FACIAL RECOGNITION TECHNOLOGY & THE CANADIAN *CHARTER*

SUBMISSION TO THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY, AND ETHICS

David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

Facial Recognition Technology and the Canadian *Charter*

The Artificial Intelligence and Constitutional Rights Working Group is led by Amy Chen, Angela Gu, Annecy Pang, and Adrienne Ralph. The students who generated this report are: Cecilia Kim, Troy Klassen, Rachael Tu, Katy Beeson, Dilan Brar, April Lewtak, Yuliya Mykhaylychenko, Jack Olson, Jamie Peltomaa, Stephanie Rei, Naya Samara, and Jasveen Singh.

For more information, please contact:

David Asper Centre for Constitutional Rights
University of Toronto, Faculty of Law
78 Queen's Park
Toronto, Ontario, M5S 2C5

Amy Chen, Working Group Leader
Email: amyjun.chen@mail.utoronto.ca
Cheryl Milne, Executive Director
Email: cheryl.milne@utoronto.ca
Tal Schreier, Program Coordinator
Email: tal.schreier@utoronto.ca

Table of Contents

About and Acknowledgements

About the David Asper Centre for Constitutional Rights

The David Asper Centre for Constitutional Rights (Asper Centre) is a centre within the University of Toronto, Faculty of Law devoted to advocacy, research, and education in relation to Canadian constitutional rights. The Asper Centre aims to play a vital role in articulating Canada's constitutional vision to the broader world and houses a unique legal clinic that brings together students, faculty, and legal professionals to work on significant constitutional cases. Through the establishment of the Asper Centre, the University of Toronto has joined a small group of international law schools that play an active role in ongoing constitutional debates. It is the only Canadian centre in existence that attempts to bring constitutional law research, policy, advocacy and education together under one roof. The Asper Centre was established through a generous gift to the law school from University of Toronto law alumnus David Asper (LLM '07).

About the Artificial Intelligence and Constitutional Rights Working Group

The Artificial Intelligence and Constitutional Rights Working Group consists of twelve first-year students at the University of Toronto, Faculty of Law, as well as four upper-year student supervisors. Our objective in this submission is to put forward recommendations regarding Canada's approach to regulating the use of facial recognition technologies in the context of law enforcement. In line with our expertise, we seek specifically to highlight the constitutional rights-related aspects of this issue.

Acknowledgements

We are deeply grateful for the input, assistance, and support of the Asper Centre's executive director Cheryl Milne, program coordinator Tal Schreier, and our faculty advisor, Professor Vincent Chiao.

List of Acronyms

AI	Artificial Intelligence
BIPA	*Biometric Information Privacy Act* (Illinois, United States)
CPPA	*Consumer Privacy Protection Act* (Canada)
DPIA	*Data Protection Impact Assessment* (United Kingdom)
FRT	Facial Recognition Technology
ICO	Information Commissioner's Office (United Kingdom)
OIPRD	Office of the Independent Police Review Director
OCPC	Ontario Civilian Police Commission
OPC	Office of the Privacy Commissioner
PIPEDA	*Personal Information Protection and Electronic Documents Act* (Canada)
RCMP	Royal Canadian Mounted Police
REP	Reasonable Expectation of Privacy

Executive Summary

The use of facial recognition technology (FRT) by law enforcement agencies carries both benefits and significant risks. While FRT may improve the efficiency and effectiveness of investigations, improper use of FRT may invade Canadians' privacy or result in wrongful arrests. This submission addresses the constitutional implications of the use of FRT under the *Canadian Charter of Rights and Freedoms* (*Charter*). Different *Charter* sections may work together to protect individuals' **privacy, liberty, and equality** from the negative effects of FRT.

We begin **Part 1** by summarizing and applying the *Charter* framework. We outline how the following *Charter* sections are relevant in the context of FRT, some possible legal arguments that an individual could raise to protect their *Charter* rights, and the difficulties that one may encounter when raising these arguments.

> **Section 8 protects individuals' privacy by prohibiting unreasonable searches.** Establishing a section 8 breach is challenging as FRT generally collects data in public spaces, where one does not expect to have privacy. Establishing that the search was unreasonable is also difficult, as the FRT use may be authorized by a warrant or justified by emergency circumstances.
>
> **Section 15 guarantees a right to equality.** The use of FRT may violate section 15 if it directly or indirectly discriminates against individuals. FRT may contribute to the systemic over-policing and overrepresentation of racialized individuals in the criminal justice system. Discrimination may arise from improperly trained FRT or from improper and biased use by law enforcement.
>
> **Section 9 protects individuals' liberty and equality by prohibiting arbitrary detentions.** Law enforcement may rely on information obtained from FRT to arrest or detain an individual. This detention may be arbitrary if the information produced by the FRT was unreliable or biased.
>
> **Section 7 protects "life, liberty, and security of the person" alongside privacy**. FRT may infringe section 7 if its use leads to an individual's arrest or detention, or if its use breaches an individual's privacy. Establishing a section 7 breach is difficult:

one must prove that the use of FRT is arbitrary, overbroad in its scope, or has a grossly disproportionate negative impact.

Charter rights are subject to reasonable limitations. After an individual successfully argues a *Charter* breach, the state may use **section 1** of the *Charter* to justify the breach by demonstrating that the societal interests of using FRT for effective and efficient policing outweigh the rights of the individual.

We also outline the **limitations of the *Charter*** to lay the foundation for the recommendations that follow. The process of seeking *Charter* protections is complex, difficult, and expensive. These protections would only be triggered in specific circumstances and would only apply retroactively after the harm has already been done. The compensation awarded to the claimant for a successful *Charter* case is often limited. **Hence, more robust legislative protections are required to supplement *Charter* protections and ensure proactive and systemic regulation of FRT.**

In **Part 2** of our submissions, we recommend the following legislative reforms to better protect individuals from the improper or unjustifiable use of FRT.

Recommendation 1: Place a national moratorium on FRT while the federal government puts the appropriate safeguards in place

We recommend a temporary national moratorium on all algorithmic policing technologies until more research is available to determine how these technologies may violate constitutional rights. In the interim, greater safeguards to *Charter* rights should be put in place, as set out in the subsequent recommendations.

Recommendation 2: Fund research on the impact of FRT, especially concerning individuals from historically marginalized backgrounds

We recommend that funding is made available to better research how algorithmic technologies interact with the relevant *Charter* rights. Research on how FRT may disproportionately affect historically marginalized groups would particularly help support arguments about the biased effects of FRT under section 15 and section 9. This research would also inform future policy development and advocacy efforts.

Recommendation 3: Implement a Data Protection Impact Assessment scheme for each law enforcement agency's use of FRT

We recommend that Canada adapts a similar regulatory framework to the Data Protection Impact Assessment (DPIA) scheme in the United Kingdom. This scheme would ensure that the processing of sensitive personal data by law enforcement bodies is fair, based on law, and strictly necessary for a legitimate law enforcement purpose. Further, the framework must ensure that FRT falls in line with best practices of personal data processing, such that each use is recorded, justified, and continually reviewed. Such safeguards would prevent arbitrary uses of FRT, contrary to section 7. It would further ensure that *Charter* rights are only limited in ways that are reasonable and justified under section 1.

Recommendation 4: Improve oversight on law enforcement's use of FRT

Improving oversight mechanisms for the use of technology by law enforcement will improve public accountability and better protect individual rights. To improve transparency, we recommend requiring law enforcement services to publicly disclose what technology they are using, whether the technology is being developed or already in use, how the technology will be used, and how the technology will be evaluated. We also recommend that law enforcement services are internally controlled with clear guidelines and training to improve *Charter* compliance and control the sources of bias arising from FRT. Improving oversight would prevent FRT from being used in ways that are arbitrary, unreasonable, or biased, contrary to each of the *Charter* sections.

Recommendation 5: Increase protection of biometric information in the private sector

Amending private sector data protection laws in conjunction with public sector protections would allow for comprehensive privacy regulation. The proposed *Consumer Privacy Protection Act* (CPPA), which may potentially replace the *Personal Information Protection and Electronic Documents Act* via Bill C-15, is an opportunity to do so. We recommend amending the CPPA to explicitly protect "biometric information" and to mandate individuals' express and informed consent for all data collection, including data collection for research and development.

Part 1: *Charter* Analysis of Facial Recognition Technology

Background

What is Facial Recognition Technology?

