

Facial Recognition Governance - April 2021

Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada

Yuan Stevens & Ana Brandusescu



Contents

- 3. About the Authors
- 4. About the Series
- 5. Summary
- 6. Introduction
 - 7. Why Recognition?
 - 9. The Harms of Facial Recognition
- 10. Facial Recognition and Law Enforcement
- 13. Canada's Vulnerable Legal Regimes
 - 13. Gaps in Canadian Privacy Law
 - 15. Weaknesses: Biometric Information, Privacy and Law Enforcement
 - 16. Exacerbating Risks and Harm (But We Deserve Better)
 - 17. The Loopholes of Public Sector Tech Procurement (Un)accountability
 - 17. Key Weaknesses: Jurisdictional Inconsistencies, Proactive Disclosure and Free Software Trials
 - 19. Profit Isn't Everything for the Tech Business Model
- 21. Conclusion
- 23. Endnotes



About the Authors

YUAN STEVENS

Policy Lead on Technology, Cybersecurity and Democracy, Ryerson Leadership Lab and Cybersecure Policy Exchange at Ryerson University

Yuan (“You-anne”) Stevens is a legal and policy expert focused on cybersecurity, privacy, and human rights. She brings years of international experience to her role at Ryerson University as Policy Lead on Technology, Cybersecurity and Democracy, having examined the impacts of technology on vulnerable populations in Canada, the US, and Germany. She has been conducting research on artificial intelligence since 2017 and has worked at Harvard University’s Berkman Klein Center for Internet & Society. She is a research affiliate at the Centre for Media, Technology and Democracy and Data & Society Research Institute. When she’s not examining the role of technology in creating dystopian futures in Canada and abroad, you can find her gardening on her balcony, taking apart hardware around her house, or keeping up with family members in Newfoundland.

ANA BRANDUSESCU

2019-21 McConnell Professor of Practice, Centre for Interdisciplinary Research on Montreal, McGill University

Ana Brandusescu is a researcher, advisor, and facilitator who works on a more publicly accountable use of data and technology. Currently, she is examining public investments in artificial intelligence (AI) to better understand its socio-economic implications. Ana is co-leading “AI for the Rest of Us”, a research project to develop a new model of public (civic) engagement in government decision making processes being automated with AI. She also serves on Canada’s Multi-Stakeholder Forum on Open Government. Previously at the World Wide Web Foundation, Ana led research on the implementation and impact of open government data in 115 countries, co-chaired the Measurement and Accountability Group of the international Open Data Charter, and co-led gender equality research advocacy.

About the Series

In this essay series, *Facial Recognition Governance*, McGill's [Centre for Media, Technology and Democracy](#) explores the policy, legal and ethical issues of facial recognition technologies faced on a global scale.

Facial recognition technology has expanded into various domains of public life including surveillance, policing, education, and employment, despite known risks ranging from identity-based discrimination and data privacy infringements to opaque decision-making. While policymakers around the world have proposed law and regulation of biometric technology, the governance landscape remains deeply divided across jurisdictions. This project evaluates the challenges posed by the adoption of facial recognition into high-stakes public contexts in order to inform the coordination and reform of global policies and to safeguard the publics on which this technology is used.



Summary

This essay highlights the Clearview AI scandal, as well as the push for a moratorium on FRT in Canada. We describe Canada's legal and government contracting systems as vulnerable systems that can bring harm to vulnerable populations. We then examine key weaknesses that exist in our privacy law and procurement practices with respect to law enforcement's use of FRT and conclude with ways forward.



1. Introduction

It was only in January 2020 that the public learned that law enforcement was using facial recognition technology provided by Clearview AI¹. Canadians learned that over 30 police departments in Canada had used free trials of Clearview AI's software without public knowledge². By that time, Canadian police had already run 3,400 searches across 150 accounts³. Privacy commissioners across the country also took notice in February, beginning an investigation into Clearview AI for using Canadians' personal information without consent⁴. It is unknown exactly which Canadian police departments used Clearview AI. No government agency or department has published this list. By February 2021, four privacy commissioners across Canada ruled that Clearview AI continues to engage in "mass surveillance" by scraping photos of people residing in Canada and refusing to delete images they have collected⁵.

Founded in 2017, Clearview AI claims to be a "web search for faces."⁶ The company has surreptitiously amassed a collection for their database of more than three billion public images from the open web. Clearview AI's software is used by the company's clients, the majority of which are governments and private companies all over the world⁷. The images are scraped from public accounts on websites like social media platforms⁸. The company culls images from websites and social media sites with little regard for applicable laws, without the permission of the websites from which they scrape and without the consent of those in the images⁹.





The Clearview AI scandal highlights how tech companies take advantage of weak privacy and procurement requirements in Canada to increase capital and power through the pretext of law enforcement protection and safety.

FRT is used to identify faces in digital images or videos¹⁰. The technology was borne out of “computer vision”, a field of study seeking to replicate the human process of observing patterns in images and videos¹¹. Similar “recognition” technology

can be used for fingerprints, genetic material, heartbeats and many other types of biometric or bodily data¹². FRT can be deployed in real-time, allowing for instantaneous identification. Police forces have already had access to such technology for several years with inadequate transparency and accountability. There are multiple, overlapping challenges in public procurement practices that allow companies like Clearview AI to operate without publicly tracking their deployments.

The Clearview AI scandal highlights how tech companies take advantage of weak privacy and procurement requirements in Canada to increase capital and power through the pretext of law enforcement protection and safety. This is just one example of how public investments are used by government to support the innovation economy with AI technologies¹³. In this essay, we demonstrate that the Clearview AI scandal reveals major existing ‘vulnerabilities’ in Canada’s privacy law and public sector tech procurement practices. We draw on the analytic framework of sociotechnical security, which identifies flaws in social systems that are entangled with technological systems, with the goal of protecting specific communities from the harm enabled by these flaws¹⁴. We identify two primary vulnerabilities when it comes to facial recognition software: (i) The omission of biometric information is a weakness in Canada’s privacy law that prizes organizational efficiency over the protection of dignity, and (ii) tech companies such as Clearview AI could easily take advantage of transparency requirements (or lack thereof) when public bodies in Canada enter into contracts with private companies.

1.2 Why Facial Recognition?

FRT is significant because it automates and speeds up a human process that would otherwise take an immense amount of time.



