Facing the Realities of Facial Recognition Technology

Recommendations for Canada's *Privacy Act*

Yuan Stevens & Sonja Solomun | February 2021

cybersecure policy exchange
Powered by RBC

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

cybersecure
policy
exchange
Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of digital privacy and security policy in Canada, and to create and advance innovative policy responses. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

For more information, visit: https://www.cybersecurepolicy.ca/

Centre *for* MEDIA,
TECHNOLOGY
and DEMOCRACY

Centre for Media, Technology and Democracy at McGill University

Collaborating with a network of academic, policy, journalistic and community stakeholders, the Centre for Media, Technology and Democracy works to understand and address the democratic harms of emerging media technologies and to inform and develop fair and accountable governance systems. The Centre for Media, Technology and Democracy produces critical research, policy activism, and inclusive events that inform public debates about the changing relationship between media and democracy, and that ground policy aimed at maximising the benefits and minimizing the systemic harms embedded in the design and use of emerging technologies.

@MediaTechDem

For more information, visit: https://www.mediatechdemocracy.com/

Facial Recognition Technology Policy Roundtable

In November 2020, the Cybersecure Policy Exchange and the **Tech Informed Policy** (TIP) initiative at McGill University convened 30 expert stakeholders and government officials for a roundtable on the governance of facial recognition technology (FRT), examining the implications of a temporary prohibition on the public sector's use of FRT in Canada. This submission and its policy recommendations build upon the ideas discussed during the roundtable event. For a full summary of the roundtable, please visit https://www.cybersecurepolicy.ca/reports.[1]

Table of Contents

Executive Summary

Canada's federal institutions are collecting, using, and disclosing people's facial information. They are also increasingly relying on technology that uses this information, in combination with automated decision-making processes, to uniquely identify individuals. This is happening in Canada today, without adequate direction and protection from the *Privacy Act*. The use of this technology raises significant privacy and security concerns for people in Canada, including the potential to enable mass surveillance and discrimination enabled by systems trained on datasets already imbued with prejudice and bias.

By implementing the following recommendations to amend the *Privacy Act,* the Government of Canada can mitigate serious privacy and security risks currently faced by people in Canada with respect to facial recognition technology:

1. **Acknowledge and explicitly account for the existence, in the *Privacy Act*, of personal information relating to a person's physical or biological characteristics** or biometric information, including facial information;

2. **Adequately safeguard the privacy and security of Canadians** by implementing requirements concerning facial information. These requirements should provide:

    a. Limitations on the collection, use, and disclosure of such information, requiring notice and either consent or explicit legislative permission;

    b. Requirements to minimize information collection; and

    c. More expansive security safeguard requirements.

3. **Align the *Privacy Act* with the requirements of the Directive on Automated Decision-Making.**[2] This alignment would dictate more specific terms for use by law enforcement — ensuring public notice, bias testing, employee training, security risk assessments, and the need for a human to make a final decision in the case of high-impact decisions. These requirements should be expanded to provide for adequate and meaningful consultation before the deployment of this technology.

4. **Implement a federal moratorium on new and expanded uses of automated facial recognition and the disclosure of facial information, until:**

    a. The framework described in this submission has been developed in consultation with Canadians, as well as with government institutions and public servants in relevant government departments; and

    b. More research is done on the disproportionate impacts, or potential for disproportionate impact, on members of particular demographic groups, particular to the realities and populations in Canada.

This would enable legislators to develop a comprehensive and effective policy regulating the development as well as both current and future usage of facial recognition technology by federal institutions. With respect to the responsible governance of facial recognition technology, the *Privacy Act* has significant gaps and weaknesses that, if addressed, will:

1. Better **respect** the privacy rights of people in Canada,

2. Provide stronger **accountability** mechanisms that facilitate and improve the public's trust in federal institutions, and

3. Enhance the **adaptability** of federal institutions' in the face of technological change.

Introduction

The Significance of Facial Information

In 2019, Michigan State Police ran grainy store surveillance footage against the state's facial recognition database in attempts to identify a shoplifter.[3] Images from the store's surveillance footage showed a man dressed in black wearing a red baseball cap, estimated to have stolen $3,800 worth of watches in 2018 from a luxury goods store.