Facial recognition technology (FRT) uses algorithms to convert facial images into templates for the purposes of identifying or authenticating individuals. The process for doing so is divided into three steps: (1) detection, or locating the face; (2) creation of a template, or numerically representing the face based on certain features; and (3) authentication or identification, or using the template for comparative purposes.[1]

Authentication, or one-to-one matching, determines whether the person is who they claim to be.[2] To authenticate a person's identity, the FRT will compare the created template against a verified image of that person.[3] If the image is sufficiently similar to the verified image, meaning that the similarities exceed the threshold set by the programmers for authentication, the FRT will produce a match.[4] Identification, or one-to-many matching, answers the broader question of who the pictured person is. To identify an individual, the created template will be compared against all the templates in the technology's database to look for a match.[5] The more closely the template matches templates within the existing data, the more likely the face will be marked as a potential match.[6]

---

[1] Office of the Privacy Commissioner of Canada, "Automated Facial Recognition: In the Public and Private Sectors" (March 2013) at 2, online (pdf): <https://www.priv.gc.ca/media/1765/fr_201303_e.pdf>; United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses" (July 2020) at 5, online (pdf): <https://www.gao.gov/assets/gao-20-522.pdf>.

[2] United States Government Accountability Office, *supra* note 1 at 6.

[3] *Ibid*; European Union Agency for Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement" (November 2019) at 7, online (pdf): <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf>.

[4] European Union Agency for Fundamental Rights, *ibid* at 7.

[5] United States Government Accountability Office, *supra* note 1 at 6.

[6] Law Enforcement Imaging Technology Task Force, "Law Enforcement: Facial Recognition UseCase Catalog" (March 2019) at 3, online (pdf): <https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf>.

FRT is frequently used for identification by law enforcement, with the goal of safeguarding the public and strengthening national security.[7] For instance, Clearview AI is a facial recognition application that claims to scrape approximately three billion photos from a myriad of websites, such as Facebook and YouTube. The front-end of the application allows users to upload a picture of an individual; the back-end converts the image into a template and compares it against existing images within the application's database. If matches are found, the application outputs any public images and associated web pages containing the individual's face — effectively reproducing the individual's digital footprint within a matter of seconds.[8] Prior to terminating its services in Canada, Clearview AI had contracts with various Canadian law enforcement agencies up until July 2020, including the Royal Canadian Mounted Police (RCMP).[9]

Benefits and Risks of FRT

FRT can help law enforcement agencies respond more quickly to new threats and open up new investigative avenues, especially when the threat to an individual or the public is extremely time-sensitive.[10] FRT is demonstrably faster at identifying suspects compared to previous biometric policing tools, such as fingerprinting and DNA collection.[11] It is also less invasive than fingerprinting or DNA collection, as it can be collected from a distance and integrated with existing surveillance systems.[12]

However, FRT also has the potential to cause greater harm than existing police tools due to inaccuracies and biases within their datasets and algorithms. These inaccuracies may compromise the intended purpose of law enforcement using these technologies. For example, errors can result in false negatives, in which the technology does not recognize a match, therefore failing to detect individuals who are suspects. Conversely, false positives,

---

[7] Office of the Privacy Commissioner of Canada, *supra* note 1 at 2, 4, 5.
[8] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times* (18 January 2020), online: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.
[9] Louise Matsakis, "Scraping the Web Is a Powerful Tool. Clearview AI Abused It," *Wired* (25 January 2020), online: <https://www.wired.com/story/clearview-ai-scraping-web/>; Office of the Privacy Commissioner of Canada, News Release, "Clearview AI ceases offering its facial recognition technology in Canada (6 July 2020), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/>.
[10] Office of the Privacy Commissioner of Canada, Investigation News Release, "Cell site simulators used by RCMP not capable of intercepting private communication: Complaint under the Privacy Act (the Act)" (21 September 2017), online:<https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/>.
[11] Sharon Naker & Dov Greenbaum, "Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy" (2017) 23:1 BU J Sci & Tech L 88 at 97.
[12] Monique Mann & Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" (2017) 40:1 UNSWLJ 121.

where a person is incorrectly identified as a match, can result in an innocent person being detained, searched or arrested.[13] While the technology's thresholds can be changed to reduce rates of false positives or false negatives, lowering one comes at the expense of increasing the other.[14] The sensitive nature of the biometric data collected by FRT also means it carries greater risks in causing wrongful arrests and detention. Most concerningly, there is a lack of transparency in exactly how, when, and where FRT is used by law enforcement to identify and charge individuals. The detriments of FRT are more thoroughly canvassed in the following submissions.

Available *Charter* Protections Against Improper Use of FRT

The *Charter* guarantees individuals certain rights and freedoms; it is a powerful legal tool that can be used to address the overreach and abuse of state power.[15] A number of *Charter* sections can combine and overlap to protect individuals' privacy, liberty, and equality from the improper use of FRT by law enforcement. These include:

- **Section 8:** Section 8 is the primary provision in the *Charter* that protects individual's privacy from state intrusion. It does so by prohibiting unreasonable searches.
- **Section 15:** Section 15 is the *Charter* provision that guarantees equality and freedom from discrimination.
- **Section 7:** Section 7 of the *Charter* is the provision that recognizes a right to "life, liberty and security of the person". Section 7 also supplements the privacy protections available in section 8.
- **Section 9:** Section 9 prohibits arbitrary detention. It supplements both section 7's protection of liberty and section 15's guarantee of equality.

Establishing a *Charter* breach is a complex, multi-step process. A *Charter* claimant must first prove that one or more *Charter* sections is violated, with each section requiring unique tests and considerations. Once a violation is established, the state has an opportunity to argue that the violation is "reasonably and demonstrably justified in a free and democratic society", as per **section 1** of the *Charter*. We set out the legal tests, arguments, and considerations for each *Charter* section below.

---

[13] *Ibid*.

[14] European Union Agency for Fundamental Rights, *supra* note 3 at 9.

[15] *Canadian Charter of Rights and Freedom,* ss 7, 8, 9, 15, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, online: <https://canlii.ca/t/ldsx> [*Charter*].

Section 8: FRT as an Unreasonable Search

"Everyone has the right to be secure against unreasonable search or seizure".

Section 8 protects individuals' privacy by prohibiting unreasonable searches. The purpose of section 8 is to protect individuals from unjustified state intrusions on their reasonable privacy interests, allowing them to carve out space in their lives.[16] While evolving technologies make it easier for state agents to gather and disseminate information, we continue to expect that our personal information will remain private.[17]

It may be difficult to successfully argue that the use of FRT breaches section 8, which in turn limits the effectiveness of this *Charter* protection. The finding of a violation of privacy rights by FRT in Canada is much more complex and difficult than in other jurisdictions. For instance, courts in the United Kingdom *assume* that there is an unjustified breach of privacy arising from the use of FRT unless its use was defined by clear guidance.[18] In Canada, courts must go through a complex and discretionary analysis in order to determine whether a section 8 infringement has occurred.

Step 1: Establishing a "Search" and Reasonable Expectation of Privacy

The first step to establishing a section 8 infringement is establishing that a "search" occurred. An inspection is only considered a "search" if one has a **"Reasonable Expectation of Privacy"** in the subject matter being searched. A "Reasonable Expectation of Privacy" is the degree of privacy that a reasonable person would expect to have in a certain context or location (both physical and digital).

Establishing a "Reasonable Expectation of Privacy" is difficult in the context of FRT, as FRT generally collects publicly available information. We have a limited expectation of privacy in public spaces.[19] Consider a situation in which a law enforcement agency uploads an image pulled from security footage to a facial recognition database. The agency then uses this image to search its FRT database to locate a match, thus allowing the agency to identify and charge a suspect. The agency then goes further to upload the security camera image onto Clearview AI, allowing the officer to view the biographical and personal information originating from the suspect's public Facebook

---

[16] *R v Jarvis*, 2019 SCC 10 [*Jarvis*].
[17] *Ibid* at para 63.
[18] *R (Bridges) v South Wales Police*, [2020] EWCA Civ 1058.
[19] *Hunter v Southam*, [1984] 2 SCR 145, 1984 CanLII 33 (SCC) at para 159 [*Hunter*]; *Jarvis*, *supra* note 16 at para 66 [*Jarvis*].

profile. The animating question would be whether a *Charter* claimant in this scenario has a "Reasonable Expectation of Privacy" in their image being captured by security cameras in a public place, and whether they have a "Reasonable Expectation of Privacy" in their public social media profile. The difficulty lies in the fact that one generally does not expect privacy when existing in public spaces, or expect one's public social media profile to remain private.

