal and provincial privacy laws that treat the collection and use of biometric information—like faces—as sensitive and requiring of especially explicit and informed consent. This is pertinent given that Clearview's technology was chiefly targeted toward law enforcement, the Royal Canadian Mounted Police (RCMP) in particular (The Offices 2021: 16). Several individual police officers in municipal forces such as Toronto and Calgary even used the software through trial accounts without formal approval from their departments (Brockbank 2021; Smith 2020).

Of interest in the Clearview case is how a US-based company, scraping user images from US-based social media platforms, could operate for a considerable period in contravention of Canadian laws (as well as those from other non-US jurisdictions) in amassing its database of over three billion images. Through paid subscriptions to its service alongside free trial accounts, Clearview provided the ability for various entities, based both inside and outside of Canada, to gather images and metadata on individuals in Canada without their consent. Clearview's secretive business model involves "a radical erosion of privacy" (Hill 2020), and the investigation of Clearview by Canadian privacy regulators raises pointed questions about online privacy jurisdiction, surveillance capitalism, and notions of informed consent for "public" data. At the same time, however, the solutions proposed to deal with these problems reflect a narrow version of digital literacy that would benefit from the expanded concerns of the DPL model.

In what follows, I first establish how the Clearview case is particularly instructive for foregrounding how, despite the frequent nuance in the Privacy Commissioners' investigation report, resulting policy actions and related literacy initiatives summarized in the following section are not sufficient to address the social threats posed by services like Clearview's. The categories contained within the DPL model—policy processes, political-economic power, and infrastructural affordances—are then used to evaluate the investigation report in the broader context of how the use of facial recognition technologies present an opportunity for more critical engagement with digital literacy on the part of privacy regulators.

Clearview in Canada: Backgrounder

Law enforcement agencies like the RCMP have been using facial recognition technologies long before Clearview's origins in 2016 (Allen, Gillis, and Boutilier 2020). These earlier technologies involved matching facial images to much smaller government databases, such as driver's license photographs (Hill 2020). Clearview's tool instead offers a big data version of this practice, one that does not merely increase the scale of the image search but also involves qualitative changes to how the search functions. As Rob Kitchin (2014: 2) has argued, big data thus involves new epistemologies where "rather than testing a theory by analysing relevant data, new data analytics seek to gain insights 'born from the data.'" These insights are made possible by new analytic techniques based on artificial intelligence; Clearview's tech involves a neural network that mimics the human brain's perceptual processing to convert faces into vectors. Consistent with

other big data business models predicated on proprietary algorithms, the company operated under notable secrecy while it refined its branding and began aggressively marketing its technology toward law enforcement agencies in 2017 (Hill 2020). In doing so, the company leveraged its founders' connections to the US Republican party, far-right groups, and notorious tech investor Peter Thiel (Hill 2020; McSorley 2021).

Based on information obtained by Buzzfeed News in early 2020, The *Toronto Star*'s front-page report on Clearview outlined how its operations in Canada included at least thirty-four distinct police forces alongside business and government agencies like the Insurance Bureau of Canada (Allen, Gillis, and Boutilier 2020). The reporters conclude that the "often apparently unsanctioned use of Clearview AI shows how far the adoption of powerful artificial intelligence technology like facial recognition has outpaced regulation and oversight" (Allen, Gillis, and Boutilier 2020: A1). In response, The Privacy Commissioner of Canada, along with provincial privacy commissioners in Quebec, Alberta, and British Columbia, launched a joint investigation into Clearview's potential violation of federal and provincial privacy laws in February 2020, releasing their findings a year later. In the meantime, Clearview voluntarily withdrew from the Canadian market in July 2020 amid controversy generated by the investigation, as well as widespread critiques of discriminatory police violence that motivated Black Lives Matter protests that summer.

While the Commissioners were restricted to evaluating Clearview's compliance with Canadian privacy legislation, it is worth highlighting that the report explicitly notes the problem of automated racial bias in systems purporting to be neutral, which has been much studied with respect to big data, algorithms, and facial recognition (e.g., Bacchini and Lorusso 2019; Benjamin 2019; Gangadharan 2014; Introna and Murakami Wood 2004; Noble 2018). As the investigation report states, "there are significant concerns regarding the efficacy and accuracy of facial recognition technologies, in particular with respect to certain demographics" (The Offices 2021: 29). The discriminatory racial profiling that already marks policing is exacerbated by facial recognition software, where Fabio Bacchini and Ludovica Lorusso (2019: 323–326) have found that: (a) black faces are overrepresented in image databases, particularly those incorporating mugshots (e.g., Stevens and Keyes 2021: 842); (b) darker skin tones more easily confound recognition algorithms and lead to false positives; (c) there is low accuracy of matches for black and female faces (e.g., Buolamwini and Gebru 2018); (d) companies and law enforcement have not independently tested the racial bias of most software, including Clearview's; and (e) there tends to be no systematic oversight or human review to verify the validity of match results. Moreover, in general terms, the historically disproportionate surveillance of black and other marginalized populations has been central to maintaining a "racialized disciplinary society" (Browne 2015: 9), which is further perpetuated by the constellation of factors that render facial recognition technology particularly prone to discrimination based on essentialized notions of race.