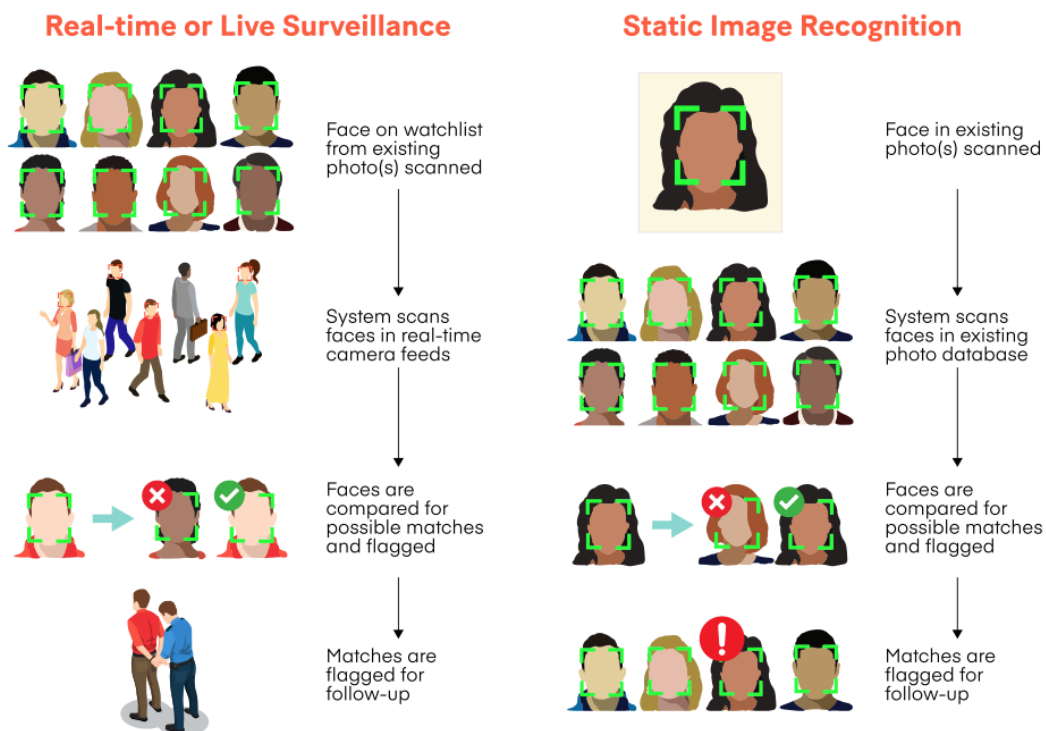


Figure 1. How it works: facial recognition technology. Facial Recognition Technology Policy Roundtable: What We Heard¹⁵.

What's the benefit of software like FRT that replicates human decision-making?

A stock phrase that has emerged in the data analytics industry involves the “three Vs” of big data¹⁶. Volume, velocity, and variety are routinely touted as the value added by data analysis software like FRT¹⁷. FRT like Clearview AI's software can analyze a significant amount of data (volume), categorize it as needed (variety), and do so at immense speeds (velocity).

FRT also has significant costs. Experts in Canada have identified the following key harms associated with the use of facial recognition software¹⁸:

- Lack of human autonomy over decisions;
- Lack of transparency for reasons behind certain results;
- Inaccuracy (e.g., false negatives);
- Discrimination; and
- Risk of unauthorized sensitive data access and manipulation.

1.3 The Harms of Facial Recognition

FRT perpetuates the subjective biases and values of the people who design and develop these systems, as well as the data used to train them¹⁹. As the computer science adage goes: garbage in, garbage out²⁰.

There is mounting evidence that FRT is discriminatory towards Black, Indigenous, people of colour (BIPOC) and trans people. For example, Joy Buolamwini and Timnit Gebru’s seminal research found IBM’s, Microsoft’s, and Face++ AI’s software to have racial and gender bias, where “darker-skinned females are the most misclassified group (with error rates of up to 34.7%). In contrast, the maximum error rate for lighter-skinned males is 0.8%²¹.” The research also found that 189 facial recognition algorithms were 10 to 100 times more likely to inaccurately identify Black and East Asian people²². Buolamwini’s research on another AI (artificial intelligence) system, Amazon Rekognition, shows similar patterns in race and gender bias: 100% accuracy on lighter males and 68.6% accuracy on darker females²³.

It is important to note that “there are other marginalized groups or cases to consider who may be being ignored. For instance, dysfunction in facial analysis systems locked out transgender Uber drivers from being able to access their accounts [in order] to begin work²⁴.” In light of these harms, Luke Stark calls facial recognition the ‘plutonium of AI’: “it’s dangerous, racializing, and has few legitimate uses; facial recognition needs regulation and control on par with nuclear waste²⁵.”

When FRT is used in real-time, such harms can occur even faster. An example of real-time or “live” FRT involves disturbing results that came out of a study from 2020. Administrators at UCLA (University of California, Los Angeles) proposed a program that would use live FRT on their campus CCTV cameras²⁶. The digital rights non-profit Fight for the Future stepped in to support students’ efforts against the program²⁷. To support this effort, Fight for the Future ran a test using Amazon Rekognition to compare more than 400 photos of the school’s faculty members and athletes to a mugshot database. The software falsely matched only 58 of the photos with images from the database with “100% confidence.” The vast majority of the incorrectly matched photos depicted people of colour²⁸. UCLA ultimately abandoned their plan to use FRT on campus²⁹. This example highlights that when organizations implement FRT, they systematize deeply-held biases to the detriment of marginalized groups and can do so at alarming speed³⁰.



2. Facial Recognition and Law Enforcement

The underlying question to ask when it comes to FRT is this: “Do we want to live in a society where, when we walk on the street, we are essentially part of a perpetual police line-up?³¹”

Facial recognition is not new in Canada. Government bodies like the Royal Canadian Mounted Police (RCMP) have been using it for the last 18 years³². The RCMP, Canada’s national police force, is unique in the world as a combined international, federal, provincial and municipal policing body³³. FRT has also been used in the province of Ontario and in cities like Calgary, Edmonton, Ottawa and Toronto³⁴. The Toronto Police Service relied on FRT to identify three men accused of murder, all of whom were sentenced to life in prison in March 2020³⁵.