In the above scenario, a *Charter* claimant may argue that they have a "Reasonable Expectation of Privacy" in their biometric data, even in public spaces. A key to the "Reasonable Expectation of Privacy" analysis is that consent to disclosure of information for one purpose does not equate to consent to the use of that same information for another purpose.[20] For instance, while an individual may consent to having their image captured by security cameras in public, they have not necessarily consented to law enforcement using biometric information from that image for identification and investigative purposes.[21] Biometrics, particularly facial recognition data scans, are associated with higher risks when it comes to wrongful disclosure, misuse, or theft of data. One's biometric data is individualized, unalterable, and useful for identification, even if one does not want or expect it to be used as such.[22] Although law enforcement bodies have previously used biometrics to identify individuals, such data is generally not collected covertly without consent in public spaces through surveillance.

Likewise, a *Charter* claimant can argue that they have a "Reasonable Expectation of Privacy" in their public social media profile. While one might expect that the public would view the pictures on one's public social media profiles,[23] one would not consent to having biometric information from those pictures scraped onto a database and matched with surveillance footage. Given that the internet has exponentially increased the information stored about users, section 8 protects individuals' anonymity by ensuring that the link between one's information and one's identity remains private.[24] In this example, Clearview

---

[20] *R v Quesnelle,* 2014 SCC 46 at para 37, 29.
[21] Office of the Privacy Commissioner of Canada, *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* (2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>
[22] Office of the Privacy Commissioner of Canada, *Guidelines for identification and authentication*, June 2016 update (2016), online: <https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth_061013/>
[23] Gerald Chan, "Text Message Privacy: Who Else is Reading This?" (2019) 88 Osgoode's SCLR 75.
[24] *R v Spencer,* 2014 SCC 43 at para 46.

AI allows law enforcement to match the *Charter* claimant's picture to their specific social media profile, therefore revealing their identity and violating their anonymity.

As we discuss in **Recommendation 5: Increase Protection of Biometric Information**, implementing robust protections for biometric data in the private sector could set a significant precedent. Although "Reasonable Expectation of Privacy" is a significant barrier to seeking section 8 protections, judicial analysis of FRT could possibly be swayed by the findings of the Office of the Privacy Commissioner (OPC) against Clearview AI. The OPC oversees compliance with the *Privacy Act*, which governs how the federal government collects personal information. The OPC also oversees compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which regulates how the private sector collects personal information. The OPC concluded in an investigation under the PIPEDA that Clearview AI processed sensitive biometric information "for purposes that a reasonable person would *not* consider appropriate in the circumstances."[25] Even though Clearview AI collected "publicly accessible" information, the OPC found that individuals who post their images online have no "reasonable expectation" that companies like Clearview AI would collect, use, or disclose their images for the purposes of identification without express consent. The test under the PIPEDA is different from that under section 8 of the *Charter*; however, this demonstrates that there can be a "Reasonable Expectation of Privacy" regarding publicly accessible online information.

Overall, the "Reasonable Expectation of Privacy" analysis looks at the entire context, such as the type of FRT technology being used, how it is used for police investigations, and the degree of control an individual has over how, when, and to whom their information is disclosed.[26] In line with **Recommendation 2: Fund Research** and **Recommendation 4: Improve Oversight**, greater transparency in the type of FRT used by law enforcement would allow us to better predict how this context-specific analysis will be conducted.

---

[25] Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc, supra* note 21 *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* (2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>; *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5.

[26] *R v MS*, 2019 ONCJ 670 at para 61; *R v Marakah*, 2017 SCC 59 [*Marakah*]; *R v Ahmad*, 2020 SCC 11 at para 36.

Step 2: Establishing that the Search was "Unreasonable"

After establishing that a "search" occurred, the second step to establishing a section 8 violation is proving that the search was unreasonable.[27] Courts generally look at whether the search was conducted with prior judicial authorization (i.e. a warrant) and whether there are reasonable and probable grounds for the search.[28] If there was no warrant, law enforcement may nonetheless justify the search if it was conducted under "exigent circumstances."[29] An exigent circumstance must be one which urgently calls for immediate police action to preserve evidence, officer safety, or public safety.[30] In line with **Recommendation 4: Improve Oversight,** clear internal guidelines on obtaining prior judicial authorizations will help avoid section 8 violations.

To use the example of Clearview AI, no law enforcement body in Canada has ever obtained a warrant for its use. Nonetheless, the RCMP has emphasized that its warrantless use of Clearview AI is justified under exigent circumstances. The RCMP stated that this technology was needed for immediate victim identification for child sexual exploitation investigations because the Internet has changed the way these offenses were being committed.[31] Although urgent circumstances may sometimes justify the use of FRT, this broad exception to section 8 protections is another hurdle to individuals seeking to establish a *Charter* breach.

Summary: Section 8 protects individuals' privacy by prohibiting unreasonable searches. Establishing a section 8 breach is challenging as FRT generally collects data in public spaces, where one does not expect to have privacy. A *Charter* claimant would have to creatively argue that the FRT is collecting biometric data without consent and intruding on their anonymity. Establishing that the search was unreasonable is also difficult, as the FRT use may be authorized by a warrant or justified by emergency circumstances. Greater oversight over law enforcement (**Recommendation 4**) and protection of biometric data in the private sector (**Recommendation 5**) can proactively prevent intrusions into section 8 or set significant precedents.

---

[27] *R v Collins*, [1987] 1 SCR 265, 1987 CanLII 84 (SCC).
[28] *Hunter, supra* note 19 at 146.
[29] *R v Paterson*, 2017 SCC 15 at paras 32-33.
[30] *Ibid.*
[31] Royal Canadian Mounted Police, News Release, "RCMP Use of Facial Recognition Technology" (27 February 2020), online: <https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-use-facial-recognition-technology>.

Section 15: FRT and Potential Discriminatory Impacts on Equality

"Every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability."

Section 15 guarantees a right to equality and freedom from discrimination. Discrimination is defined as *differential treatment* that *perpetuates a historic/systemic disadvantage*. Section 15 protects against direct discrimination, where a group is deliberately targeted in a discriminatory manner. Section 15 also protects against indirect systemic discrimination, where laws or state actions appear neutral but in fact are discriminatory in effect.[32]

Courts have recognized that the state could violate section 15 by perpetuating the systemic over-representation of racialized individuals in the criminal justice system. Racialized individuals, particularly Black and Indigenous individuals, are targeted, policed, and incarcerated at a disproportionate rate. This discriminatory over-representation stems from a long history of colonialism and racism. Courts will look at whether the *effects* of the state action perpetuate over-representation, including any intersectional effects on individuals that belong to more than one marginalized group. For example, in *R v Sharma*, the court found that a seemingly-neutral law violated section 15 because it exacerbated the over-incarceration of Indigenous women and the disadvantages they face on the basis of their race and gender.[33] The jurisprudence demonstrates that courts consider anti-Black racism, anti-Indigenous racism, and systemic overrepresentation as one of the most serious problems within our justice system.[34] FRT may therefore violate section 15 by indirectly or directly targeting racialized individuals and perpetuating this problem.

FRT algorithms may cause discriminatory effects because of inherent data flaws. FRT may be improperly trained on datasets that are not reflective of the general population; these datasets may contain proportionally less and lower quality images of racialized individuals.[35] A comprehensive study conducted by the U.S. National Institute of Standards and Technology found that ethnic subjects were more likely to be matched to a

---

[32] *Fraser v Canada (Attorney General)*, 2020 SCC 28 [*Fraser*].
[33] *R v Sharma,* 2020 ONCA 478 at para 101.
[34] *R v Sharma,* 2020 ONCA 478 at 130; See also *R v Morris,* 2021 ONCA 680 at para 1, 86; *R v Le,* 2019 SCC 34.
[35] Jacqueline G Cavazos et al, "Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?" (January 2021) 3:1 *IEEE Transactions on Biometrics, Behavior and Identity Science* 101 at 105.

suspect's photo.[36] Other studies found that there were higher false positives among women over men, for those with lighter skin compared to those with darker skin, and for the elderly and children. The inaccuracies are more pronounced for individuals belonging to more than one marginalized group, such as racialized women.[37] Even if the FRT algorithm appears to be neutral, these performance asymmetries have the effect of disproportionately targeting racialized individuals and perpetuating systemic over-policing.

Law enforcement may also be using FRT in a discriminatory manner. The use of FRT can be susceptible to two types of bias: institutional/unconscious bias and automation bias. Institutional/unconscious bias arises from police policies and misconduct that have a disproportionate effect, such as increasing use of FRT surveillance in neighborhoods that have more racialized individuals. Automation bias is the tendency "to rely on the judgments of automated decisions as superior to their own," even when one has reason to believe that the technology is flawed or biased.[38] The fact that training has not been shown to effectively address automation bias underscores the importance of avoiding complete reliance on FRT.[39] These two types of bias combine to perpetuate the discrimination of racialized individuals in the criminal justice system. As we address in **Recommendation 4: Improving Oversight**, greater external and internal controls in how law enforcement chooses and uses technology is needed to minimize these two types of biases.