More generally, facial recognition systems have also been critiqued for their lack of accuracy in producing matches, contrary to big data's claims to optimal accuracy and the automated generation of "insight" (Kitchin 2014: 5). The investigation report also notes this with regard to Clearview's misrepresentation of the results of accuracy testing that it had commissioned on its software (The Offices 2021: 31). Of course, the accuracy of facial recognition systems has long been paramount to their evaluation, where accuracy rates touted by tech firms tend to represent ideal rather than actual circumstances and are compromised by the increasing size of image databases (Introna and Murakami Wood 2004: 189). These problems support Shoshana Magnet's (2011: 29) argument that failure is endemic to biometric identification technologies of all kinds, given that the body is not a stable property free from cultural representation. Therefore, biometric identification technologies such as facial recognition software can enact significant harms in their inherent misidentifications, which in Clearview's case, are compounded by the technology's adoption by law enforcement agencies in a wider climate of discriminatory and racist policing in Canada (Maynard 2017).

Accordingly, the Privacy Commissioners' main finding was that Clearview's technology does pose significant potential harms while it also contravenes both Canadian privacy laws in its non-consensual scraping of social media images for inappropriate and illegitimate purposes and Quebec laws around the

security of biometric databases. As the report summary states, Clearview's business in Canada "represents the mass identification and surveillance of individuals by a private entity in the course of commercial activity" (The Offices 2021: 6). Clearview's activities are consistent with the development of a "surveillance society," built upon the multitude of digital traces of identity generated passively as a by-product of everyday life (Lyon 1994). This specific version of digital surveillance is further conditioned by a distinctly American tech industry culture of "move fast and break things" as a means to commercialize passive surveillance (Taplin 2017), which is evident in the way that jurisdictional issues mired the Commissioners' investigation of Clearview in Canada.

Policy and Literacy Initatives in the Wake of the Investigation

The OPCC's responses to the Clearview investigation have so far manifested in some degree of policy activity directed toward Parliamentarians and law enforcement. As yet, Clearview itself has faced no direct penalties from the OPCC, unlike in the UK, where the Information Commissioner's Office fined the company over £7.5 million (ICO 2022). In 2021, the Canadian commissioners did order Clearview to comply with the recommendations of the joint investigation, but by that time, Clearview had already exited the Canadian market, and regional police departments as well as the RCMP had ceased using the service. Moreover, as the report asserts, the investigation itself worked to deter Clearview and other similar services from violating Canadian privacy laws by "ensur[ing] that other organizations have the benefit of our conclusions as they contemplate initiatives that may share certain similarities with Clearview's practices" (The Offices 2021: 36).

It is unclear, however, whether Clearview has in fact complied with the report's recommendation to delete photos of individuals in Canada that are contained in its database, or if that might yet trigger further action by the Commissioners. The final words of the investigation report do threaten that, should Clearview fail to comply with all recommendations, "we will pursue other actions available to us under our respective Acts to bring Clearview into compliance with federal and provincial privacy laws applicable to the private sector" (The Offices 2021: 36). These further actions could include issuing a financial penalty as in the UK, engaging in legal action through the Attorney General's office, or using its public platform to further Clearview's reputation loss with clients such as police agencies. With regard to law enforcement's uses of facial recognition in particular, in 2022, the OPCC published specific guidelines and a revised legal framework for police agencies' use of facial recognition (discussed in greater detail below), which include express authorization before such uses occur.

The Clearview investigation further set a precedent for the overhaul of federal privacy laws proposed in the Bill C-27, The Digital Charter Implementation Act, tabled in June 2022 (based on an earlier version tabled in November 2020), and still under debate in the House of Commons at the time of writing. The OPCC's presentations to Parliamentarians have argued that the Clearview case should inform Bill C-27's provisions for specific authorized uses of facial recognition technology, risk-benefit analyses in the form of Privacy Impact Assessments, strong independent oversight, and rights-based approaches to privacy that explicitly delineate conditions of accuracy, retention, and transparency in facial recognition data (Therrien 2021). While the Bill proposes new legislation that would implicate facial recognition systems in the Consumer Privacy Protection Act and the Artificial Intelligence and Data Act, as well as in amendments to existing private-sector privacy legislation, there is yet to be any specific wording in the Bill about facial recognition or biometric data in any form.

The OPCC's advice to Parliament in the discussion around Bill C-27 has repeatedly emphasized a rights-based approach to privacy, reflecting the Office's "mission to protect and promote the privacy rights of individuals" (noted across several of its publications and webpages). The promotion aspect manifests particularly in the OPCC's vast digital privacy literacy resources and public awareness campaigns. Nonetheless, and part of the reason I argue below for the importance of the more critical DPL model, the self-proclaimed "rights-based approach" in these materials is limited by the framing of privacy in individual terms. For example, the OPCC's "A Guide for Individuals: Protecting Yor Privacy" (2015) is the most

comprehensive downloadable brochure on federal privacy legislation designed to help individuals understand their privacy rights. In the brochure, such rights in the context of commercial data collection are anchored in the assumption that, "By understanding the value of personal privacy, you can do a lot to defend it. For example, you can be careful about sharing personal information or letting it circulate freely" (OPCC 2015: 14). While the guide articulates this dynamic in relation to rights enshrined with the federal privacy law as well as Charter rights, ultimately the solutions posed for privacy breaches are individualized according to the complaints resolution framework that puts the onus on individual users to: (1) be aware of privacy rights infringements; and (2) take action with the correct institutional bodies, such as the OPCC, to initiate the process of defending those rights. Such shortcomings of privacy literacy in contexts where data collection is invisible has long been noted by scholars of data privacy (e.g., Agre and Rotenberg 1997; Allen 1999).