Out of the law enforcement agencies that trialled Clearview AI’s software in Canada, 50% of them were in Ontario. By July 2020, Canadian privacy commissioners conducted an investigation and stated that Clearview AI was no longer providing its services to the RCMP as a result of their inquiry³⁶. The Office of the Privacy Commissioner (OPC) publicly announced that Clearview AI would “cease offering its facial recognition services in Canada³⁷.” OPC’s statement declared the “indefinite suspension” of Clearview AI’s contract with the RCMP, which was apparently Clearview AI’s last remaining Canadian client³⁸.

Despite the fact that the RCMP and all other law enforcement agencies in the country have ostensibly stopped using Clearview AI’s product, the first and only testimony on Clearview AI’s page comes from a Canadian law enforcement agent (see Figure 2).



FRT, biometrics, and AI are nebulous terms that further obfuscate how to search for them on public record, especially details around classification and terminology used for the technology itself.

"Clearview AI is hands-down the best thing that has happened to victim identification in the last 10 years. Within a week and a half of using Clearview AI, [we] made eight identifications of either victims or offenders through the use of this new tool."

Detective Constable in the Sex Crimes Unit
Canadian Law Enforcement

"Clearview AI is hands-down the best thing that has happened to victim identification in the last 10 years. Within a week and a half of using Clearview AI, [we] made eight identifications of either victims or offenders through the use of this new tool."

Detective in the Sex Crimes Unit
Law Enforcement

Figure 2. Screenshots of Clearview AI website only testimony from September 17, 2020 (above) and October 6, 2020 (below). Notice that the company removed "Constable" and "Canadian" in the updated version. This most likely a quote from someone at the RCMP – the only law enforcement agency in Canada to have signed a contract with Clearview AI.

Clearview AI provides a window into much larger conversations happening in Canada and the US. Amnesty International then published a letter in July 2020 signed by 77 privacy, human rights and civil liberties advocates, calling for the immediate ban on FRT for Canada's law enforcement and intelligence agencies³⁹. Beyond law enforcement, "the problem of large-scale surveillance-data collection and the deployment of AI-based facial-recognition technology will only get more challenging as more of our public spaces become governed by private companies⁴⁰." To this extent, Open Media, a Canadian digital rights non-profit, launched the "Stop Clearview AI's Facial Recognition" campaign to provide support for individuals to retrieve data about them from Clearview AI⁴¹.

The harms associated with the use of FRT by law enforcement are so significant that cities across the US have banned their police forces from using the technology. City governments that banned FRT include Portland (Maine), Portland (Oregon), San Francisco and Oakland⁴². In June 2020, lawmakers in the US proposed a bill to ban the use of FRT by federal law enforcement⁴³. Even Big Tech seems to agree that there is imminent need for better regulation over the use of this technology. When George Floyd was tragically murdered in May 2020⁴⁴, IBM, Amazon, and Microsoft released public statements in June 2020 stating that they would temporarily cease providing their FRT software to police departments until the US federal government enacted law to protect people's fundamental freedoms and rights to privacy⁴⁵. The UK Court of Appeal rendered a landmark decision in August 2020, holding that the use of FRT by police breaches data protection as well as both equality and privacy laws⁴⁶.

In contrast, Canada's current approach to regulating the harms of FRT is *laissez-faire*, involving few enforceable requirements for privacy rights in biometric information or transparent procurement processes of technology for law enforcement. This approach renders Canada's privacy law and procurement systems vulnerable in ways we describe below.



3. Canada's Vulnerable Legal Regimes

3.1 Gaps in Canadian Privacy Law

“Privacy is about power. It is about how law allocates power over information⁴⁷.” Privacy law in Canada, as it does elsewhere around the world, “determines who ought to be able to access, use, and alter information⁴⁸.” Laws that protect privacy are one of main tools in North America to protect human dignity, personal integrity, as well as control and autonomy over one’s information and body⁴⁹. Yet Canadian privacy law fails to protect biometric information, including facial patterns and images. This legal gap puts us at greater risk of surveillance by law enforcement as well as violations of our fundamental rights protected under the *Charter of Rights and Freedoms*⁵⁰.

Canada’s privacy law is regulated at the federal and provincial levels, and is generally split into the public and private sectors. At the federal level, the *Privacy Act* dictates how federal government institutions — such as the RCMP — collect, use, and disclose personal information⁵¹. The *Privacy Act*, enacted in 1983, provides a right to access to this information as well as the right to correct this information. The law also established the Office of the Privacy Commissioner (OPC) of Canada⁵², which acts as an oversight body for the *Privacy Act*.

The OPC also provides oversight for Canada’s federal private sector privacy law enacted in 2000, the *Personal Information Protection and Electronic Documents Act* (PIPEDA)⁵³. PIPEDA provides guidelines on the collection, use,

and disclosure of personal information for private organizations in the course of for-profit, commercial activities across Canada⁵⁴. PIPEDA applies for all personal information that crosses provincial or national borders, and does not apply to organizations that operate entirely within Alberta, British Columbia, or Quebec. These three provinces have private-sector privacy laws that have been deemed substantially similar to PIPEDA⁵⁵.

The Canadian federal government began long-awaited concrete efforts to overhaul PIPEDA through the proposal of C-11 in November 2020⁵⁶. The Department of Justice also began a public consultation on the *Privacy Act* in the same month, with submissions due in early 2021⁵⁷. A discussion paper released with the public consultation launch stated that the “Government is not currently considering specifying categories of personal information to which special rules would apply (such as “sensitive” personal information or information relating to minors), though some other jurisdictions do so⁵⁸.”

Yet data protection laws such as the EU’s General Data Protection Regulation (GDPR)⁵⁹, the UK’s Data Protection Act⁶⁰ and California’s Consumer Protection Privacy Act⁶¹ all acknowledge the existence of biometric information. The GDPR requires EU member states to presumptively prohibit the processing of special category data such as biometric information for the purpose of uniquely identifying a person⁶². In our scan of privacy law at all levels of Canadian government and in both the public and private sectors, we identified only two pieces of privacy legislation that account for the existence of biometric information⁶³. Only the provincial governments of Alberta and Prince Edward Island acknowledge biometric information in privacy law that applies to government but not industry. Quebec is the only province that requires both government *and* industry to disclose when they “create” a database of biometric information⁶⁴. Canadian privacy law therefore fails to protect biometric information as it occurs elsewhere around the world.