Even if FRT might not breach the *Charter,* the court may still find that the technology does not align with best practices. In the case *Ewert v Canada*, a Métis inmate challenged the use of algorithmic inmate risk assessment tools by the Correctional Service of Canada. He argued that the risk assessment tools were developed and tested on predominantly non-Indigenous populations, and thus less accurate when applied to Indigenous offenders. The Supreme Court of Canada found that although the risk assessment tools were less accurate and susceptible to cultural bias, there was insufficient evidence to show that the tools created a differential impact on Indigenous offenders compared to non-Indigenous offenders under s. 15. The evidence was sufficient, however, to establish that the use of the tools fell short of the obligations under the *Corrections and Conditional Release Act* by "disregarding the possibility that these tools are systematically disadvantaging Indigenous

---

[36] Patrick Grother, Mei Ngan and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (December 2019), U.S. Department of Commerce, National Institute of Standards and Technology, online: <https://doi.org/10.6028/NIST.IR.8280>.

[37] *Ibid;* Cavazos et al., *supra* note 35; Naker & Greenbaum, *supra* note 11.

[38]Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020) at 154, online (pdf): <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>

[39] *Ibid* at 136-137, 172.

offenders and by failing to take any action to ensure that they generate accurate information."[40] This demonstrates that courts could still recognize the potentially discriminatory effects of FRT outside of the *Charter* framework. *Ewert v Canada* will also be discussed below for **section 7** of the *Charter*.

There is currently insufficient evidence on how the data flaws in FRT arise, and how these data flaws may affect racialized individuals. Current research demonstrates that even a developer is unable to trace how differential results are produced by the algorithm.[41] Like with *Ewert v Canada,* courts may not have the evidence available to conduct a section 15 analysis. However, even if there is no direct evidence of the discriminatory effects of certain state actions, courts are entitled to make limited inferences based on the link between systemic racism, over-policing and the overrepresentation of racialized individuals in the criminal justice system.[42] In line with **Recommendation 2: Fund Research**, more information is needed on how FRT has been used against racialized individuals and how this may implicate equality rights.

Summary: Section 15 guarantees a right to equality. The use of FRT may violate section 15 if it directly or indirectly discriminates against individuals. In particular, FRT can be discriminatory by disproportionately affecting racialized individuals and perpetuating their systemic overrepresentation in the criminal justice system. Discriminatory treatment may arise from improperly trained FRT algorithms that are less accurate for certain marginalized groups. It may also arise from biased use or overreliance by law enforcement. Greater research (**Recommendation 2**) is needed on how FRT may implicate equality rights and how they may compare to existing law enforcement tactics.

[40] *Ewert v Canada,* 2018 SCC 30 at para. 66 [*Ewert*]*; Corrections and Conditional Release Act,* SC 1992, c 20.
[41] Robertson, Khoo and Song, *supra* note 38 at 129, 136-137, 172.
[42] *R v Sharma,* 2020 ONCA 478 at para 101.

Section 7: FRT as an Infringement to Life, Liberty, and Security of the Person

"Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."

Section 7 guarantees everyone within Canada the right to life, liberty, and security of the person. This means that the government has an obligation to act in a way that does not threaten individual freedoms or increase the risk of death, physical or psychological harm. If the government must interfere with life, liberty, or security, they can only do so in a way that conforms with the "principles of fundamental justice," or our notions of justice and fair process. For example, the police are allowed to detain individuals (violating their liberty interest) as long as they do so in a rational and justified manner.[43]

Section 7 protects individuals if use of FRT poses a risk to life, liberty, or security of the person. For example, a law enforcement body could rely on FRT to find, arrest, and detain an individual, impacting their liberty interests. The heightened police scrutiny and the humiliation from wrongful police activity may affect the individual's personal dignity, physical, and mental health, impacting their life and security of the person.

Section 7 also protects individuals from breaches of privacy. Courts have recognized the great value of privacy in our society. Privacy is important to one's liberty, as liberty includes personal autonomy over decisions affecting one's private life. Privacy is also important to the security of the person, since loss of privacy could negatively affect one's psychological security and integrity.[44]

Establishing a section 7 is difficult. The use of FRT by law enforcement must violate the principles of fundamental justice by being "arbitrary, overbroad, or grossly disproportionate."[45] FRT use is "arbitrary" or "overbroad" if it was used in a manner that was irrational and does not serve to meet its law enforcement objective. FRT use is "grossly disproportionate" if the impact of the technology is so severe that it violates our fundamental norms.[46]

---

[43] *Charkaoui v. Canada (Citizenship and Immigration),* 2007 SCC 9 at para 19.
[44] *R v O'Connor,* [1995] 4 SCR 411, 1995 CanLII 51 (SCC) at paras 110-112.
[45] *Canada (Attorney General) v Bedford*, 2013 SCC 72 at paras 96, 120 [*Bedford*].
[46] *Ibid; Ewert, supra* note 40 at para 73.

The jurisprudence suggests that the merely inaccurate nature of FRT would be insufficient to breach the principles of fundamental justice, as the government is not obligated to use the most effective or accurate tools. For example, in *Ewert v Canada*, the finding that inmate risk assessment tools were less accurate and susceptible to cultural bias when applied to Indigenous offenders was not sufficient to establish a section 7 breach. The Supreme Court of Canada did not have enough evidence to assess the degree of bias in the technology. Thus, the judges did not have enough evidence to find that the technology was so inaccurate as to be arbitrary and overbroad, since the tools were still relevant to the government's objective of assessing inmate risk.[47]

Ewert v Canada underscores the importance of funding more research on the impacts of algorithmic technologies (**Recommendation 2**), as it would be difficult to establish a breach of section 7 without sufficient evidence. This case further underscores the importance of creating additional safeguards and oversight to how FRT is used by law enforcement. In **Recommendation 3: Implement a Data Protection Impact Assessment Scheme** and **Recommendation 4: Improve Oversight,** we outline ways in which the use of FRT can be regulated to avoid arbitrariness, overbreadth, and gross disproportionality. For instance, we recommend that police choose FRT rationally, only use it when strictly necessary, and only use it for narrowly tailored objectives. In doing so, the limitation of life, liberty, or security by FRT will still be compliant with the *Charter.*

Summary: Section 7 protects "life, liberty, and security of the person" alongside privacy. Establishing a section 7 breach is difficult. It is not enough to prove that FRT is inaccurate; one must prove that FRT was used in an arbitrary or overbroad manner (disconnected from its purpose) or that its use resulted in grossly disproportionate negative impacts. Implementing measures like a Data Protection Impact Assessment Scheme (**Recommendation 3**), conducting more research (**Recommendation 2**), and improving oversight of law enforcement (**Recommendation 4**) could proactively prevent arbitrariness, overbreadth, and gross disproportionality

[47] *Ewert, supra* note 40 at para. 73.

Section 9: FRT Use Resulting in Arbitrary Detentions

"Everyone has the right not to be arbitrarily detained or imprisoned."

Section 9 prohibits arbitrary detentions and imprisonments, thus offering protection to liberty and equality. A detention occurs when the state suspends an individual's liberty through physical or psychological restraint.[48] Law enforcement bodies may violate an individual's section 9 rights if they rely on information from FRT to detain an individual in an arbitrary manner. The protections offered in section 9 supplement **section 7**'s protection of liberty and **section 15**'s guarantee of equality rights.

Section 9 and section 15 protections may intersect in the context of FRT. Law enforcement must have reasonable and probable grounds to arrest or detain individuals; such grounds cannot be based on unreliable information, biased inferences, or discriminatory motives.[49] The Supreme Court of Canada has recognized that race is a relevant factor when analyzing whether a detention is arbitrary under section 9, given the disproportionate policing of racialized minorities.[50] As outlined in the discussion above, there are significant concerns about the accuracy of FRT, the potential for bias against certain marginalized groups, and the potential for automation bias when relying on FRT. If it can be proved that the detention was carried out on the basis of illegitimate information, then an individual may be able to establish that their detention was arbitrary.

Summary: Section 9 prohibits arbitrary detentions and provides supplementary protection to liberty and equality. Law enforcement may rely on information obtained from FRT to arrest or detain an individual. This detention may be arbitrary if the information produced by the FRT was unreliable or racially biased.

[48] *R v Grant*, 2007 SCC 32 at para 44 [*Grant*].
[49] *R v Storrey,* [1990] 1 SCR 241, 1990 CanLII 125 (SCC) at 251-252.
[50] *R v Le,* 2019 SCC 34 at paras 89-90.