The OPCC has produced several other resources that have the potential to offer more critical approaches to the question of privacy rights in facial recognition systems, but that likewise share the same limited, individualized solutions. For example, a tipsheet on protecting your digital privacy begins with, "Whether it's online or in person, you are constantly being asked for your personal data. Don't just blindly give it up" (OPCC 2018). A resource on businesses' obligations to protect personal information advises that, "if you have concerns about how a business has handled your personal information, your first step should generally be to raise the concern directly with the organization" (OPCC 2016). The only literacy guide that seems to address the issue of covert data collection is "Biometrics and the Challenges to Privacy," which proposes Privacy Impact Assessments as a self-regulatory mechanism for organizations to evaluate their practices against the requirements of Canadian privacy law (OPCC 2011). And yet, this guide to biometric privacy has last been updated over a decade ago and chiefly describes government, rather than commercial, biometric data collection (although it is currently undergoing an update).

This brief summary is not intended to dismiss the OPCC's production of literacy resources that are certainly helpful and necessary. But, as the Clearview case highlights, according to the principles of the DPL model elaborated below, many of the threats to privacy posed by facial recognition technologies outstrip an individualized version of protecting one's rights. Moreover, these literacy resources may be accessed inconsistently or not at all by the people most impacted by facial recognition systems, leading to a more general lack of collective and critical thinking about surveillance technologies and a context where companies like Clearview can thrive.

Digital Policy Literacy's Intervention

The apparent flaws in facial recognition technology, the problems with Clearview specifically, and the limitations of the Commissioners' investigation and digital literacy materials demonstrate the need for digital policy literacy (DPL) to bolster critical perspectives on the surveillance society. As part of critical digital literacy, DPL situates legislative and regulatory frameworks relative to the ways that digital technology is shaped by the political economy of media systems and networked communication infrastructures (Shade 2012). The DPL model has been applied to digital privacy (Shade and Chan 2021; Shade and Shepherd 2023), networked surveillance (Smith, Shade, and Shepherd 2017), and digital activism (Shade 2015). Integrating the idea of policy literacy pedagogy—one that moves away from the protectionist impulse of more traditional media literacy and toward an interventionist stance on participating in media policy struggles (Lentz 2014)—DPL provides pointed suggestions for expanding notions of digital literacy in view of contemporary challenges like those posed by facial recognition technology. The Clearview case is used here to highlight how policy processes, the political economy of platforms, and the affordances of networked infrastructure could be addressed more fulsomely in literacy frameworks.

Policy Processes

The DPL model foregrounds how policy is not static but is a battleground fought over by competing interests, including and especially public interests. In this way, it reflects critical approaches to media and

information literacy that situate digital privacy among interrelated spheres of state governance, market power, and technological affordances in order to bring nuance to digital literacy frameworks focused simply on how to use technology (Shade and Chan 2020: 335).When considering private sector privacy laws that apply to the Clearview case, for example, the Privacy Commissioners' investigation centered on the federal Personal Information Protection and Electronic Documents Act (PIPEDA), alongside Alberta's Personal Information Protection Act (PIPA AB), British Columbia's Personal Information Protection Act (PIPA BC), and Quebec's Act Respecting the Protection of Personal Information in the Private Sector. These laws reflect an approach to networked privacy—as a subset of commercial uses of data—informed by the constitutional rights to privacy articulated in the Charter of Rights and Freedoms (Scassa 2020: 57). They have been devised and interpreted through federal and provincial Privacy Commissioners, who conduct extensive public consultation, fund robust programs of research, and investigate violations of the laws according to a complaint resolution ombuds framework. The laws are based on several guiding "fair information" principles common to international privacy frameworks, including consent, limiting collection, accuracy, and individual access (e.g., OPCC 2019). While these principles afford flexible adaptation of the laws to changing technological contexts, the lack of a coordinated reform of the legislation devised in the context of emerging e-commerce in the early 2000s means that increasingly, the weak enforcement provisions of PIPEDA and similar laws have been insufficient to deal with new issues in digital privacy (Scassa 2020: 72). In the meantime, internet companies that do business globally have begun to comply with stronger privacy laws, such as the global standard set by the EU's 2018 General Data Protection Regulation (GDPR) (Rustad and Koenig 2019).

Aligning with these pieces of legislation, the investigation report identifies informed consent as its primary concern. Contextually appropriate consent is legally required from the individual for the collection, use, and disclosure of their personal information according to all the Canadian laws. The investigation found that Clearview's technology collected sensitive personal information (faces as biometric markers), which if disclosed risk resulting in harm, and which exceed the reasonable expectations of the individual (The Offices 2021: 19). Consent is evidently central to Clearview's violations of Canadian privacy law, and yet consent represents an individualist notion of privacy that favours data-based businesses and erodes collective privacy rights (Weinberg 2017). Companies can claim to have obtained consent based on a one-time "click to agree," which behavioural studies have shown to be inadequate to generate informed, considered, or ongoing consent (Borgesius 2015; Pasquale 2013). In Clearview's case, however, not even this superficial level of consent was sought or obtained.