Then in 2020, Robert Julian-Borchak Williams pulled into his driveway after a day at the office. The Detroit Police Department pulled in behind him, blocking him in. They handcuffed him on his front lawn, in front of his distressed wife and two children. The police didn't explain why, exactly, they were arresting him and told his wife to "Google it" when she asked where they were taking him. Williams was held in detention for 30 hours, breaking his four-year record of perfect work attendance on the day before his 42nd birthday.

Williams was arrested because the police relied on facial recognition technology (FRT). Michigan State Police — using the services of the law enforcement software company DataWorks Plus — compared the blurry surveillance footage to the state's mugshot and driver's licence databases containing millions of images. Williams' photo appeared as one of the six closest matches to the suspected thief. An external consultant, hired by the luxury goods store to investigate the theft, simply looked at the six photos and identified Williams as the suspect. Neither the consulting firm nor the police sought any other evidence that Williams, a Black man, had committed the crime.

The investigators — and the facial recognition software — got it wrong. Two weeks after his arrest, the prosecutor in Williams' case moved to dismiss the charges against him. Detroit police accepted the prosecutor's decision, with the caveat that Williams could be charged again if the eyewitness who saw the theft identifies William as the suspect in the future. Williams was perhaps the first person in the U.S. to be wrongfully identified (and arrested) because of government reliance on facial recognition technology, and he most certainly is not the last.

Facial recognition technology, fuelled by ever-larger databases of images and ever more-powerful computer processes and distributed networks, is more powerful — and more pervasive — than ever. During protests over the tragic death of Freddie Gray, Baltimore police scanned social media photos against a photo database to identify and arrest protestors in real-time.[4] China is using facial information to identify jaywalkers and track minority groups such as Uyghur Muslims.[5]

The use of facial recognition technology with detrimental impact on the lives of individuals — particularly vulnerable and minority populations — is not new and is also happening in Canada. Federal institutions as defined by the *Privacy Act*, including the Royal Canadian Mounted Police (RCMP), Canada Border Services Agency as well as Immigration, Refugees and Citizenship Canada, are using FRT software.[6, 7] Several police forces across Canada were also using Clearview AI's FRT software that collects and analyzes every face available on the Internet until Canada's privacy commissioners began investigating use of the company's software in 2020.[8] That investigation found that Clearview AI had collected "highly sensitive biometric information" and engaged in the "indiscriminate scraping and processing" of facial images, subjecting all members of Canadian society to continual mass surveillance.[9] In an increasingly digitized world, use of such automated decision-making software continues to impact the privacy, security and fundamental freedoms of individuals in Canada, including vulnerable populations such as seniors, women, children, and racial and sexual minorities.

Automated decision-making software involving our facial information also relates to issues pertaining to society-at-large. Brenda McPhail, Director of the Privacy, Technology, and Surveillance Project at the Canadian Civil Liberties Association, poignantly questioned the kind of society that Canadians may face without substantial checks on the use and expansion of automated facial recognition: **"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?"**[10] The prospect of a society far-removed from any real autonomy over our personal and private information, including the consistent use of our facial information for profiling, is a somber reality that Canadians already face.

In this submission, the Cybersecure Policy Exchange at Ryerson University and the Centre for Media, Technology and Democracy at McGill University offer four recommendations to inform amendments to the *Privacy Act*. This work is based on the prior research of our organizations, a literature review, and a roundtable discussion hosted by our organizations in November 2020 with 30 expert stakeholders and government officials.

Defining Facial Recognition Technology

Facial recognition technology refers to software that uses computer pattern recognition to find commonalities in images depicting human faces. FRT can be used for identification, authentication, verification, or categorization of a person.

Facial recognition can be used in real-time or on still images, such as mugshots. *After-the-fact* FRT relies on static image recognition, in which existing photos are scanned into systems that match against existing photo databases. *Real-time or live* FRT relies on software that consistently monitors video footage, and looks for a positive match against an image or image set. Real-time or live facial recognition essentially resembles live surveillance but with an increased capacity to instantaneously identify those being recorded, and can result in police approaching or apprehending the identified individuals.[11]

Key Problems in Need of Solutions

In light of such technological advancements, we have identified three key problems in the *Privacy Act's* current approach regarding facial information. **First,** the *Privacy Act* fails to explicitly acknowledge that biometric and facial information are subsets of personal information. As we describe below, facial information is extremely sensitive with a high potential for abuse, rendering this biometric category deserving of specific acknowledgement and protection in the *Privacy Act*.