Justifying a *Charter* Infringement under Section 1

"The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

Section 1 of the *Charter* imposes reasonable limits on our rights and freedoms by balancing the rights of the individual with the interests of society in using FRT for effective and efficient policing. If a *Charter* claimant can establish that their *Charter* rights have been breached, the state has an opportunity to argue that the infringement is justified in a free and democratic society. The analysis is heavily dependent on the context and the evidence available before the court.

Below is the four-part framework for how courts would analyze law enforcement's use of FRT to determine whether it is justified: (1) FRT must be used to further a pressing and substantial objective; (2) the use of FRT must have a rational connection to the objective; (3) the FRT must impair rights as minimally as reasonably possible; and (4) the benefits of the technology must outweigh its detriments.

Firstly, courts would likely find that FRT is used to further a pressing and substantial objective, since it is used to increase the effectiveness and efficiency of policing. Second, the use of FRT is rationally connected to this objective as it aims to increase the efficiency and effectiveness of such investigations. Courts are often deferential to law enforcement goals and their choice of methodology.[51]

Third, FRT might not impair rights as minimally as reasonably possible. Courts would consider whether there were alternative investigative techniques available that could have achieved the same objective without needing to covertly collect sensitive biometric information from the public. The collection, use and disclosure of biometric information poses broader risks than that of non-biometric information, given that it is immutable and personal.[52]The alternative investigative techniques do not have to be equally as effective as long as it sufficiently achieves the intended goal.[53] For instance, courts may find that instead of using FRT to identify a suspect, the police could have used traditional

---

[51] *R v Paterson*, 2017 SCC 15; Peter McGuinty, "Section 24(2) of the *Charter;* Exploring the Role of Police Conduct in the *Grant* Analysis" (2018) 41:4 The MLJ 273.

[52]Tunca Bolca, "Can PIPEDA 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation Against Facial Recognition Technology" (2020) 18 Can. J. L. & Tech. 51.

[53] *Alberta v. Hutterian Brethren of Wilson Colony,* 2009 SCC 37 at para 55.

eyewitnesses. How courts may approach this issue would depend on the particular objective and the sophistication of the technology.

Finally, it is uncertain whether the benefits of FRT in achieving effective policing outweigh its detriments. The disproportionate impact of technological inaccuracies on minority groups, as cited in the above **section 15** analysis, could be seen as incredibly problematic given the current unregulated uses of FRT by law enforcement. Courts may consider the technology's unknown efficacy and the possibility of built-in bias to outweigh its possible benefits to police investigations. However, if the flaws of the technology arise from mere novelty and inaccurate training, it may be difficult to convince a court that FRT is more discriminatory compared to existing law enforcement tactics. FRT is far from the first of the police's foray into biometrics; fingerprinting and genetic markers have been collected in databases for decades, and FRT has shown to be much faster at helping identify suspects than these alternatives.[54] Using FRT to better identify perpetrators of crimes could also benefit minority groups, as racialized people are overrepresented as victims of crime.[55]

The four-part test set out in section 1 is similar to the requirements for FRT use set out in **Recommendation 3: Implement a Data Protection Impact Assessment Scheme** (i.e. ensuring that use is rational, minimally impairing, and demonstrably effective at achieving public benefits). Such a scheme would proactively ensure that all uses of FRT, to the extent that they infringe *Charter* rights, only infringe in a manner that is justifiable.

Summary: Section 1 of the *Charter* imposes reasonable limits on our rights and freedoms by balancing the rights of the individual with the interests of society in using FRT for effective and efficient policing. Courts would apply a four-part test, considering the full context of the technology and its use. The most contentious parts of the analysis would be whether FRT infringes rights as little as reasonably possible, and whether the benefits of FRT outweighs its detriments. Implementing a Data Protection Impact Assessment Scheme (**Recommendation 3**) would proactively ensure that use of FRT passes each stage of the section 1 test.

[54] Naker & Greenbaum, *supra* note 11.
[55] Clayton J Mosher & Taj Mahon-Haft, "Race, Crime and Criminal Justice in Canada" in Anita Kalunta-Crumpton, ed, *Race, Crime and Criminal Justice International Perspectives*, 1st ed (Basingstroke, UK: Palgrave Macmillan, 2010).

Limitations of *Charter* Protections and Compensation

Although courts have attempted to address the threats to privacy and equality presented by emerging technologies, the *Charter* is still limited for the following three reasons.

First, establishing a *Charter* breach is a long, complex, and expensive process. It requires significant financial and legal resources that most individuals do not have. Hence, many individuals would not have the benefit of enforcing their *Charter* rights in court due to inadequate access to justice.

Second, it is difficult to claim compensation ("remedies") in a successful *Charter* case. While courts have a wide range of powers to grant remedies that it considers "appropriate and just in the circumstances" under section 24(1) of the *Charter*, they generally only exercise this power in rare cases of egregious rights infringements.[56] Courts also have the power to exclude improperly obtained evidence from FRT under section 24(2) of the *Charter*, but generally give significant deference (or leeway) to law enforcement goals in analyzing whether exclusion is warranted. If law enforcement bodies can demonstrate that its use of FRT was done in good faith, an individual could potentially be left without any recourse even if they have established that their rights were unjustifiably infringed.[57]

Third, *Charter* protections are applied retroactively, after the harm has already occurred, not proactively to address future wrongs. Unless the court declares that a technique, technology, or policy to be unconstitutional *in general,* the benefits of a successful *Charter* case also might not extend beyond the individual *Charter* claimant. This means that the *Charter* would not protect the general public from privacy breaches resulting from other police activities, such as in cases where law enforcement is surreptitiously testing novel facial recognition software. ***Charter* protections should therefore be conceptualized as the baseline upon which additional legislative and systemic protections are built in order to proactively prevent rights infringements.**

---

[56] *Canada (Attorney General) v. PHS Community Services Society*, 2011 SCC 44. For instance, in exceptional circumstances the court may order a government body to do or cease to do a specific action ("*mandamus*") if that is the only way to remedy the unconstitutionality. Such a remedy could be used to stop law enforcement from using FRT. Courts may also strike down specific laws and policies using s. 52(1) of the *Charter.*

[57] Peter McGuinty, "Section 24(2) of the *Charter;* Exploring the Role of Police Conduct in the *Grant* Analysis" (2018) 41:4 The MLJ 273. Courts have also analyzed "good faith policing" in an inconsistent and broad manner, making it difficult to predict under what circumstances evidence will be excluded.

Part 2: Recommendations

Throughout the submissions, we have highlighted how law enforcement bodies' use of FRT interacts with the protections granted under the *Charter*. The recommendations below are centred around bolstering our data protection laws and improving oversight mechanisms for law enforcement bodies as they implement new technologies. We turned to international sources for inspiration, drawing from the United Kingdom, the European Union, and the United States.

We propose the following legislative reforms:

Recommendation 1: Place a national moratorium on FRT while the government puts the appropriate safeguards in place

Recommendation 2: Fund research on the impact of FRT, especially concerning individuals from historically marginalized backgrounds

Recommendation 3: Implement a "Data Protection Impact Assessment" scheme for each law enforcement agency's use of FRT and other new technologies

Recommendation 4: Improve oversight on law enforcement bodies' use of FRT

Recommendation 5: Increase privacy protection of biometric information in the private sector

Recommendation 1: Place a National Moratorium on Algorithmic Policing Technologies

Temporarily banning the use of FRT by law enforcement bodies while the federal government amends legislation that outlines the lawful use of FRT

Objectives:

- To recognize and document the disproportionate impact that FRT has on historically marginalized groups
- To limit the infringement of constitutional rights during FRT's infancy

Overview:

- Prohibit law enforcement bodies from using new FRT that may infringe an accused's *Charter*-protected rights, including for "trial periods"
- Carve out a narrow and principled system for granting exemptions

Research regarding the reliability and accuracy of these technologies is still in its infancy. Without comprehensive research, it is impossible to accurately determine how these technologies could violate constitutional rights. We recommend a temporary national moratorium on all algorithmic policing technologies.[58] In the interim, greater safeguards to *Charter* rights should be put in place, as set out in the subsequent recommendations.

The federal government can create a set of prerequisite conditions — such as reliability, necessity, and proportionality — that can be used to evaluate technologies and provide exemptions where applicable. However, given the potential consequences arising from the misuse or flaws of these technologies, exemptions should not be given out loosely and threshold levels for granting exemptions should be set high.[59]

[58] Robertson, Khoo, and Song, *supra* note 38 at 154.
[59] *Ibid* at 154.