Further, the precedent for the investigation's finding that Clearview did not obtain adequate consent was set in the 2020 joint investigation of Cadillac Fairview (by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia) for the use of facial monitoring software in their shopping centres. In that case, the mall directory screens covertly recorded images of shoppers' faces and used facial recognition software to render those faces into biometric identifiers in order to determine their age and gender for marketing purposes (OPCC 2020). Similarly, Clearview represents a commercial application of facial recognition technology that neglected to seek any sort of consent from the individuals whose images populate its database. A significant difference between the two cases—and the basis upon which Clearview argued it did not need to obtain consent—is that the images were scraped from social media sites where users voluntarily uploaded their photos. The ability for Clearview to scrape images from external sites like Facebook offers an instructive example of how it is usually the private policies of social media platforms like Facebook that can adapt more quickly to technological changes; the Terms of Service of Facebook and other platforms forbid data scraping, for instance, meaning that Clearview violated these private terms as well as the technological measures that platforms have put in place to thwart scraping through regulation by code (Rezende 2020: 380).

Given the ways that Clearview evaded consent—both from users and external platforms—the DPL model suggests that an integration of privacy policy making into digital literacy frameworks should include understandings of consent: what it is, how it might be violated, and its limitations. Consent is an active

process and technologically neutral principle, but at the same time, it puts the onus on individual users to protect their privacy in a context of legal and technical jargon (Terms of Service) as well as technological obfuscation (scraping). Therefore, more robust privacy legislation like the GDPR is informing the revisions to Canadian law proposed in Bill C-27 (Therrien 2022)—this is also an area where regulatory reform could include intentionally designed public consultation supported by literacy resources that plainly lay out the ways that stronger privacy laws would prevent covert social media scraping without the need for individuals to request information about and protection of their biometric data post hoc.

Political-Economic Power

The DPL model considers political economy from a critical perspective on how digital technologies are suffused with power relations through the process of commodification (e.g., Mosco 2009). The commercial context of surveillance capitalism forms the obvious political-economic backdrop for evaluating the profit motive behind Clearview's use of facial recognition. As the investigation report finds, even though most of the entities using Clearview in Canada had not paid for the service and were using trial accounts (other than the RCMP), "The colour and character of Clearview's activities were commercial in nature, with trials existing for the express purpose of enticing the purchase of accounts" (The Offices 2021: 16). The argument for facial recognition as a reasonable tool for identifying suspects is compromised by Clearview's express commercial purpose (The Offices 2021: 29), as well as its massive scope and scale that draw from the more familiar versions of social media surveillance on popular platforms.

Shoshana Zuboff's (2015; 2019a) term "surveillance capitalism" describes contemporary networked platforms' rationality, and, along with related ideas like "data capitalism" (West 2019), "data capital" (Sadowski 2019), and "platform capitalism" (Srnicek 2017), it has been influential in centering big data analytics within capital accumulation (Lyon 2019: 66). Although subject to significant critique (e.g., Morozov 2019; Mueller 2022), Zuboff's (2019a) analysis illustrates how the rapid pace at which platforms have developed increasingly exploitative algorithmic prediction based on mass dataveillance has outpaced public understanding and thus regulation and law (see also Zuboff 2015: 83). While privacy law is certainly relevant to surveillance capitalism, and by extension, the activities of a firm like Clearview, there are also more encompassing values of modern liberalism and social justice at stake (Cinnamon 2017), which include: "the sanctity of the individual and the ideals of social equality; the development of identity, autonomy, and moral reasoning; the integrity of contract, the freedom that accrues to the making and fulfilling of promises; norms and rules of collective agreement; the functions of market democracy; the political integrity of societies; and the future of democratic sovereignty" (Zuboff 2019b). The Privacy Commissioners' investigation of Clearview hints at some of these implications, even though they are technically out of scope, such as in the discussion of accuracy when it is noted that harms could involve "individuals being excluded from opportunities" (The Offices 2021: 30). This vague reference to social exclusion is indicative of the broader refashioning of subjectivity that is enacted through surveillance capitalism.

The social justice implications of surveillance capitalism are, moreover, deeply geopolitical. With its origins at Google in the wake of the 2001 dot-com crash (Zuboff 2019a: 20), surveillance capitalism reflects the Californian ideology of Silicon Valley's economic and social liberalism (Barbrook and Cameron 1996), combined with the surveillance exceptionalism engendered by 9/11 (Zuboff 2019a: 118). This exceptionalism is married with the "surveillance-innovation complex" that positions privacy as anathema to innovation, contributing further to a US regulatory environment that has been particularly lax around privacy protection (Cohen 2016: 218), which has further provided the conditions for a host of surveillance-based privacy scandals that implicate both industry and the state (Kunelius and Russell 2019). The jurisdictional frictions between the US and Canada are evident in Clearview's (false) claim that "none of [the Privacy Commissioners'] Offices have jurisdiction over its activities," on the basis "that '[n]one of Clearview's activities take place in Canada,'" and "that PIPEDA does not apply 'because there is no real and substantial connection to Canada'" (The Offices 2021: 15). Clearview's argument here, while incorrect, reveals how surveillance capitalism is inherently territorial despite relying on supposedly

borderless networked platforms. In turn, the territorial nature of data flows and storage undermines the ability of users to seek justice in this system (Cinnamon 2017: 617; Clement and Obar 2015: 27).