All levels of government in Canada are putting at risk the privacy and security of people’s information. Canadian government bodies are failing to adequately account for (and therefore adequately protect) information such as our facial patterns. Fundamental freedoms like privacy are never wholly absolute. Governments must strike a balance between the dignitary interest in privacy and the necessity of public safety. It is therefore critical to provide explicit regulation for the object of protection — in this case biometric information — serving as a fault line over these dividing interests.



A. Weaknesses: Biometric Information, Privacy and Law Enforcement

There are two primary ways for law enforcement to process Canadians' facial information through FRT: 1) Law enforcement agencies can procure software or services from a third party (e.g. Toronto and Calgary of NEC's mugshot database⁶⁵) and; 2) law enforcement agencies and their employees can access FRT databases used by other government bodies.

The collection, use, and processing of data by law enforcement is of critical importance. In contrast to Canada, legislators in the EU have enacted a separate, detailed piece of legislation, the *Data Protection Law Enforcement Directive*⁶⁶. An addition to the GDPR, the Directive limits when law enforcement agencies can process biometric data. The Directive states that law enforcement can process biometric data for identification purposes only when doing so is necessary and appropriately safeguards privacy rights, in addition to at least one other procedural condition from a list of options⁶⁷.

On the other hand, Canada's privacy law for federal public bodies makes no mention of biometric information; in fact, legislators have actively decided against acknowledging its existence as mentioned above⁶⁸. The *Privacy Act* simply allows these bodies to disclose our personal information in a vast array of situations — including to the RCMP, so



When we compare Canada's privacy laws to the more robust protection provided by laws like the GDPR, it is clear that privacy law in Canada neither explicitly allows nor prohibits law enforcement agencies from processing biometric information.

long as it provides a written request that merely specifies the request is for law enforcement purposes and describes the information sought⁶⁹. Ontario's public sector privacy law provides an even more laissez-faire approach: law enforcement is simply granted the ability to access and use information collected by another public body, without any mention of a requirement to provide a written request⁷⁰. In short, the bar in Canada is extremely low for law enforcement to access and use our personal data, and by extension, our biometric data.

When we compare Canada's privacy laws to the more robust protection provided by laws like the GDPR, it is clear that privacy law in Canada neither explicitly *allows* nor *prohibits* law enforcement agencies from processing biometric information. It is difficult to find any provision in Canadian privacy law that explicitly and unequivocally allows law enforcement to access, use, or process our biometric information⁷¹. We have not uncovered any law in Canada that *prevents* the use by law enforcement of biometric information, such as facial patterns for identification purposes. Nor is there anything in Canadian law that prevents law enforcement agencies from procuring facial recognition software.

B. Exacerbating Risks and Harm (But We Deserve Better)

This regulatory oversight renders our legal system vulnerable. Cumulative weaknesses in Canada's legal system can be exploited by law enforcement and tech companies. We have seen this happen with companies like Clearview AI. By failing to acknowledge that biometric information exists and deserves extra protection due to its (highly) sensitive nature, this gap in federal and provincial Canadian privacy regulation currently leaves our legal systems (and this type of information) susceptible to exploitation. People working at law enforcement agencies can be lured in by tech companies' promises of increased organizational efficiency through collection, analysis and predictions arising from our biometric information at huge scale.

The risk of harm when it comes to law enforcement's use of biometric information and automated decision-making technology cannot be understated. Echoing our explanation above of the risks posed by facial recognition software, it has long been understood by Canadian courts that the collection of bodily information without a person's consent is a serious violation and invasion of one's body and privacy⁷². This intrusion is the "ultimate invasion of personal dignity and privacy⁷³." Our bodily and particularly facial data is comprised of inherited, immutable characteristics that, by virtue of these characteristics, can be the subject of discrimination⁷⁴. When our body is violated, we are deprived of our dignity, integrity and autonomy as fundamental aspects of the *Canadian Charter of Rights and Freedoms*⁷⁵.

The Supreme Court of Canada has determined that legislators must work to prevent intrusions into our private lives by the state *before* intrusions occur. "If the privacy of the individual is to be protected," the Court ruled, "we cannot afford



to vindicate it only after it has been violated⁷⁶.” If the state otherwise decides that certain invasions of privacy are nonetheless to be tolerated (to achieve another societal purpose), then “there must be clear rules setting forth the conditions in which [privacy] can be violated⁷⁷.” This is especially true when law enforcement violates our privacy, because the consequences can involve deprivation of our freedom and liberty including punishment in prison. In other words, law enforcement must be made to satisfy certain conditions in Canada before using our biometric information due to potential for abuse.

Canada’s vulnerable legal system maintains and exacerbates the vulnerability already experienced by certain communities in Canada. Those who stand to be the most affected by gaps in Canada’s privacy laws — including people of colour (particularly Black and Indigenous populations), people in the LGBTQ community, women, religious minorities, etc. — deserve better from the Canadian government, and a first logical step involves acknowledging the existence in our privacy laws of biometric information.

3.2 The Loopholes of Public Sector Tech Procurement (Un)accountability

The Clearview AI scandal demonstrates the dire need for public sector tech procurement reform in Canada. There are multiple, overlapping challenges in tech procurement practices that allow the government to enter into agreements with companies like Clearview AI without public knowledge. First, there are jurisdictional inconsistencies in the openness of contracting information and proactive disclosure policies. Second, many government contracts awarded to technology firms fall below the minimum amount set for public and proactive disclosure. And third, free trials that companies give to government agencies and departments essentially override the procurement process.

A. Key Weaknesses: Jurisdictional Inconsistencies, Proactive Disclosure and Free Software Trials

Since 2004, public procurement in Canada at the federal level has proactively disclosed government contracts that are over \$10,000. Proactive disclosure embodies the open government mantra of transparency and accountability in

government⁷⁸. Proactive disclosure extends to Canada's commitment as a member of the Open Government Partnership (OGP). The OGP is an initiative established during the Obama administration, consisting of 78 countries — including national and local governments with civil society counterparts⁷⁹.