Secondly, the *Privacy Act* inadequately guards against the significant risks and harms associated with the collection, use, and disclosure of biometric information, such as our facial information. The Department of Justice is currently faced with the timely and critical opportunity to proactively set out requirements for federal institutions before these harms occur, rather than burdening Canada's court systems with unnecessary and preventable legal cases after damage has been caused.

Thirdly, the *Privacy Act* currently leaves Canadians in the dark about how, when, and why federal institutions collect our facial information, disclose it, and use it for identification or profiling in the context of algorithmic decision-making. It is largely only through news reports that Canadians have learned that the Department of National Defence,[12] the RCMP,[13] and CSIS,[14] among others, have used or are using automated facial recognition. Other uses by other federal departments and institutions may, in the absence of a comprehensive review, be continuing or planned, without public notice or accountability. There is also a growing body of legal cases involving challenges to the disclosure by a federal institution of personal information, and particularly facial information depicted in photographs,[15] demonstrating a growing need for clarity in the *Privacy Act* concerning this highly sensitive type of information.

The *Privacy Act* therefore has significant gaps and weaknesses that, if addressed sooner rather than later, will be critical steps to achieving the three pillars set out for this public consultation:

1. Better **respect** the privacy rights of people in Canada,

2. Provide stronger **accountability** mechanisms that facilitate and improve the public's trust in federal institutions, and

3. Enhance the **adaptability** of federal institutions in the face of technological change.

By implementing the following recommendations to amend the *Privacy Act*, the Minister of Justice and Treasury Board of Canada Secretariat will mitigate serious privacy and security risks currently faced by people in Canada stemming from the under-protection of biometric and facial information.

Recommendation:

Acknowledge the Existence of Biometric and Facial Information

01

Recommendation

We recommend that the *Privacy Act* be amended to **explicitly acknowledge and account for** the existence of personal information relating to a person's **physical or biological characteristics or biometric information**, including **facial information.**

Description

The *Privacy Act* currently does not differentiate biometric information from other types of personal information in its treatment or protections. We note that the Government's consultation discussion paper indicated that it is currently not considering specifying categories of personal information to which special rules would apply, as other jurisdictions like the European Union and several US states have done.

Our recommendation aligns with that of the Office of the Privacy Commissioner of Canada, which has recommended that the *Privacy Act* be amended to explicitly regulate all biometric information use, collection, and disclosure.[16] The term facial information could also be circumscribed (e.g., referring to photos or videos) in the *Privacy Act* if deemed appropriate, as it is in New Zealand's recently enacted privacy law.[17]

Justification

Biometric information is one of the most sensitive types of personal information. Biometric information is bodily information unique to each individual and is an extension of the body. The Supreme Court of Canada has ruled that any invasion of one's body is the "ultimate invasion of personal dignity and privacy."[18] This is because "Canadians think of their bodies as the outward manifestation of themselves. It is considered to be uniquely important and uniquely theirs. Any invasion of the body is an invasion of the particular person."[19]

The Supreme Court has held that the state's collection of bodily information without a person's consent is a serious violation of one's body, ultimately compromising the core values of dignity, integrity and autonomy protected under sections 7 and 8 of the *Canadian Charter of Rights and Freedoms* (the "*Charter*").[20] The mere collection of biometric information by federal institutions may therefore constitute interference with a person's right to life, liberty, and security of the person. Collection may also constitute an unreasonable search and seizure by the state in the absence of reasonable limits on these rights prescribed in a law, such as the *Privacy Act*, that can be demonstrably justified in a free and democratic society.[21]

The failure to explicitly account for biometric and facial information also leaves Canadians vulnerable to other significant *Charter* harms that must be imminently addressed. Use of facial information for profiling can have a chilling effect on people's willingness to participate in essential elements of a free and democratic society, such as engaging in free expression or political participation as protected under section 2 of the *Charter*.[22] This is particularly true when facial information is used for live identification and profiling: it has long been understood that people behave differently and in more conforming ways when they are being watched.[23] Canadians should not expect to be part of a perpetual police line-up when they walk on the streets.