One recourse that should be emphasized in a DPL model that foregrounds surveillance capitalism alongside an understanding of policy processes is to explore the potential applicability of foreign laws to US firms. Clearview offers an instructive case to demonstrate how, as the report outlines, "PIPEDA applies to organizations outside of Canada where a 'real and substantial connection' to Canada exists" (The Offices 2021: 16). The connections to Canada in this case included Clearview's: (a) active marketing of its services to Canadian organizations; (b) public framing of Canada as part of its core market; (c) database of over three billion images, which presumably includes millions of Canadians' faces; and (d) web data that were transmitted through Canadian servers (The Offices 2021: 16–17). The fact that a US company can be subject to Canadian laws, as in this instance, offers a route toward checking not only the immense commercial but also geopolitical power of US tech firms. The influence of the GDPR further suggests that the laxity of US commercial privacy laws could be countered by extraterritorial frameworks predicated on alternatives to the increasing commodification of personal data under surveillance capitalism.

Infrastructural Affordances

Surveillance capitalism both shapes and takes form from the affordances of digital platforms and networked communication infrastructures. The infrastructural level is important for the DPL model in the Clearview case, given the impact of technology design on the firm's justification of its non-consensual scraping practices. It has already been noted that Clearview transgressed anti-scraping Terms of Service and site code on the part of platforms like Facebook; however, the fact that scraping images and other data is possible at all should be interrogated as a design feature. As Greg Elmer (2015: 122) has argued, scraping occurs according to the "first-person perspective" typical of social media platforms that construct identity as an exploitable commodity. Accordingly, scraping is not a neutral means of collection; it reproduces a version of identity that aligns with the platform's incentive to produce users as data objects. In this way, scraping enacts a kind of violence that implicates privacy concerns beyond the consent of the target individual, given that social media photos include contextual elements like surroundings and other people, as well as metadata that can facilitate tracking (Rezende 2020: 379). As the investigation report notes, Clearview engaged in "the mass and indiscriminate scraping of images from millions of individuals across Canada, including children, amongst over 3 billion images scraped world-wide" (The Offices 2021: 26). Clearview could thus not rest on the common justification that social media data are "already public" or could be anonymized (e.g., Zimmer 2010), given their scraping of photos from private profiles and minors, and their use specifically for identification. In this way, the violence of the scraping practices that are afforded—even though they may not be condoned—by social media platforms conditions the way that Clearview approached the report's findings.

While scraping was key to Clearview's operations, the value of its services lies chiefly in the way that the image database furnishes identification by rendering faces into biometric markers. The identification process rests on the infrastructures of artificial intelligence, and specifically neural networks that seek to mimic brain processing by finding relationships between facial features that get quantified as vectors (Rezende 2020: 372). Magnet (2011: 21) details the steps involved in such biometric renderings of facial information, noting that the proprietary algorithmic creation of a biometric template for identification and matching is at the core of biometrics as an industry. Despite Clearview's repeated assertion of its matching algorithm's accuracy (see, e.g., Marks 2021), biometrics in general are prone to failure due to what Magnet (2011: 2) terms the "biometric fallacy" of reducing bodies to code based on false assumptions about the body's integrity and stability (see also Agre 2001; Black 2023). As Magnet (2011: 12) states, "The knowledge generated by the use of biometrics to test identity is asked to perform the cultural work of stabilizing identity—conspiring in the myth that bodies are merely containers for unique identifying information which may be seamlessly extracted and then placed into a digital database for safekeeping." Such a myth relies on the mystification of infrastructures such as neural nets that perform the "magic" of rendering bodies into information, into forms of capital. Demystifying this process should be a part of DPL-

inspired frameworks, particularly when it comes to sensitive personal attributes such as faces. In its revised guide to biometric privacy, for instance, the OPCC could include some discussion of the indexical gaps in rendering bodies into data points and the failures endemic to the process.

Among biometric identifiers like irises and fingerprints, faces hold a special place in social life, in that "we reveal our faces to each other as part of a social order where recognition is mutual, as part of social relationships over which we exercise relative control" (Introna and Murakami Wood 2004: 178). Faces also act as a medium of emotion given their "dynamism and mutability" (Black 2021: 11), informing the politics of faces as representational of human subjectivity. Particularly when faces become data, their politics draw on longstanding essentialism that has informed social injustice and legitimized colonial oppression (Browne 2015; Stevens and Keyes 2021: 847). Facial recognition systems further crystallize the conflation of body with identity specifically according to categorizations of identity based on difference, especially racial difference (Bacchini and Lorusso 2019: 327). As the investigation report takes pains to note, even though it is out of scope of Canadian privacy law, facial recognition systems tend to be associated with discriminatory outcomes for people of colour (The Offices 2021: 30). In this way, the affordances of biometric identification technologies such as facial recognition are built upon long histories of othering through supposedly scientific categorization. The OPCC's biometric guide could make a note that this type of data collection is not only potentially threatening to universally framed privacy rights but also should be examined on the basis of how it further entrenches existing racial discrimination and control.

The deeper infrastructural systems of human categorization that underlie Clearview's technology are especially concerning given the firm's explicit marketing of its services toward law enforcement. Kashmir Hill's (2020) famous exposé on the company for *The New York Times* quotes Clearview's founders, who initially entertained various applications for their facial recognition tool: "Maybe it could be used to vet babysitters or as an add-on feature for surveillance cameras. What about a tool for security guards in the lobbies of buildings or to help hotels greet guests by name? 'We thought of every idea'" (qtd. in Hill 2020). But not until the company began targeting law enforcement through free trials and low-cost accounts—via one founder's connections to the US Republican party—did it secure investor funding (Hill 2020). These origins of the company demonstrate how the development of facial recognition technologies more broadly can never be neutral as they are at the outset infused with the power dynamics of highly stratified social relations (e.g., Andrejevic and Selwyn 2022: 135).