Proactive disclosure is managed by the Treasury Board Secretariat of Canada, a government agency that oversees how public resources (i.e., goods and services) are allocated in the federal government⁸⁰. On top of government tenders, the public can search for contracts or awards that the government has awarded to different suppliers. Contracts are searchable by department and amount. Beyond contracts, standing offer agreements and supply arrangements used by government departments are also publicly and openly searchable. The publication of contracts are reported every three months based on contracts awarded by CIC in the three months prior⁸¹.

There is insufficient proactive disclosure of public contracts beyond the federal government. In the Clearview AI case, the majority of law enforcement agencies that used the company's software are municipalities based in the province of Ontario, a jurisdiction that does not have an open public procurement registry.



Clearview AI was never listed as a vendor to any of the law enforcement agencies because the company offered free trial versions of their software.

For example, the Government of Ontario's enterprise-wide

Vendor of Record Program provides a list of companies that they contract for goods and services commonly acquired by government ministries⁸². At the provincial level, "the Ontario Public Service Procurement Directive requires ministries to post contract award notifications for competitive procurement processes valued at \$25,000 or more for goods and \$100,000 or more for services⁸³." Notices of opportunities and awards are required above a given threshold for all public bodies. This obligation comes from local laws, as well as from trade agreements with the EU and others. However, the accessibility of the information varies. The Ontario Tenders Portal uses Jaggaer (one of the big providers of tendering portals), which loads very slowly, but allows for filtering by award value to find non-zero awards⁸⁴. The open data catalogue seems to have a variety of datasets because procurement is not fully centralized, similar to federal government procurement⁸⁵.

In the case of municipal and provincial jurisdictions across Canada, Clearview AI was never listed as a vendor to any of the law enforcement agencies because the company offered free trial versions of their software. Offering free software trials and selling their services for extremely low prices is an effective strategy for Clearview AI to attract clients⁸⁶. The next effect meant that any person or organization “could access Clearview AI for as little as \$2,000 per year. Most comparable vendors — whose products are not even as extensive — charged six figures.” Consequently, Clearview AI’s business model evaded Canada’s public procurement process requirements for nearly all law enforcement agencies that used their product. In fact, only one agency (the RCMP) entered into a contract with the company. The rest of the units used free trials. There is no proactive disclosure when no contracts exist.

Software companies (vendors), like in any field, showcase their products at conferences⁸⁷. In this instance, Clearview AI presented at child exploitation conferences to advertise the chance to try their software for 30 to 60 days⁸⁸, all while expanding their network and creating new connections within governments all over the world. Of course, Clearview AI still has private clients, yet it chooses to focus on public clients — especially law enforcement agencies. In Figure 2, we see an endorsement of the company’s credibility by law enforcement employees⁸⁹.

B. Profit Isn’t Everything for the Tech Business Model

Clearview AI’s business model is effective from a private interest standpoint in that its use was quick and efficient. Arguably, the company’s added value is the analysis (i.e., the business intelligence) it collects based on its user base and behaviour. There were no bureaucratic time restrictions or context-based laws they had to comply with as no government contract was required. In addition to the free trials provided by Clearview AI, the software is affordable. The company’s contract with the RCMP totalled \$5,000 — well under the \$10,000 government contract proactive disclosure limit set by the Government of Canada. According to Clearview AI’s CEO, the “ballpark” cost of the Clearview AI software is \$2,000/year per officer⁹⁰. When one searches for “Clearview AI” zero records are found⁹¹. In this case, the policies set forth by open government are insufficient, with the public having no access to the contract because no contract ever existed.



However, this does not negate the fact that as taxpayers, we are essentially paying to be surveilled, where companies like Clearview AI can exploit public sector tech procurement processes.

Clearview AI is one of many FRT companies that has provided services to law enforcement departments without the public's knowledge. One reason could be that their contracts are well below the \$10,000 threshold. Even if the contracts exceed \$10,000, these contracts are not always

published. Some contracts under the RCMP or the National Defence, for example, are considered to be of national security and therefore remain closed. If the public had access to that information, much more information could have surfaced from the Clearview AI case. NEC corporation is a supplier of the Toronto Police Service (TPS), as well as many other law enforcement agencies across the country⁹². The TPS website publishes tenders but not contract awards⁹³. In a 2019 Public Meeting, the TPS includes the \$451,000 grant awarded to NEC, demonstrating that transparency is possible⁹⁴.

The focus on costs is too limited in scope, as FRT companies are inexpensive (in the thousands of dollars, not millions). In fact, this is what makes them so attractive to law enforcement agencies. However, this does not negate the fact that as taxpayers, we are essentially paying to be surveilled, where companies like Clearview AI can exploit public sector tech procurement processes. The surveilling and sorting analysis made possible by Clearview AI's software (and the billions of images it stores) is more valuable — and dangerous — than we know.



Conclusion



First they had our fingerprints. Now they have our faces. The case of Clearview AI reveals long-standing gaps and weaknesses in Canadian privacy law, and opaque selection practices when it comes to FRT. Tech companies and law enforcement are taking advantage of weak legal requirements in Canada to increase capital and power through the pretext of public safety. Law enforcement may serve and protect, but they also surveil, control, and conceal.

Eventually they could have our voices, gait, veins, heartbeats, signatures and more. It is not just law enforcement that wants unfettered access to our highly sensitive biometric data with the use of FRT. Ruha Benjamin aptly states: “And so it’s not just police use of it [facial recognition system], but across our institutions: educational, healthcare. We [also] have to be wary of the idea that these systems are accurate and neutral, but also of the way that they reinforce racist forms of policing and surveillance⁹⁵.” As a result, our findings have implications for *all* sectors of society where organizations are increasingly relying on automated decision-making systems that surveil, sort us into categories and deprive us of the privacy and freedom from discrimination that we deserve.

In Canada, government agencies and tech companies — of all kinds — can currently take advantage of the non-existence of biometric information in privacy law and a lack of transparency requirements for government contracts. Therefore, it is important for governments to require mandatory privacy impact assessments⁹⁶, as well as algorithmic impact assessments (AIA⁹⁷) (e.g., Government of Canada AIA), with consequences for non-compliance. Governments should also consider applying legislation like the Directive on Automated Decision-Making⁹⁸ across multiple jurisdictions in Canada⁹⁹.