Moreover, research from other jurisdictions has found that the accuracy of automated decision-making such as FRT varies across gender, race, and age, resulting in higher rates of inaccuracy particularly for people of colour and women.[24] In a 2019 study examining the accuracy of 189 FRT algorithms, the U.S. National Institute of Standards and Technology found that many of these algorithms were 10 to 100 times more likely to inaccurately identify Black or East Asian people in comparison to white people.[25] The study also found higher inaccuracy rates when identifying women, seniors and children. The use of facial information for identification therefore exacerbates existing inequalities in Canadian society and increases opportunities for discrimination on the basis of one's facial characteristics, ultimately depriving Canadians of their privacy, dignity, and autonomy.[26]

Federal law already provides special treatment for certain forms of information. For example, the Criminal Code requires a warrant for law enforcement's collection of bodily substances for the purposes of DNA analysis, which is a type of biometric information. The *Privacy Act* allows federal institutions in Canada to create databases or "banks" of information containing Canadians' personal information — which have implicitly been deemed more sensitive and in need of protection not with the individual's privacy rights in mind, but instead in the interest generally of managerial efficiency.[27] There are no such protections in place for facial information, the collection of which can be performed without the knowledge of the subject much more readily than genetic material, at a much larger scale and in real-time using live video.

As ruled by the Supreme Court, "[i]nvasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject."[28] Courts in Canada have already begun rendering decisions on the *Privacy Act* regarding the use, collection, and particularly the disclosure of facial information.[29] By explicitly accounting for and protecting facial information, the *Privacy Act* will proactively prevent privacy violations and other harms from occurring involving one of the most sensitive types of personal information that currently remains unacknowledged and under-protected in the *Privacy Act*.

Recommendation:

Adequately Protect Facial Information

02

Recommendation

We recommend that the *Privacy Act* be amended to include **specific requirements for the collection, use, or disclosure of facial information,** developed in consultation with Canadians. This should include, at minimum, requirements for: a) limitations for collection, use, and disclosure, b) information minimization, and c) information security requirements.

Description and Justification

A) Limitations for the Collection, Use and Disclosure

We recommend that the *Privacy Act* be amended to require a presumption against the collection, use, and disclosure of facial information by federal institutions for the purpose of uniquely identifying a person, unless an individual has been given notice and either provided valid consent or there exists explicit legislative permission allowing otherwise.

Such legislative permission already exists, for example, in the *Identification of Criminals Act*, which allows for photographing of those in lawful custody but only for indictable or dual procedure offences,[30] as well as the *Immigration and Refugee Protection Act*, which authorizes the collection of photographs from foreign nationals applying for temporary and permanent resident status.[31] Canadian passport regulations also allow for an applicant's photograph to be converted into a biometric template for the purpose of verifying the applicant's identity and entitlement.[32]

Of serious concern is the use or disclosure of biometric information other than for the lawful purposes for which they were collected.[33] The *Privacy Act* needs to guard against improper and expansive disclosure of our biometric and facial information by federal institutions to other bodies, foreign institutions or non-governmental third parties. The Department of Justice is currently faced with the timely and critical opportunity to proactively set out specific requirements for federal institutions before harms arise, rather than burdening Canada's court systems with unnecessary and preventable legal cases after damage has been caused by improper disclosure of our facial information.

B) Information Minimization

As is already being contemplated, the *Privacy Act* needs a principled approach requiring federal institutions to limit their collection, use, and disclosure of our personal information a) in order to achieve a specific purpose and b) that is reasonably required to achieve that purpose.

Information minimization is particularly critical when it comes to the collection of facial information by federal institutions. For example, in the case of facial information, it is often possible to minimize the storage of this data to templates or mathematical summaries of the data, rather than storing picture or video files which increase the risk of harm arising from unauthorized or inappropriate data use or matching.[34] The Privacy Commissioner's guidelines on police video surveillance also suggest important limits on collection and retention, that likewise could be supported by amendments to the *Privacy Act*.[35]

C) Security Safeguards and Notifications

Institutions must be required to safeguard the security and privacy of all information, to safeguard against loss, access, use, modification or disclosure, and any other misuse. We support the suggestion in the discussion paper for the addition of a safeguarding principle in the Privacy Act, similar to PIPEDA, and for accompanying Treasury Board Secretariat operational policies.