Recommendation 2: Fund Research on the Impacts of FRT

Fund research projects that seek to understand the impacts of the use of FRT by law enforcement bodies, particularly on historically marginalized groups

Objectives:

- To increase understanding of how FRT interacts with the constitutional rights of the accused, given how readily law enforcement bodies are adopting new technologies
- To increase understanding of how the use of FRT by law enforcement may exacerbate issues in the criminal justice system, particularly on historically marginalized groups who are over-represented

Overview:

- Fund individuals and organizations who are seeking to understand how algorithmic technologies are used by law enforcement bodies

Law enforcement agencies continue to adopt new technologies and predictive policing tools at a rapid rate.[60] Given the proliferation of new technologies, the government should make funding available to individuals and organizations to gain knowledge and expertise on how FRT and other algorithmic technologies interact with the criminal justice system and affect historically marginalized groups. This can assist in policy development and broader advocacy efforts, such as advocating for improved oversight of law enforcement.

Further research is also necessary to robustly understand how FRT interacts with constitutional rights.[61] First, greater transparency in the technology used by law enforcement would allow us to better predict how this technology could be scrutinized by courts. Some of the information that would be relevant to the **section 8** analysis includes: the specific type of FRT used by each major law enforcement agency; when, where, and how it is used by law enforcement; how it is used, if at all, in conjunction with other types of technology and corroborating evidence; and the sources of the images of the accused uploaded by law enforcement. Second, whether a **section 15** or **section 9** *Charter*

---

[60] Kate Allen, "Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known", *Toronto Star* (27 February 2020), online: <https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html>; Michelle McQuigge, "Predictive Policing Tools Use in Canada Spark Human Rights Concern: Report", *Vancouver Sun* (1 September 2020), online: <https://vancouversun.com/news/local-news/predictive-policing-tools-use-in-canada-spark-human-rights-concerns-report>

[61] Robertson, Khoo, and Song, *supra* note 38 at 168.

infringement would arise depends on the potential flaws and biases within the FRT. Further research into how the biases arise and how these biases can be mitigated in the future would inform how courts weigh the benefits and detriments of the technology.

Recommendation 3: Implement a Data Protection Impact Assessment Scheme

Implement a scheme for each and every use of FRT by every police force in Canada, similar to the Data Protection Impact Assessment (DPIA) scheme in the United Kingdom

Objectives:

- To ensure that the processing of sensitive personal data is fair and based on law
- To ensure FRT is only used when it is strictly necessary to do so for a valid law enforcement purpose
- To ensure uses of FRT bylaw enforcement are properly documented

Overview:

- Implement a DPIA-like document to accompany every use of FRT by police forces
- Commission Data Protection Officers (DPOs) to oversee the use of FRT and compliance with the DPIA-like scheme

The United Kingdom's Data Protection Impact Assessment (DPIA) scheme under the *Data Protection Act* is a written instrument created and maintained for each and every specific use of FRT, with the goal of ensuring that such uses fall in line with the principles of personal data processing.[62] The Information Commissioner's Office (ICO) is the governmental body in the United Kingdom responsible for overseeing the use of information technologies by government entities. The ICO released a statement in 2019 that reinforces and clarifies the safeguards of the DPIA.[63] The statement was in response to the case *R (Bridges) v South Wales Police*, which held that processing of public security camera footage to locate a person of interest is a violation of one's privacy rights. The England and Wales Court of Appeal found that the current DPIA scheme was not sufficient to justify this violation as it fails to give adequate guidance for the processing of sensitive

[62] *Data Protection Act 2018* (UK), 2018 c 12.
[63] United Kingdom, Information Commissioner's Office, *The Use of Live Facial Recognition Technology by Law Enforcement in Public Places* (London: 2019), online (pdf): <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf>

personal data or properly assess the risks posed by FRT.[64] It is recommended that Canada adopt a DPIA-like scheme that takes into consideration the ICO's clarifications and the inadequacies identified by the United Kingdom's Court of Appeals. A DPIA-like regulatory framework, outlined below, would ensure that every use of FRT by Canadian police forces is justified despite its violation of privacy.

The DPIA-like regulatory framework ensures that all uses of FRT must be fair and based on law.[65] In other words, the legal basis for using FRT must be sufficiently clear, precise, and foreseeable. The ICO also insists that police forces' use of FRT must be strictly necessary for a legitimate law enforcement purpose, unless such processing of personal data is consented to.[66] This essentially means that a police forces' use of FRT must be stringently proportional to its purpose.

- Police forces must demonstrate that their use of FRT was rationally chosen. They must have an understandable reason for using FRT to achieve their purpose.
- Use of FRT must be minimally intrusive. The processing of sensitive personal data must be kept to a minimum, to only what is necessary to achieve the police force's purpose.
- Use of FRT must be targeted. Police forces must only use FRT for a specific purpose, for instance, to catch a specific suspect of an ongoing criminal investigation.
- Use of FRT must be demonstrably effective at achieving its purpose.[67] The benefit of a police force's use of FRT must have an understandable benefit to the public.

As mentioned above, the DPIA-like framework imposes requirements that limit infringements of the principles of fundamental justice under **section 7**, given that it requires all uses of FRT to be connected to its objective (rather than being arbitrary, overbroad, or grossly disproportionate). The DPIA-like framework also mirrors the justification test under **section 1** of the *Charter*. It ensures that all uses of FRT are targeted towards a pressing and substantial object, that the use is rational and connected to the objective, that it infringes rights as minimally as possible, and that it is demonstrably effective at achieving benefits rather than imposing detriments. Such a scheme would proactively ensure that all uses of FRT, to the extent that they infringe *Charter* rights, only

[64] *R (Bridges) v South Wales Police*, [2019] EWHC 2341 (Admin), rev'd *R (Bridges) v South Wales Police*, [2020] EWCA Civ 1058 at paras 85-88, 153.
[65] United Kingdom, Information Commissioner's Office, *supra* note 63 at 7-8.
[66] *Ibid* at 11, 15-17.
[67] *Ibid* at 17.

infringe in a manner that is reasonable and justifiable.

The DPIA-like framework must also ensure that uses of FRT fall in line with the principles of personal data processing:[68]

- It must be created and updated for every single use of FRT by a police force, at the earliest design stage of a proposed use of FRT.
- It must clearly and comprehensively explain why FRT is strictly necessary (see above for specific substantive requirements).
- It must clearly assess the likelihood of effectively achieving the police force's purpose for using FRT.
- It must explain how effective mitigating measures have been implemented by the police force to avoid unnecessary violations of privacy rights when processing personal data.
- It must be continually reviewed (DPIA-like documents are "living" and require constant attention so long as a police force continues the use of FRT).

The scope of a DPIA-like document must capture not only the actual processing of personal data with FRT, but also the database or watchlist where such processed data is stored.[69] After processing, such data storage and use must likewise be scrutinized under the same principles mentioned above. The DPIA-like document should be maintained by a Data Protection Officer (DPO),[70] a separate government employee that attends to the police force's use of FRT and ensures that the integrity of the processing of personal data falls in line with the principles of the DPIA-like scheme.

- They must be allowed to oversee the police force's use of FRT
- They must be given ongoing support by the police force to maintain the DPIA-like document
- They must notify a governing body of any concerns or complaints in regard to the police force's use of FRT

[68] *Ibid* at 14.
[69] *Ibid* at 17-18.
[70] *Ibid* at 20.

Recommendation 4: Improve Oversight for Law Enforcement Bodies' Use of FRT

Improve oversight mechanisms for law enforcement bodies' use of FRT through mandatory public disclosure policies, and internal guidance and training

Objectives:

- To ensure public accountability and trust of law enforcement bodies' use of FRT
- To ensure there are clear internal policies that guide the appropriate usage of FRT, especially given the potentially rights-infringing nature of FRT
- To address sources of bias that is built into algorithms and FRT

Overview:

- Law enforcement bodies should publicly disclose what algorithmic technologies are used and for which purposes
- Create internal guidelines that limit excessive reliance on the results of FRT
- All officers who use the technologies should undergo effective prior training on relevant *Charter* issues that may arise

There is very little information available on how police services adopt new technologies, and very little oversight available in the adoption and use of this technology. In general, the information available is ill-defined, and it is ambiguous to what extent oversight policies are in place and are followed.