The risks of harm emanating from FRT are significant. The power wielded by those with techno-utopian ideals can facilitate serious violations of our privacy by law enforcement and tech companies, as well as the sorting or categorization

of people resulting in discrimination, alienation and ostracization. Ultimately, law enforcement's use of FRT will only sustain and worsen the legacy of mistrust between the government and the public.

The failure to acknowledge biometric information in privacy law and a lack of transparency for government contracts allows for exploitation of these gaps in Canadian policy. But it is Canada's marginalized communities who will most acutely experience the harm arising from this exploitation and who deserve protection, transparency, and accountability.

Endnotes

- 1 Hill, K. ["The Secretive Company That May End Privacy As We Know It."](#) *The New York Times*, 2020; ["Announcement: OPC launches investigation into RCMP's use of facial recognition technology."](#) *Office of the Privacy Commissioner of Canada*, 2020.
- 2 Mac, R., Haskins, C., and McDonald, L. ["Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, and The NBA."](#) *BuzzFeed News*, 2020.
- 3 Ibid.
- 4 ["Announcement: Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology."](#) *Office of the Privacy Commissioner of Canada*, 2020.
- 5 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, PIPEDA Report of Findings #2021-001, 2021.
- 6 ["Clearview AI's founder Hoan Ton-That speaks out \[Extended interview\]."](#) *CNN Business*, 2020.
- 7 Hill, K. ["The Secretive Company That May End Privacy As We Know It."](#) *The New York Times*, 2020.
- 8 O'Flaherty, K. ["Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked."](#) *Forbes*, 2020.
- 9 Hill, K. ["The Secretive Company That May End Privacy As We Know It."](#) *The New York Times*, 2020.
- 10 Owen, T., Ruths, D., Cairns, S., Parker, S., Reboul, C., Rowe, E., Solomun, S., and Gilbert, K. ["Facial Recognition Briefing #1."](#) *TIP – Tech Informed Policy*, 2020.
- 11 Zhao, W., Rama Chellappa, P., Phillips, J., and Rosenfeld, A. ["Face Recognition: A Literature Survey."](#) *ACM computing surveys (CSUR)*, vol.35, no.4, 2003, pp.399-458.
- 12 See e.g. ["Types of Biometrics,"](#) *Biometrics Institute* (blog) for an explanation of the various types of data (e.g. visual, chemical, behavioural) that can be analyzed.
- 13 Brandusescu, A. ["Artificial Intelligence Policy and Funding in Canada: Public investments, Private interests."](#) *Centre for Interdisciplinary Research on Montreal*, McGill University, 2021.
- 14 Goerzen, M., Watkins, E.A. and Lim, G. ["Entanglements and Exploits: Sociotechnical Security as an Analytic Framework."](#) *USENIX Workshop on Free and Open Communications on the Internet*, 2019.
- 15 ["Facial Recognition Technology Policy Roundtable: What We Heard."](#) *The Cybersecure Policy Exchange and Tech Informed Policy Initiative*, 2021.
- 16 There may also be four Vs or five Vs depending on the source.
- 17 ["Volume, Velocity, Variety: What You Need to Know About Big Data."](#) *Forbes*, 2012; ["Data Protection Act and General Data Protection Regulation: Big data, artificial intelligence, machine learning and data protection."](#) *UK's Information Commissioner's Office*, n.d.
- 18 ["Facial Recognition Technology Policy Roundtable: What We Heard. Cybersecure Policy Exchange."](#) *The Cybersecure Policy Exchange and Tech Informed Policy Initiative*, 2021.
- 19 Robertson, K., Khoo, C., and Song, Y. ["To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada."](#) *Citizen Lab and International Human Rights Program*, 2020, p. 25.



- 20 Garvie, C. "Garbage In, Garbage Out: Face Recognition on Flawed Data." *Georgetown Law Center on Privacy & Technology*, 2019.
- 21 Buolamwini, J. and Gebru, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." In *Conference on fairness, accountability and transparency*, 2018, pp. 77-91.a
- 22 Hao, K. "A US Government Study Confirms Most Face Recognition Systems are Racist." *MIT Technology Review*, 2019.
- 23 Buolamwini, J. "Response: Racial and Gender Bias in Amazon Rekognition — Commercial AI System for Analyzing Faces." *Medium*, 2019.
- 24 Raji, I.D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., and Denton, E. "Saving face: Investigating the Ethical Concerns of Facial Recognition Auditing." *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, pp. 145-151; Melendez, S. "Uber Driver Troubles Raise Concerns About Transgender Face Recognition." *Fast Company*, 2018.
- 25 Stark, L. "Facial Recognition is the Plutonium of AI." XRDS: Crossroads, *The ACM Magazine for Students*, vol. 25, no. 3, 2019, pp. 50-55.
- 26 Law, K. "Students Share Concerns about Facial Recognition on Campus Security Cameras." *Daily Bruin*, 2021.
- 27 Paul, K. "'Ban This Technology': Students Protest US Universities' Use of Facial Recognition." *The Guardian*, 2020.
- 28 Fight for the Future, "Backlash Forces UCLA to Abandon Plans for Facial Recognition Surveillance on Campus." *Fight for the Future*, 2021.
- 29 Burke, L. "Facial Recognition Surveillance on Campus." *Inside Higher Ed*, 2020.
- 30 Israel, T. "Facial Recognition at a Crossroads: Transformation at our Borders & Beyond." *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic*, 2020.
- 31 McPhail, B., Israel, T., Schroeder, J., & Lucht, B. Facial Recognition: A Pathway or Threat to our Future. *Centre for Free Expression*, 2021, 75:59.
- 32 Carney, B. "'You Have Zero Privacy' Says an Internal RCMP Presentation. Inside the Force's Web Spying Program." *The Tyee*, 2020.
- 33 Organization for Security and Co-operation in Europe. "Country profile: Canada." n.d. Canada has three levels of police services: municipal, provincial, and federal.
- 34 Robertson, K., Khoo, C., and Song, Y. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada." *Citizen Lab and International Human Rights Program, University of Toronto*, 2020, p. 62.
- 35 Powell, B. "How Toronto Police Used Controversial Facial Recognition Technology to Solve the Senseless Murder of an Innocent Man." *The Toronto Star*, 2020.
- 36 Solomon, H. "Clearview AI cancels contract with RCMP and is no longer offering its facial recognition tech in Canada." *Financial Post*, 2020.
- 37 "Clearview AI ceases offering its facial recognition technology in Canada." *Office of the Privacy Commissioner of Canada*, 2020.
- 38 Carney, B. "Clearview, Maker of RCMP's Facial Recognition Software, Exits Canada." *The Tyee*, 2020.
- 39 Amnesty International. "Open Letter: Canadian Government Must Ban Use of Facial Recognition Surveillance by Federal Law Enforcement, Intelligence Agencies." *Amnesty International Canada News*, 2020.
- 40 Owen, T., and Ahmed, N. "Opinion: Let's Face the Facts: To Ensure Our Digital Rights, We Must Hit Pause on Facial-Recognition Technology." *The Globe and Mail*, 2020.
- 41 Open Media. "Take back your data from Clearview AI!" *Open Media*, n.d.
- 42 Statt, N. "Massachusetts on the Verge of Becoming First State to Ban Police Use of Facial Recognition." *Vox*, 2020.
- 43 Jee, C. "A New US Bill Would Ban the Police Use of Facial Recognition." *MIT Technology Review*, 2020.
- 44 Hill, E., Tiefenthäler, A., Triebert, C., Jordan, D., Willis, H., and Stein, R. "How George Floyd Was Killed in Police Custody." *The New York Times*, 2020.