The solidification of Clearview's business model to indiscriminately collect facial images, render them into biometric markers to facilitate matching, and sell that matching service to police forces via government representatives illustrates the broader infrastructural matrices behind the investigation report's finding that facial recognition was used inappropriately and illegitimately by Clearview in Canada (The Offices 2021: 25). As Isadora Neroni Rezende (2020: 376) argues further,

> the Clearview case differs from other scenarios involving the disclosure of personal data from the private sector to law enforcement: personal data are not transferred to police forces on a case-by-case basis, against payment or pursuant to a legal obligation, but they are collected by a private company with the precise intent of making them available, through an institutional arrangement, to government agencies for policing purposes.

Rezende (2020: 389) evaluates Clearview against European laws around data protection and the transfer of data from private companies to law enforcement agencies, noting that its uses by law enforcement are, in fact, unlawful. Clearview's operations as a particularly secretive private company means that its data collection and matching algorithm are not subject to the appropriate oversight required by European police (Eneman et al. 2022: 227).

In Canada, the particular issues posed by police uses of facial recognition technology more generally—inspired by the Clearview case—was the subject of the OPCC's subsequent public consultation and policy recommendations addressed to Parliamentarians in 2021–2022. In May 2022, for instance, the OPCC

published its "Privacy Guidance on Facial Recognition for Police Agencies," which echoes the Clearview investigation in its contention that, while the many risks of facial recognition technology outstrip its benefits, there is room for law enforcement "to appropriately manage risks through careful planning and diligent application of privacy protections," to be audited through Privacy Impact Assessments (OPCC 2022: paras. 34, 68–74). While Privacy Impact Assessments are a recognized tool for encouraging systems that give individuals greater control over their data, they tend to lack a broader analysis of how surveillance capitalism entrenches societal-level inequalities and potentially violates human rights (Marx 2012: vi). Further, Privacy Impact Assessments maintain the fallacy that facial recognition technologies are inherently neutral, produce accurate matches, and could be used equally for good or bad purposes. An infrastructural view on technologies as embedded within larger power dynamics suggests instead that the failures endemic to biometric surveillance are, as Magnet (2011: 150) argues, borne of a desire to deepen the links between the state, law enforcement, and industry by strengthening the security apparatus.

Conclusion

The Clearview case's intersecting policy, political-economic, and infrastructural dimensions make the DPL model especially relevant for not only encouraging learning about technology and rights but also situating the idea of rights beyond the individual and within broader social justice ideals. Writing nearly twenty years ago about CCTV camera surveillance, Lucas Introna and David Murakami Wood (2004: 195) opined that future critiques of facial recognition technologies will need to transcend privacy to understand surveillance technologies in the context of their socio-technical relationships to broader democratic values. Magnet (2011: 14) similarly contends that, "at stake in the application of biometric technologies to state programs are constrained possibilities for substantive equality, democracy and socially just forms of subjectivity." While some of these values are addressed in the investigation report, the limitations of the individual privacy rights framework prevent a more holistic assessment of facial recognition in general. The failures of biometric systems—which Magnet (2011: 6) argues are "endemic to their technological functioning"—must be subject to rigorous oversight and scrutiny from a critical perspective that should infuse the work of privacy regulators, lawmakers, and the larger social context. This work is especially important given the geopolitical dynamic of US firms actively exporting their particular form of surveillance capitalism globally.

The DPL model thus involves an orientation toward contemporary digital technologies that is not only about privacy or equality but also justice. This critical perspective offers expanded ways of thinking about digital literacy that go beyond simply protecting oneself. As Becky Lentz (2014: 139) articulates about such a critical pedagogy, it "depends on the capacity of people to consider themselves as more than merely digital consumers," and involves "an obligation to team up with open source, media democracy, media justice, and freedom of expression communities of practice to render classrooms as collaboratories of theory and practice." This notion also suggests room for the OPCC to extend outward into communities and advocacy organizations dealing with the social justice issues implicated by discriminatory surveillance capitalism to develop more critical literacy materials and approaches to data privacy regulation that offer collective visions for privacy. This is particularly important given how facial recognition systems reinforce the racist objectives of dehumanization (Stevens and Keyes 2021: 848). What should be conveyed more broadly, according to the DPL model, are the ways that people might intervene in policy processes, might question political-economic configurations of power, and might subvert the technical and social infrastructures that constrain them. Despite the enormity of this task, there is still room for critical literacy initiatives to uncover "conditions of possibility—of worlds, subjects, and rights" (Ruppert, Isin, and Bigo 2017: 6), which could spark struggles for justice against contemporary technological rationality.

References

Agre, Philip E. 2001. Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places. *Whole Earth* 106: 74–77.

Agre, Philip E., and Marc Rotenberg, eds. 1997. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press.

Allen, Anita L. 1999. Coercing Privacy. *William and Mary Law Review* 40 (3): 723–757.

Allen, Kate, Wendy Gillis, and Alex Boutilier. 2020. Mounties, Rexall, Small-town Cops: They've All Used Controversial Face-match App. *Toronto Star*, February 28. https://www.thestar.com/news/canada/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously/article_2de39e45-4bf1-5b56-9f07-ad117454569e.html [accessed August 21, 2022].

Andrejevic, Mark, and Neil Selwyn. 2022. *Facial Recognition*. Cambridge, UK: Polity.