At the municipal level, police service boards are responsible for "establishing priorities, objectives and policies for police services in their community."[71] In practice, police services boards are limited in their effectiveness, as there is little actual oversight, or even knowledge, of the policies implemented.[72] For instance, after controversy regarding the use of Clearview AI technology by Toronto Police Service members, the Toronto Police Services Board released a statement that they were "in the information-gathering stage as it relates to Clearview AI" and were conducting a review on the "unauthorized use" of the AI.[73] Despite their commitment to communicate these findings to the public, no further

[71] Ontario Association of Police Services Boards, "Governing Police" (2017), online: <https://oapsb.ca/>.
[72] Michael H. Tulloch, "Report of the Independent Police Oversight Review" (2017) at s 7.344, online: Attorney General of Ontario <https://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/police_oversight_review/>
[73] Toronto Police Services Board, "Toronto Police Services Board's Statement With Respect to the Use of Clearview AI Technology" (25 February 2020), online:

information has been shared. Similarly, the Ottawa Police Services Board was "made aware" of a pilot project using facial recognition software NeoFace by police service members, but was unaware of the trial use of Clearview AI.[74] In their statement, the Ottawa Board recognized their "need to develop an IT Governance and Information Management Strategy based on recognized industry standards," implying that they currently do not have technology oversight.[75] These examples in Toronto and Ottawa highlight the insufficient oversight and operational control police service boards have.

At the provincial level, police service boards and police services are generally subject to oversight in accordance with specific statutes. In Ontario, the lack of sufficient transparency, accountability, independence, cultural competency, and effectiveness of police oversight bodies[76] limits their ability to address individual or systemic police use of FRT. Under the Ontario *Police Services Act*[77], the Office of the Independent Police Review Director (OIPRD) is responsible for investigating individual complaints against police services, conducting performance audits against police service boards on their methods of handling complaints, and reporting on systemic policing issues. For police services boards, the Ontario Civilian Police Commission (OCPC) has powers to investigate individual complaints against board members and identify systemic failings in the boards' abilities to oversee its police service.[78] While both the OIPRD and the OCPC can make recommendations about systemic issues in policing (such as FRT), they have no actual powers to enforce these recommendations or bring about practical changes.

At the federal level, the RCMP is overseen by the Civilian Review and Complaints Commission for the RCMP. The RCMP has released a digital policing strategy to outline their planned use of digital services and technology.[79] While the oversight portion of the policy is vague, the RCMP has committed to "introduce clear governance structures to ensure quality controls and risk management."[80] In order to develop this, they plan to engage the "existing governance framework, the Investment Oversight and Prioritization

---

<https://tpsb.ca/mmedia/news-release-archive/listid-2/mailid-175-toronto-police-services-board-s-statement-with-respect-to-the-use-of-clearview-ai-technology>.

[74] Ottawa Police Services Board, "Response to Inquiry Facial Recognition Software" (27 April 2020), online (pdf): <http://ottwatch.ca/meetings/file/635623>.

[75] *Ibid*.

[76] Michael H. Tulloch, "Report of the Independent Police Oversight Review" (2017), online: Attorney General of Ontario <https://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/police_oversight_review/>

[77] *Police Services Act,* RSO 1990, c P15.

[78] Ontario Civilian Police Commission, "About the OCPC", online: Tribunals Ontario <https://tribunalsontario.ca/ocpc/>

[79] Royal Canadian Mounted Police, "Digital Policing Strategy", online: <https://www.rcmp-grc.gc.ca/en/connected-rcmp>

[80] *Ibid* at 36.

Committee, and the Committee on Digital Investments."[81] While the policing strategy speaks of the development of an oversight strategy, the RCMP also states they plan to "adopt the digital standard used by the Government of Canada and our National Police Service partners and embrace market standard technologies." This indicates the digital standards of the RCMP are dependent on the quality of the standards of National Police Service partners. This digital policy is ill-defined and has not been able to safeguard against unapproved use of facial recognition technologies.

Internal Controls: Clear Guidelines and Training

Internal guidelines for the use of algorithmic technologies like FRT should be implemented on a municipal, provincial, and federal level. Controls must be put in place to ensure that use of FRT is reasonable, rational, and unbiased, thus avoiding violations of the *Charter* sections described in **Part 1**.

Before using algorithmic policing technology, clear guidelines and training for its use need to be implemented systematically across all law enforcement bodies in Canada. Training sessions should be used to advise officials on best practices for authorized technologies, advise officials on how to recognize and avoid unconscious and automation biases when using technology, and distill *Charter* requirements into clear guidelines.[82] Crown prosecutors and judges should also receive mandatory training on relevant *Charter* issues that can possibly arise in cases where algorithmic policing technologies have been used.[83]

In the operational use of algorithmic policing technology, certain practices should be adopted to best protect individual rights and increase transparency. Where an individual has been stopped, detained, or arrested and algorithmic policing technologies were used, officials should inform them that technology was involved and how it was used.[84] Where biometric data has been lawfully collected but the charges are later dropped, stayed, or dismissed, the data should be automatically destroyed.[85] In order to ensure the accuracy of the algorithmic decisions, law enforcement databases should be subject to regular maintenance and derived from the most current data sources.[86] Additionally, regular

---

[81] *Ibid* at 49.
[82] Robertson, Khoo, and Song, *supra* note 38 at 178.
[83] *Ibid* at 180.
[84] *Ibid* at 176.
[85] *Ibid* at 166.
[86] *Ibid* 165-166.

internal review regarding new police technologies and possible rights violations arising from them could serve to avoid and reduce rights violations.

External Controls: Public Disclosure and Transparency

External controls on police technology use are lacking because the public does not have an opportunity to hold police services accountable. The public often does not even know about police wrongdoings. For instance, of the many police forces that have admitted in 2020 to using Clearview AI, nine had at first told news sources that they were not using Clearview AI.[87] Law enforcement agencies employing algorithmic policing technologies, especially FRT, should be required by law to publicly disclose:

1. Which technology they are using;
2. Whether the technology is being developed or already in use;
3. How the technology is or will be used; and
4. How use of the technology is or will be evaluated

Recommendation 5: Increase Privacy Protection for Biometric and Personal Information

Amend the private sector data protection laws to strengthen "biometric information" beyond "personal information," drawing from Illinois's Biometric Information Privacy Act

Objectives:

- To strengthen privacy protection for biometric information, which includes retina scans, fingerprints, voice prints, or scan of face geometry
- To recognize the inherently elevated risk of the wrongful disclosure, misuse, or theft of biometric information

Overview:

- Amend the proposed *Consumer Privacy Protection Act* (CPPA) to explicitly mention "biometric information," instead of relying exclusively on "personal information"
- Amend the proposed CPPA to mandate an individual's express and informed consent for all data collection purposes, including research and development

[87] Allen, *supra* note 60.

Strengthening private sector protections in conjunction with public sector protections would allow for comprehensive privacy regulation. A legislative definition and framework for the processing of biometric information can set an important precedent for how this type of data is handled by the public sector and law enforcement. As described above in our analysis of **section 8**, courts may also be influenced by private sector definitions of "privacy" and biometric information.

The potential replacement of the PIPEDA with the CPPA via Bill C-11[88] provides an opportunity to increase privacy protection specifically for biometric information. As indicated above, while biometric information certainly falls under the category of "personal information," the OPC has recognized the inherently elevated risk in using biometrics for identification and authentication compared to other types of data.[89]

Illinois has one of the strongest biometric protection legislation in North America. The *Biometric Information Privacy Act* (BIPA) provides substantial protections for individuals' privacy in the private sector.[90] The statute ensures that all biometric data collected by private entities is stored for only a limited time and for a valid purpose.[91] As per section 15(c) of the BIPA, such data cannot be used by the private entities for profitable purposes.[92] Prior to collection of such data, private entities must obtain informed, written consent from the individual or their legally authorized representative. The statute also notably provides a right of action to individuals aggrieved by any statutory violations. These wide protections afforded by the BIPA are similarly found in the *California Consumer Privacy Act of 2018*.[93]

The proposed CPPA introduces more robust protection for individuals' personal information, but is different from the BIPA in crucial respects. First, the CPPA does not explicitly define "biometric information." It ought to do so to ensure that biometric information is actively being protected, instead of relying on the broad definition of personal information as "information about an identifiable individual."[94] The CPPA could

---

[88] Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 43-2 (2020) at § 15 (as passed by the House of Commons 17 November 2020) [*Bill C-11*].
[89] Office of the Privacy Commissioner of Canada, *Guidelines for identification and authentication*, *supra* note 22.
[90] *Biometric Information Privacy Act*, 740 ILCS 14 (2018) [*BIPA*].
[91] *BIPA, ibid* at § 15.
[92] *Ibid*.
[93] *California Consumer Privacy Act of 2018*, 3 CIV 1.81.5. (2018) at § 1798.100.
[94] *Bill C-11*, *supra* note 88 at § 2.

adopt similar terminology to section 10 of the BIPA, which states that biometric identifiers protected under the Act mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[95]

Second, while Illinois requires consent in written form, section 15(4) of the CPPA allows for the less certain form of implied consent in certain appropriate circumstances.[96] These circumstances are left undefined by the CPPA, which could lead to future issues of judicial interpretation.