For sensitive information, like facial information, we would suggest clear requirements around adequate encryption and storage in Canada. These risks are not theoretical. Last year, inadequate safeguards for a facial recognition technology pilot by US Customs and Border Protection disclosed 184,000 images, at least 19 of which ended up on the dark web.[36]

Institutions should also be required to notify the Privacy Commissioner and affected individuals not only for "breaches" but also for any activity for which security safeguards are required (i.e., loss, access, use, modification or disclosure, and any other misuse).[37]

Recommendation:

Provide Adequate and Meaningful Public Consultation on Automated Facial Recognition

03

Recommendation

We recommend that the *Privacy Act* be amended to require not only notice before use but also **adequate and meaningful public consultation regarding automated decision-making**, particularly when a federal institution carries out **unique identification of an individual involving their facial information.**

Description

We support the suggestion in the Government's discussion paper to align the *Privacy Act* with the requirements of the Directive on Automated Decision-Making.[38] There are several important requirements in the Directive that apply to facial recognition technology and support transparency and accountability by federal institutions, including:

- Public notice for the use of such technology on institutions' websites;
- Meaningful explanations to affected individuals of how and why the automated decision was made;
- Testing for unintended data biases before use and processes to monitor outcomes;
- Adequate employee training;
- Security risk assessments; and
- The need for a human to make a final decision when it is likely to have a high impact on the rights, health, well-being, or economic interests of individuals or communities.

We note, however, with some concern the suggestion in the discussion paper that there could be exceptions for law enforcement, which is among the principal users of facial recognition technology in Canada. We would advocate for any such exceptions to be explicitly set out and very narrow in scope to ensure law enforcement's use of highly impactful technology is subject to transparency and accountability. Adding these provisions to the *Privacy Act* would increase compliance with the Directive's provisions, which has been an area of concern for federal institutions, including the RCMP and the Department of National Defence.[39]

On top of such notice and transparency requirements, we would suggest adequate and meaningful consultation with the public before new and expanded uses of automated facial recognition technology. Public consultation can take many forms, such as this consultation currently being undertaken for the *Privacy Act*.

Justification

The current flexible principles-based approach prioritizes organizational efficiency for federal institutions, but Canadians are often left in the dark about how, when, and why these institutions collect, use, and share one of the most sensitive types of information.

Recommendation:

Federal Moratorium Until Responsible Governance in Place

04

Recommendation

Until a responsible governance framework is developed like that outlined above in consultation with Canadians, a **federal moratorium on current, new, and expanded uses of automated facial recognition and the disclosure of facial information** should be put in place.

A moratorium is also appropriate until there is more research on FRT's disproportionate impacts, or potential for disproportionate impacts, on members of particular demographic groups, particular to the populations and realities faced by these demographic groups in Canada. Publicly accessible studies are needed that audit the systematic biases and discriminatory impacts of facial recognition software, building on existing expertise but tailored to the Canadian context in terms of factors such as demographics and legal context.[40] More research is also needed, as it has occurred in jurisdictions such as the U.S., which examines Canadians' level of trust in FRT dependent on use case or context, and how this trust varies across various demographic populations in Canada.[41]

A temporary moratorium would enable legislators to develop a comprehensive and effective policy regulating the development as well as both current and future usage of facial recognition technology by federal institutions.

There is precedent for moratoria in the Canadian context involving activity that involves significant safety risks to the public or the long-term well-being of a particular subset of people in Canada, as is the case in the current context. In 1967, a 5-year moratorium was implemented for most uses of the death penalty in Canada, ultimately leading to its abolishment in 1973.[42]

Jurisdictions around the world have moved to explicitly regulate or ban the collection of facial information and/or the use of facial recognition technology, including more than a dozen municipalities across the United States.[43] Montreal's city council is considering the same.[44] It is Canada's best interest for the federal government to lead the way on a national approach that other jurisdictions can model.

Changes to the *Privacy Act* are urgently needed with respect to the collection, use, and disclosure of some of our most sensitive personal information — our faces. These changes are necessary to better respect the privacy and fundamental rights of people in Canada, to provide stronger accountability mechanisms and to maintain trust in federal institutions as they embrace emerging technology that represents significant new risks.