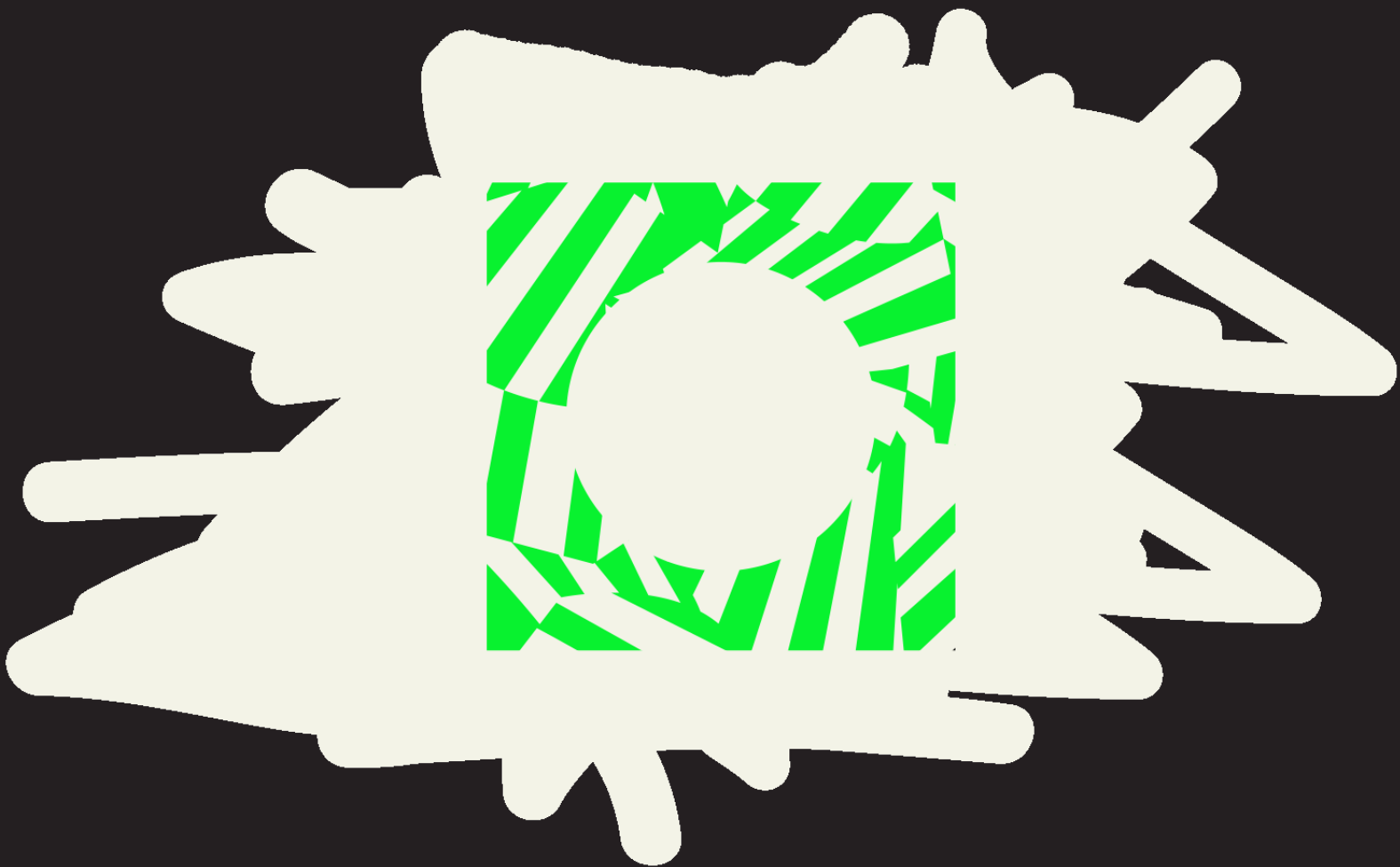


- 45 Krishna, A. “IBM CEO’s IBM CEO’s Letter to Congress on Racial Justice Reform.” *IBM*, 2020; Haskins, C. “Amazon Is Suspending Police Use Of Its Facial Recognition Tech For One Year.” *BuzzFeed News*, 2020; Heilwell, R. “Big Tech Companies Back Away from Selling Facial Recognition to Police. That’s Progress.” *Vox*, 2020.
- 46 Winder, D. “Police Facial Recognition Use Unlawful—U.K. Court Of Appeal Makes Landmark Ruling.” *Forbes*, 2020.
- 47 Bambauer, D.E. “Privacy Versus Security.” *Journal of Criminal Law & Criminology*, vol. 103, 2013, p. 667.
- 48 Ibid.
- 49 Resta, G. “Personnalité, Persönlichkeit, Personality.” *European Journal of Comparative Law and Governance*, vol. 1, no. 3, 2008, p. 215; Bailey, J. “Towards an Equality-Enhancing Conception of Privacy.” *Dalhousie Law Journal*, vol. 31, no. 2, 2008, p. 267.
- 50 The Constitution Act, Schedule B to the Canada Act 1982 (UK), 1982, c 11; Stevens, Y., and Solomun, S. “Facing the Realities of Facial Recognition Technology: Recommendations for Canada’s Privacy Act.” *Cybersecure Policy Exchange*, 2021.
- 51 Privacy Act, RSC 1985, c P-21.
- 52 Privacy Act, RSC 1985, c P-21, at section 53.
- 53 Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
- 54 “Summary of Privacy Laws in Canada.” *Office of the Privacy Commissioner of Canada*, 2014.
- 55 Ibid.
- 56 Hyslop, C. “Bill C-11: Canada Proposes New Data Privacy Legislation.” *Norton Rose Fullbright Blog*, 2020.
- 57 “Government of Canada Launches Public Consultation on the Privacy Act.” *Department of Justice News Releases*, 2020.
- 58 “Respect, Accountability, Adaptability: A Discussion Paper on the Modernization of the Privacy Act.” *Department of Justice*, 2020.
- 59 European Parliament and Council of European Union. Regulation (EU) 2016/679, at Articles 4(14), 9(1), 9(4), and Recitals 51, 53, 91.
- 60 Data Protection Act 2018, c. 12.
- 61 AB375, Title 1.81.5, The California Consumer Privacy Act of 2018, CCPA.
- 62 European Parliament and Council of European Union (2016) Regulation (EU) 2016/679, at Article 9(1).
- 63 Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25, <http://canlii.ca/t/5442j> [Alberta]; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, <<https://canlii.ca/t/54vnx>> [PEI]. Out of scope for this essay is health sector privacy laws.
- 64 An Act to Establish a Legal Framework for Information Technology, SQ 2001, c 32, at s. 45. Law was proposed in 2020 that would require a timeframe within which organizations must disclose to the information commissioner when a biometric database is brought into service, see e.g., Reynolds, M. et al. “Québec’s Bill 64 Proposes Sweeping Changes To Its Privacy Regime.” *Mondaq*, 2020.
- 65 Presser, J. “Perils of Facial Recognition Algorithmic Tools in Policing.” *The Lawyer’s Daily*, 2019; “Calgary Police Launch New Facial Recognition Crime-Fighting Tool.” *The Calgary Herald*, 2014.
- 66 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, at Articles 10 and 11.
- 67 Ibid at Article 10.
- 68 “Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act.” *Department of Justice*, 2020: “The Government is not currently considering specifying categories of personal information to which special rules would apply (such as “sensitive” personal information or information relating to minors), though some other jurisdictions do so.”
- 69 Privacy Act, RSC 1985, c P-21, at s. 8(2).