Third, unlike in Illinois, the CPPA allows businesses to use de-identified personal information without consent for research and development purposes per section 15(21).[97] Furthermore, per section 15(20), businesses "may use an individual's personal information without their knowledge or consent to de-identify the information."[98] This is particularly troubling as the CPPA defines "de-identify" in rather ambiguous terms: "[...] to modify personal information [...] by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances [...] to identify an individual."[99] What constitutes "reasonably foreseeable circumstances" is uncertain and possibly too flexible and deferential to businesses. Private organizations should have to acquire explicit consent for every use of biometric information, even if it is de-identified. Amendments to the CPPA would recognize the immutable and individualized nature of biometric data, as well as the heightened privacy concerns attached to biometrics.

---

[95] *BIPA, supra* note 90 at § 10.
[96] *Bill C-11*, *supra* note 88 at § 15.
[97] *Bill C-11*, *supra* note 88 at § 2.
[98] *Bill C-11*, *supra* note 88 at § 15.
[99] *Ibid.*

Conclusion

We hope that the Standing Committee will take the foregoing recommendations and considerations into account in their study on the Impact of Facial Recognition and Artificial Intelligence, as well as in any future legislation or projects on the subject. As FRT quickly becomes more integrated into public services, and law enforcement in particular, it is of the utmost importance to ensure that Canadians' constitutional rights are well protected from potential infringement. If deeper research is not done and appropriate measures are not put in place, these technologies can have devastating impacts on Canadians' constitutional rights, including exacerbating current issues and discrimination in the criminal justice system.

References

Literature and Reports

European Union Agency for Fundamental Rights, “Facial recognition technology: fundamental rights considerations in the context of law enforcement” (November 2019), online (pdf): <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf>.

Clare Garvie et al, “The Perpetual Line-Up” (October 18, 2016), online: <https://www.perpetuallineup.org/>.

Clayton J Mosher & Taj Mahon-Haft, “Race, Crime and Criminal Justice in Canada” in Anita Kalunta-Crumpton, ed, *Race, Crime and Criminal Justice International Perspectives*, 1st ed (Basingstroke, UK: Palgrave Macmillan, 2010).

Gerald Chan, “Text Message Privacy: Who Else is Reading This?” (2019) 88 Osgoode’s SCLR 75.

Jacqueline G Cavazos et al, “Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?” (January 2021) 3:1 *IEEE Transactions on Biometrics, Behavior and Identity Science* 101.

Joy Buolamwini & Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification” (2018), PMLR 81:77-91, online: <https://proceedings.mlr.press/v81/buolamwini18a.html>.

Kate Allen, “Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known”, *Toronto Star* (27 February 2020), online: <https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html>.

Kate Robertson, Cynthia Khoo, and Yolanda Song, “To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada” (September 2020) at 154, online (pdf): <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.

Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” *The New York Times* (18 January 2020), online: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

Law Enforcement Imaging Technology Task Force, “Law Enforcement: Facial Recognition UseCase Catalog” (March 2019) at 3, online (pdf): <https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf>.

Louise Matsakis, “Scraping the Web Is a Powerful Tool. Clearview AI Abused It,” *Wired* (25 January 2020), online: <https://www.wired.com/story/clearview-ai-scraping-web/>.

Michael O'Flaherty, “Facial Recognition Technology and Fundamental Rights” (2020) 6:2 Eur Data Prot L Rev 170.

Michael H. Tulloch, "Report of the Independent Police Oversight Review" (2017) at s 7.344, online: Attorney General of Ontario <https://www.attorneygeneral.jus.gov.on.ca/english/about/pubs/police_oversight_review/>.

Michelle McQuigge, "Predictive Policing Tools Use in Canada Spark Human Rights Concern: Report", *Vancouver Sun* (1 September 2020), online: <https://vancouversun.com/news/local-news/predictive-policing-tools-use-in-canada-spark-human-rights-concerns-report>.

Monique Mann & Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" (2017) 40:1 UNSWLJ 121.

Office of the Privacy Commissioner of Canada, "Automated Facial Recognition: In the Public and Private Sectors" (March 2013), online (pdf): <https://www.priv.gc.ca/media/1765/fr_201303_e.pdf>.

Office of the Privacy Commissioner of Canada, News Release, "Clearview AI ceases offering its facial recognition technology in Canada (6 July 2020), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/>.

Office of the Privacy Commissioner of Canada, *Guidelines for identification and authentication*, June 2016 update (June 2016), online: <https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth_061013/>.

Office of the Privacy Commissioner of Canada, *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* (2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

Ontario Association of Police Services Boards, "Governing Police" (2017), online: <https://oapsb.ca/>.

Ontario Civilian Police Commission, "About the OCPC", online: Tribunals Ontario <https://tribunalsontario.ca/ocpc/>.

Ottawa Police Services Board, "Response to Inquiry Facial Recognition Software" (27 April 2020), online (pdf): <http://ottwatch.ca/meetings/file/635623>.

Patrick Grother, Mei Ngan and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (December 2019), U.S. Department of Commerce, National Institute of Standards and Technology, online: <https://doi.org/10.6028/NIST.IR.8280>.

Peter McGuinty, "Section 24(2) of the *Charter;* Exploring the Role of Police Conduct in the *Grant* Analysis" (2018) 41:4 The MLJ 273.

Royal Canadian Mounted Police, "Digital Policing Strategy", online: <https://www.rcmp-grc.gc.ca/en/connected-rcmp >.

Royal Canadian Mounted Police, News Release, "RCMP Use of Facial Recognition Technology" (27 February 2020) online: <https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-use-facial-recognition-technology>.

Sharon Naker & Dov Greenbaum, "Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy" (2017) 23:1 BU J Sci & Tech L 88 at 97.

Toronto Police Services Board, "Toronto Police Services Board's Statement With Respect to the Use of Clearview AI Technology" (25 February 2020), online: <https://tpsb.ca/mmedia/news-release-archive/listid-2/mailid-175-toronto-police-services-board-s-statement-with-respect-to-the-use-of-clearview-ai-technology>.

Tunca Bolca, "Can PIPEDA 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation Against Facial Recognition Technology" (2020) 18 Can. J. L. & Tech. 51.

United Kingdom, Information Commissioner's Office, *The Use of Live Facial Recognition Technology by Law Enforcement in Public Places* (London: 2019), online (pdf): <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf>.

United States Government Accountability Office, "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses" (July 2020), online (pdf): <https://www.gao.gov/assets/gao-20-522.pdf>.

Legislation

Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 43-2 (2020) at § 15 (as passed by the House of Commons 17 November 2020).

Biometric Information Privacy Act, 740 ILCS 14 (2018).

California Consumer Privacy Act of 2018, 3 CIV 1.81.5. (2018).

Canadian Charter of Rights and Freedom, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Corrections and Conditional Release Act, SC 1992, c 20.

Data Protection Act 2018 (UK)*,* 2018 c 12.

Police Services Act, RSO 1990, c P15.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Case law

Alberta v. Hutterian Brethren of Wilson Colony, 2009 SCC 37.

Canada (Attorney General) v Bedford, 2013 SCC 72.

Canada (Attorney General) v. PHS Community Services Society, 2011 SCC 44.

Charkaoui v. Canada (Citizenship and Immigration), 2007 SCC 9.

Ewert v Canada, 2018 SCC 30.

Fraser v Canada (Attorney General), 2020 SCC 28.

Hunter v Southam, [1984] 2 SCR 145, 1984 CanLII 33 (SCC) .

R v Marakah, 2017 SCC 59.

R v MS, 2019 ONCJ 670.

R v Ahmad, 2020 SCC 11.

R v Collins, [1987] 1 SCR 265, 1987 CanLII 84 (SCC) .

R v Grant, 2007 SCC 32.

R v Jarvis, 2019 SCC 10.

R v Le, 2019 SCC 34.

R v Quesnelle, 2014 SCC 46.

R v Morris, 2021 ONCA 680.

R v O'Connor, [1995] 4 SCR 411, 1995 CanLII 51 (SCC) .

R v Paterson, 2017 SCC 15.

R v Spencer, 2014 SCC 43.

R v Sharma, 2020 ONCA 478.

R v Storrey, [1990] 1 SCR. 241, 1990 CanLII 125 (SCC) .

R (Bridges) v South Wales Police, [2019] EWHC 2341 (Admin) .

R (Bridges) v South Wales Police, [2020] EWCA Civ 1058.