References

[1] Cybersecure Policy Exchange & Tech Informed Policy. (2021). *Facial Recognition Technology Policy Roundtable: What We Heard.* Cybersecure Policy Exchange and Tech Informed Policy. https://www.cybersecurepolicy.ca/reports

[2] Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making* (2019), online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[3] Hill, K. (2020, June 24). Wrongfully Accused by an Algorithm. *The New York Times.* https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[4] ACLU. (2016). *Case Study: Baltimore County PD: Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots.* ACLU. https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf

[5] Tao, L. (2018, March 27). Jaywalkers under surveillance in Shenzhen soon to be punished via text messages. *South China Morning Post.* https://www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text

[6] Office of the Privacy Commissioner of Canada. (2017, March 16). *Your privacy at airports and borders*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/your-privacy-at-airports-and-borders/, see "Biometrics and facial recognition"

[7] Office of the Privacy Commissioner of Canada. (2013). *Automated Facial Recognition in the Public and Private Sectors.* Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/media/1765/fr_201303_e.pdf

[8] Office of the Privacy Commissioner of Canada. (2021, February 3). Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/

[9] 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, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[10] McPhail, B., Israel, T., Schroeder, J., & Lucht, B. (2021, February 3). *Facial Recognition: A pathway or threat to our future.* https://youtu.be/na3limdly6g at 75:59

[11] Schuppe, J. (2018, July 30). Facial recognition gives police a powerful new tracking tool. It's also raising alarms. *NBC News.* https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936

[12] Gillis, W., Boutilier, A., & Allen, K. (2020, February 28). MPs call for parliamentary investigation as Canadian military and police forces confirm they've tried facial-recognition technology. *Toronto Star.* https://www.thestar.com/politics/federal/2020/02/28/mps-call-for-parliamentary-investigation-as-military-and-police-forces-confirm-theyve-tried-facial-recognition-technology.html

[13] Carney, B. (2020, March 10). Despite Denials, RCMP Used Facial Recognition Program for 18 Years. *The Tyee.* https://thetyee.ca/News/2020/03/10/RCMP-Admits-To-Using-Clearview-AI-Technology/

[14] Pearson, J. (2017, June 20). Canada's Spies, Police, and Border Agents Are Quietly Coordinating on Biometrics. *Vice.* https://www.vice.com/en/article/new5q8/canadas-spies-police-and-border-agents-are-quietly-coordinating-on-biometrics

[15] See e.g., R. v. Truong, 2017 BCSC 736 (CanLII), <https://canlii.ca/t/h3lfh>, Privacy Act (Can.) (Re), 2001 SCC 89 (CanLII), [2001] 3 SCR 905, <https://canlii.ca/t/51w3>, affirming [2000] 3 F.C. 82 (C.A.), Canada (Minister of Public Safety and Emergency Preparedness) v. Kahlon, 2005 FC 1000 (CanLII), [2006] 3 FCR 493, <https://canlii.ca/t/1ldlc>, U.S.A. v. Lucero-Echegoyen, 2011 BCSC 1028 (CanLII), <https://canlii.ca/t/fmjf0>, R. v. Baldovi et al, 2016 MBQB 221 (CanLII), <https://canlii.ca/t/gvvbd>, R. v Flintroy, 2018 BCSC 1692 (CanLII), <http://canlii.ca/t/hzn2r>

[16] Office of the Privacy Commissioner of Canada. (2008, April 29). Proposed Immediate Changes to the Privacy Act. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2008/parl_080429_02/#rec7

[17] Privacy Act 2020, s. 109c (New Zealand).

[18] R. v. Stillman, 1997 CanLII 384 (SCC), [1997] 1 SCR 607, http://canlii.ca/t/1fr32, para 87

[19] R. v. Stillman, 1997 CanLII 384 (SCC), [1997] 1 SCR 607, http://canlii.ca/t/1fr32, para 87

[20] The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11, <https://canlii.ca/t/ldsx> (*the Charter*); R. v. Plant, 1993 CanLII 70 (SCC), [1993] 3 SCR 281 at para 93, <http://canlii.ca/t/1fs0w>; Blencoe v. British Columbia (Human Rights Commission), 2000 SCC 44 (CanLII), [2000] 2 SCR 307, <https://canlii.ca/t/525t> at para 50, citing *R. v. Morgentaler,* 1988 CanLII 90 (SCC) at p. 166