Bacchini, Fabio, and Ludovica Lorusso. 2019. Race, Again: How Face Recognition Technology Reinforces Racial Discrimination. *Journal of Information, Communication and Ethics in Society* 17 (3): 321–335.

Barbrook, Richard, and Andy Cameron. 1996. The Californian Ideology. *Science as Culture* 6 (1): 44–72.

Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity.

Black, Daniel. 2023. Facial Analysis: Automated Surveillance and the Attempt to Quantify Emotion. *Information, Communication & Society* 26 (7): 1438–1451.

Borgesius, Frederik Zuiderveen. 2015. Informed Consent: We Can Do better to Defend Privacy. *IEEE Security & Privacy* 13 (2): 103–107.

Brockbank, Nicole. 2021. Toronto Police Used Clearview AI Facial Recognition Software in 84 Investigations. *CBC News*, December 23. https://www.cbc.ca/news/canada/toronto/toronto-police-report-clearview-ai-1.6295295 [accessed January 31, 2023]

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Buckingham, David. 2007. Digital Media Literacies: Rethinking Media eEducation in the Age of the Internet. *Research in Comparative and International Education* 2 (1): 43–55.

Buolamwini, Joy, and Timnit Gebru. 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In *Proceedings of the Conference on Fairness, Accountability and Transparency, New York, February 23–24*, 77–91. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [accessed February 2, 2023].

Choi, Moonsun. 2016. A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Theory & Research in Social Education* 44 (4): 565–607.

Cinnamon, Jonathan. 2017. Social Injustice in Surveillance Capitalism. *Surveillance & Society* 15 (5): 609–625.

Clement, Andrew, and Jonathan A. Obar. 2015. Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 13–44. Ottawa, CA: University of Ottawa Press.

Cohen, Julie. 2016. The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 207–226. Minneapolis, MN: University of Minnesota Press.

Elmer, Greg. 2015. Scraping the First Person. In *Compromised Data: From Social Media to Big Data*, edited by Greg Elmer, Ganaele Langlois, and Joanna Redden, 112–125. New York: Bloomsbury Academic.

Eneman, Marie, Jan Ljungberg, Elena Raviola, and Bertil Rolandsson. 2022. The Sensitive Nature of Facial Recognition: Tensions Between the Swedish Police and Regulatory Authorities. *Information Polity* 27: 219–232.

Gangadharan, Seeta Peña. 2014. Data-based Discrimination. In *Data and Discrimination: Collected Essays*, edited by Seeta Peña Gangadharan, with Virginia Eubanks, and Solon Barocas, 1–5. Washington, DC: New America Foundation.

Hill, Kashmir. 2020. The Secretive Company that Might End Privacy as We Know It. *New York Times*, January 18. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [accessed July 12, 2022].

ICO [Information Commissioner's Office (UK)]. 2022. ICO Fines Facial Recognition Database Company Clearview AI Inc more than £7.5m and Orders UK Data to be Deleted. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ [accessed July 11, 2023]

Introna, Lucas, and David Murakami Wood. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2 (2/3): 177–198.

Kitchin, Rob. 2014. Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society* 1 (1): 1–12.

Kosta, Eleni. 2022. Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights. *Regulation & Governance* 16 (1): 212–224.

Kunelius, Risto, and Adrienne Russell. 2019. Surveillance Scandals and the Systemic Crisis of the Public. In *The Routledge Companion to Media and Scandal*, edited by Howard Tumber and Silvio Waisbord, 295–303. London: Routledge.

Lentz, Becky. 2014. The Media Policy Tower of Babble: A Case for "Policy Literacy Pedagogy." *Critical Studies in Media Communication* 31 (2): 134–140

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis, MN: University of Minnesota Press.

———. 2019. Surveillance Capitalism, Surveillance Culture and Data Politics. In *Data Politics: Worlds, Subjects, Rights,* edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 64–77. London: Routledge.

Magnet, Shoshana. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.

Marks, Paul. 2021. Can the Biases in Facial Recognition be Fixed; Also, Should They? *Communications of the ACM* 64 (3): 20–22.

Marx, Gary T. 2012. Foreword: Privacy is Not Quite Like the Weather. In *Privacy Impact Assessment*, edited by David Wright and Paul de Hert, v–xiv. Dordrecht, NL: Springer.

Maynard, Robyn. 2017. *Policing Black Lives: State Violence in Canada from Slavery to the Present*. Winnipeg, CA: Fernwood Publishing.

McSorley, Tim. 2021. The Case for a Ban on Facial Recognition Surveillance in Canada. *Surveillance & Society* 19 (2): 250–254.

Morozov, Evgeny. 2019. Capitalism's New Clothes. *The Baffler*, February 4. https://thebaffler.com/latest/capitalisms-new-clothes-morozov [accessed August 24, 2022].