- 70 Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, at s. 39(g).



- 71** This is true whether for the purpose of broadly aiding police investigations or to specifically allow the police to uniquely identify an individual, the latter which is presumptively prohibited under the GDPR.
- 72** *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 SCR 281 para 93; *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44 (CanLII), [2000] 2 SCR 307, para 50, citing *R. v. Morgentaler*, 1988 CanLII 90 (SCC) at p. 166.
- 73** *R. v. Stillman*, 1997 CanLII 384 (SCC), [1997] 1 SCR 607, para 87.
- 74** Reference re Genetic Non Discrimination Act, 2020 SCC 17 (CanLII), at headnote and paras 82-90.
- 75** Ibid; *The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK)*, 1982, c 11.
- 76** *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 SCR 417 at para 23.
- 77** Ibid.
- 78** “Proactive Disclosure - Contracts.” *Government of Canada, Open Data Portal*, n.d.
- 79** Open Government Partnership. “Members.” *Open Government Partnership*, 2020.
- 80** “Contracting Policy.” *Government of Canada, Treasury Board Secretariat of Canada*, n.d.
- 81** “The rules and principles governing government contracting are outlined in the *Treasury Board Contracting Policy*.”
- 82** Government of Ontario. “Enterprise Vendor of Record Arrangements.” *Ontario Data Catalogue*, n.d.
- 83** Government of Ontario. “Procurement and Contracts.” *Open Government Open Data Guidebook: A Guide to the Open Data Directive*, 2019.
- 84** Zero-value awards are for unsuccessful procedures. The Excel export is fairly minimal, with more information actually available on the Ontario Tenders Portal itself; Personal conversation with James McKinney, open contracting and open data expert.
- 85** Ibid.
- 86** Hill, K. “Your Face Is Not Your Own.” *The New York Times*, 2021.
- 87** “Cornwall Police Officers Dabbled in Facial Recognition Software: Clearview AI to Leave Canadian Market.” *Cornwall Newswatch*, 2020.
- 88** “Clearview AI’s founder Hoan Ton-That speaks out [Extended interview].” *CNN Business*, 2020.
- 89** Mac, R., Haskins, C., and McDonald, L. “Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, and The NBA.” *BuzzFeed News*, 2020.
- 90** “E1100: Clearview AI CEO Hoan Ton-That on Balancing Privacy & Security, Engaging with Controversy.” *This Week In Startups*, 2020.
- 91** “Government Contracts Over \$10,000: Keyword Search.” *Government of Canada*, n.d.
- 92** Burt, C. “Toronto Police Talk Responsible Use of NEC Facial Recognition in First Case to Identify Murderers.” *Biometric Update*, 2020.
- 93** “Tenders by Toronto Police Service.” *Toronto Police Service*, n.d.
- 94** Toronto Police Services Board. “Public Meeting.” *Toronto Police Service*, 2019, p. 244.
- 95** Benjamin, R., and Young, N. “How Emerging Technologies Amplify Racism - Even When They’re Intended to be Neutral.” *CBC Spark*, 2020.
- 96** “Privacy Impact Assessments (PIAs).” *Office of the Privacy Commissioner of Canada*, n.d.
- 97** “Algorithmic Impact Assessment (AIA).” *Government of Canada*, n.d.
- 98** “Directive on Automated Decision-Making.” *Government of Canada*, n.d.
- 99** Stevens, Y., and Solomun, S. “Facing the Realities of Facial Recognition Technology: Recommendations for Canada’s Privacy Act.” *Cybersecure Policy Exchange*, 2021.





Designed by Yasmeeen Safaie



Centre for
MEDIA,
TECHNOLOGY
and DEMOCRACY



McGill
UNIVERSITY



**MAX BELL SCHOOL
of PUBLIC POLICY**