[21] R. v. Oakes, 1986 CanLII 46 (SCC), [1986] 1 SCR 103, <https://canlii.ca/t/1ftv6>

[22] The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11, <https://canlii.ca/t/ldsx> (*the Charter*)

[23] Steinmetz, J. (2020, February 27). How cameras in public spaces might change how we think. *The Conversation*. http://theconversation.com/how-cameras-in-public-spaces-might-change-how-we-think-132537

[24] Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Conference on Fairness, Accountability and Transparency.* https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf

[25] Bushwick, S. (2019, December 27). How NIST Tested Facial Recognition Algorithms for Racial Bias. *The Scientific American*. https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/

[26] Reference re Genetic Non Discrimination Act, 2020 SCC 17 (CanLII), <https://canlii.ca/t/j8l59> at headnote and paras 82-90.

[27] Becker, M. (2019). Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics and Information Technology, 21(4), 307–317. https://doi.org/10.1007/s10676-019-09508-z

[28] R. v. Dyment, 1988 CanLII 10 (SCC), [1988] 2 SCR 417, <http://canlii.ca/t/1ftc6>, para 23

[29] See e.g., R. v. Truong, 2017 BCSC 736 (CanLII), <https://canlii.ca/t/h3lfh>, Privacy Act (Can.) (Re), 2001 SCC 89 (CanLII), [2001] 3 SCR 905, <https://canlii.ca/t/51w3>, affirming [2000] 3 F.C. 82 (C.A.), Canada (Minister of Public Safety and Emergency Preparedness) v. Kahlon, 2005 FC 1000 (CanLII), [2006] 3 FCR 493, <https://canlii.ca/t/1ldlc>, U.S.A. v. Lucero-Echegoyen, 2011 BCSC 1028 (CanLII), <https://canlii.ca/t/fmjf0>, R. v. Baldovi et al, 2016 MBQB 221 (CanLII), <https://canlii.ca/t/gvvbd>, R. v Flintroy, 2018 BCSC 1692 (CanLII), <http://canlii.ca/t/hzn2r>

[30] Identification of Criminals Act, RSC 1985, c I-1, <https://canlii.ca/t/544lz> at s. 2.

[31] Immigration and Refugee Protection Act, SC 2001, c 27, <https://canlii.ca/t/53z6t> at s. 16

[32] Canadian Passport Order, SI/81-86, <https://canlii.ca/t/53msk> at s. 8.1

[33] R. v. Dyment, 1988 CanLII 10 (SCC), [1988] 2 SCR 417, <http://canlii.ca/t/1ftc6>

[34] Office of the Privacy Commissioner of Canada (2011, February.) 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/

[35] Office of the Privacy Commissioner of Canada. (2006, March). Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/vs_060301/

[36] Sands, G. (2020, September 23). Border institution did 'not adequately safeguard' facial recognition data, watchdog finds. *CNN*. https://www.cnn.com/2020/09/23/politics/customs-border-protection-data-breach-watchdog-report/index.html

[37] Privacy Act 2020, Part 2: Information privacy principles, Principle 6 (Storage and security of personal information) (New Zealand).

[38] Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making* (2019), online: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[39] Cardoso, T., & Curry, B. (2021, February 7). National Defence skirted federal rules in using artificial intelligence, privacy commissioner says. *Globe and Mail*. https://www.theglobeandmail.com/canada/article-national-defence-skirted-federal-rules-in-using-artificial/

[40] Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Conference on Fairness, Accountability and Transparency.* https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf

[41] Vanian, J. (2019, September 5). Most Americans Distrust Companies Using Facial Recognition Technology. *Fortune*. https://fortune.com/2019/09/05/pew-research-facial-recognition/

[42] Correctional Service of Canada Government of Canada. (2007, July 11). *50 Years of Human Rights Developments in Federal Corrections*. https://www.csc-scc.gc.ca/text/pblct/rht-drt/08-eng.shtml

[43] Cybersecure Policy Exchange & Tech Informed Policy. (2021). *Facial Recognition Technology Policy Roundtable: What We Heard*. Cybersecure Policy Exchange and Tech Informed Policy. https://www.cybersecurepolicy.ca/reports

[44] Serebrin, J. (2020, September 18). Montreal should restrict police use of facial recognition technology: councillor. *Global News*. https://globalnews.ca/news/7345106/montreal-police-facial-recognition-technology/