Mosco, Vincent. 2009. *The Political Economy of Communication.* 2nd edition. London: Sage.
Mueller, Milton. 2022. A Critique of the "Surveillance Capitalism" Thesis: Toward a Digital Political Economy. SSRN, August 2. http://dx.doi.org/10.2139/ssrn.4178467 [accessed August 24, 2022]
Noble, Safia U. 2018. *Algorithms of Oppression*. New York: New York University Press.
O'Neill, Brian. 2010. Media Literacy and Communication Rights: Ethical Individualism in The New Media Environment. *International Communication Gazette* 72 (4–5): 323–338.
Offices, The. 2021. Investigation Report P2021-IR-01: Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta. February 3. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ [accessed July 13, 2022].
OPCC [Office of the Privacy Commissioner of Canada]. 2011. Data at Your Fingertips: Biometrics and the Challenges to Privacy. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/ [accessed July 10, 2023].
———. 2015. A Guide for Individuals: Protecting Your Privacy. https://www.priv.gc.ca/media/2036/guide_ind_e.pdf [accessed July 10, 2023].
———. 2016. Businesses and Your Personal Information. https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/businesses-and-your-personal-information/ [accessed July 10, 2023].
———. 2018. 10 Tips for Protecting Personal Information. https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/02_05_d_64_tips/ [accessed July 10, 2023].
———. 2019. PIPEDA Fair Information Principles. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/ [accessed January 31, 2023].
———. 2020. Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. October 28. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/ [accessed July 13, 2022].
———. 2022. Privacy Guidance on Facial Recognition for Police Agencies. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/ [accessed July 10, 2023].
Pasquale, Frank A. 2013. Privacy, Antitrust, and Power. *George Mason Law Review* 20 (4): 1009–1024.
Rezende, Isadora Neroni. 2020. Facial Recognition in Police Hands: Assessing the "Clearview Case" from a European Perspective. *New Journal of European Criminal Law* 11 (3): 375–389.
Ruppert, Evelyn, Engin Isin, and Didier Bigo. 2017. Data Politics. *Big Data & Society* 4 (2): https://doi.org/10.1177/2053951717717749.
Rustad, Michael L., and Thomas. H. Koenig. 2019. Towards a Global Data Privacy Standard. *Florida Law Review* 71 (2): 365–454.
Sadowski, Jathan. 2019. When Data Is Capital: Datafication, Accumulation, and Extraction. *Big Data & Society* 6 (1): 1–12.
Scassa, Teresa. 2020. Data Protection and the Internet: Canada. In *Data Protection in the Internet*, edited by Dário Moura Vicente and Sofia de Vasconcelos Casimiro, 55–76. Cham, CH: Springer.
Shade, Leslie Regan. 2012. Toward a Model of Digital Policy Literacy. In *iConference '12: Proceedings of the 2012 iConference, Toronto, Canada, February 7–10*, 459–461. https://dl.acm.org/doi/10.1145/2132176.2132247 [accessed January 25, 2023].
———. 2015. I Want My Internet! Young Women on the Politics of Usage-based Billing. In *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices*, edited by Jane Bailey and Valerie Steeves, 411–434. Ottawa, CA: University of Ottawa Press.
Shade, Leslie Regan, and Sharly Chan. 2020. Digital Privacy Policy Literacy: A Framework for Canadian Youth. In *The Handbook of Media Education Research*, edited by Divina Frau-Meigs, Sirkku Kotilainen, Manisha Pathak-Shelat, Michael Hoechsmann, and Stuart R. Poyntz, 327–338. Hoboken, NJ: John Wiley & Sons.
Shade, Leslie Regan, and Tamara Shepherd. 2013. Viewing Youth and Mobile Privacy through a Digital Policy Literacy Framework. *First Monday* 18 (12): https://firstmonday.org/ojs/index.php/fm/article/view/4807.
Shore, Alexis. 2022. Talking About Facial Recognition Technology: How Framing and Context Influence Privacy Concerns and Support for Prohibitive Policy. *Telematics and Informatics* 70: https://doi.org/10.1016/j.tele.2022.101815.
Smith, Alanna. 2020. Two Calgary Officers Tested Clearview AI Facial-recognition Software. *Calgary Herald*, February 28. https://calgaryherald.com/news/local-news/two-calgary-officers-tested-clearview-ai-facial-recognition-software [accessed January 31, 2023]
Smith, Karen Louise, Leslie Regan Shade, and Tamara Shepherd. 2017. Open Privacy Badges for Digital Policy Literacy. *International Journal of Communication* 11: 2784–2805.
Srnicek, Nick. 2017. *Platform Capitalism*. Hoboken, NJ: John Wiley & Sons.
Stevens, Nikki, and Os Keyes. 2021. Seeing Infrastructure: Race, Facial Recognition and the Politics of Data. *Cultural Studies* 35 (4–5): 833–853.
Taplin, Jonathan. 2017. *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy*. New York: Little, Brown.
Therrien, Daniel. 2021. Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on Facial Recognition Technology. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2021/parl_20210510_02/ [accessed July 10, 2023].
———. 2022. The State of Privacy as I End My Term. Presented at at *The International Association of Privacy Professionals (IAPP) Canada Privacy Symposium, Toronto, Canada*, *May 26*. https://www.priv.gc.ca/en/opc-news/speeches/2022/sp-d_20220526/ [accessed July 25, 2022].

Weinberg, Lindsay. 2017. Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Communication and Culture* 12 (3): 5–20.
West, Sarah Myers. 2019. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society* 58 (1): 20–41.
Zimmer, Michael. 2010. "But the Data is Already Public": On the Ethics of Research in Facebook. *Ethics and Information Technology* 12: 313–325
Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89.
———. 2019a. *The Age of Surveillance Capitalism*. New York: Public Affairs.
———. 2019b. The Threat of Surveillance Capitalism, and the Fight for a Human Future. *ABC: Religion & Ethics*, August 21. https://www.abc.net.au/religion/shoshana-zuboff-threat-of-surveillance-capitalism/11433716 [accessed August 29, 2022].