Interim Report: Facial Recognition Technology in Canada

Jan. 4, 2021

Laksmiina Balasubramaniam

Charlie Cooper-Simpson

Jordan Morello

Pamela Pietrusiak

A Report Created by Student Volunteers from the Public Good Initiative, Munk School of Global Affairs and Public Policy for the CCLA

Table of Contents

Introduction

This report examines the state of affairs in Canada regarding the use of facial recognition technology in the private and public sectors. The use of facial recognition technology in Canada has received significant attention recently following a spate of reporting on previously undisclosed uses of the controversial technology. As the report shows, its use exposes Canadians to possible violations of their privacy and security. Yet despite its increasing popularity among law enforcement agencies and in the retail sector, there is no regulatory framework in place in Canada that specifically responds to the advent of this technology.

Section 1, "What is Facial Recognition Technology?", introduces the basics of how facial recognition technology is used to verify identity or identify individuals and describes the processes of developing facial recognition technology. It also begins to identify equality and privacy concerns that are further explored in the remainder of the report.

Section 2, "Quality Control: The Risks of Misidentification," summarizes the existing literature examining sources of error in the use of facial recognition technology and examines the associated risks. Understanding the risk of misidentification and the possible sources of error when facial recognition technology is used is essential to understanding its impact on Canadians, yet evaluating the accuracy of a given facial recognition algorithm presents a significant technical challenge.

Section 3, "Privacy Concerns Regarding Facial Recognition Technology in Canada," provides a summary of current privacy laws in Canada and how they limit the collection of public information by both the public and private sector. This section will outline the current shortcomings of privacy laws to highlight the need for a clearly defined legal framework as it pertains to the harvesting of biometric data. An analysis of recent cases that demonstrate the use of biometric technologies with and without consent will also be examined.

Section 4, "Facial Recognition Technology in the Public Sector," summarizes the use of facial recognition technology within the public sector in Canada. This includes adoption by law enforcement agencies at the municipal, provincial and federal level as well as public administration bodies outside of law enforcement.

Section 5, "Facial Recognition Technology in the Private Sector," summarizes the use of facial recognition technology within the private sector in Canada, focusing primarily on the

Office of the Privacy Commissioner of Canada's (OPC) recent report concerning Cadillac Fairview Corporation Limited's use of facial analytics in shopping malls, and connecting the OPC's decision to proposed changes to Canada's private sector privacy law.

Section 6, "Existing Facial Recognition Technology Policies and Regulations," consists of a jurisdictional scan of the regulatory and policy environment in the United States, paying particular attention to the use of municipal bans/moratoriums and state biometric laws. The findings from this scan are used to analyze the regulatory and policy trends in Canada.

1. What is Facial Recognition Technology?

Facial recognition technology (FRT) works by extracting biometric information based on key facial features and analysing this information to allow for comparisons between different representations of a face.[1] The first step is capturing an image of an individual's face which serves as the input—the biometric or facial probe into the facial recognition system. To capture an image a static image or video recording may be used. Before using a facial recognition algorithm, the system must rely on a face detection algorithm to separate out a face from background elements of the picture. From the captured image of a face, the FRT will extract a template consisting of a numerical representation of key facial features.[2] Exactly which features are extracted and the process of encoding varies between systems because it is "learned by the algorithm".[3] The biometric description created should be very similar to what would be produced for the same person at a different time and different from templates that would be extracted from different individuals.[4] In certain cases, additional information may be stored with the facial features. For example, when FRT is used for border control, templates may be linked to identifying information such as name, address, nationality and passport number. Once a template is extracted from this information, it is not necessary for the image or recording to be stored. This is because facial recognition systems identify or verify individuals by comparing the extracted facial template to a reference, not by comparing two facial images directly. Therefore, facial images or recordings should be deleted to avoid risk of privacy breaches.[5] This will be discussed further in the privacy concerns section.

A facial recognition system may extract a biometric template from a photograph of a face or from a video recording.[6] While it may be possible to extract images from videos and at a distance, close-up photographs may provide higher quality images which may be better for accuracy. Pose and lighting can alter the effectiveness of facial recognition technology and therefore setting out requirements for minimum criteria for images to be used with facial

---

[1] Tamir Israel, "Facial Recognition at a Crossroads: Transformation at our Borders and Beyond." *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC),* 1-16, (2020).
[2] Ibid, 21-25.
[3] Taylor Owen et al., "Facial Recognition Moratorium Briefing #1: Implications of a Moratorium on Public Use of Facial Recognition Technology in Canada", 4, August 18, 2020.
[4] Supra note 1 "Facial Recognition at a Crossroads", 21-25.
[5] Ibid, 13.
[6] Ibid, 21-25.

recognition technology can be an important safeguard. This is also important as poorer quality images may disproportionately impact the effectiveness of facial recognition technology in identifying certain demographics. These issues will be discussed in the quality control section.

Following extraction of the template, the newly captured facial template needs to be compared to one or more existing templates stored for reference.[7] Comparing the newly captured facial template to one or more existing templates will generate a comparison score to reflect the level of similarity. The output produced will vary by the facial recognition system. Some may produce a simple match or non-match decision that the two samples are either from the same individual or not. The decision will vary based on the adopted confidence threshold—the benchmark for estimated similarity before there is recognition, where anything below the threshold is labelled as a non-match. Some systems may produce a series of potential matches that meet the confidence threshold or produce the top number of similar images after which a human manually makes a decision on whether there is a match. There is no industry wide standard for the threshold required for a match.[8] While a developer may suggest a default match threshold, organizations using the technology may adjust the threshold for their own use.

1.1 Developing Facial Recognition Technology

To develop facial recognition technology, there must be a facial recognition algorithm that "learns" to recognize faces.[9] This process of learning to recognize faces will require the use of many facial images that are part of a training data. To develop accuracy rates sufficient for practical use, this may require training data sets composed of millions or even tens of millions of images.[10] This raises many concerns because a lot of the images in the training data set used in algorithm training processes have not been collected with meaningful consent.[11] There are some publicly available datasets intended for use of facial recognition learning. Some training datasets draw from public websites such as Flickr while private companies such as Google and Facebook have been reported to train facial recognition algorithms on privately held images of their users.[12]

The composition of training datasets has important implications for the accuracy of the facial recognition technology. Using images of racially biased, front-facing images do not

---

[7] Ibid, 26-30.
[8] Supra note 2 "Facial Recognition Moratorium Briefing #1".
[9] Supra note 1 "Facial Recognition at a Crossroads", 5.
[10] Ibid.
[11] Ibid, 3.
[12] Ibid, 17.

account for the variety of factors that will affect accuracy of facial recognition systems in real world use.[13] Testing on datasets that lack demographic diversity reduces practical accuracy and can produce misleading estimates of accuracy. Many of the biggest publicly available training sets rely on images of celebrities that include a relatively homogenous population. After a facial recognition algorithm that can recognize faces is developed, it must be tested. Again, the types of facial images in the testing dataset has serious implications for estimates of accuracy of facial recognition and racial bias. These concerns will be discussed in detail in the quality control section.

Finally, when a facial recognition system is in use, there must be a reference dataset.[14] The reference data set includes the information serving as the comparison for the newly collected facial images. Including quality assessment procedures to ensure only images of sufficient quality are used in the reference data set can help increase accuracy of facial recognition, but this is not adopted by all facial recognition systems.[15] Additionally, as ageing can reduce effectiveness of facial recognition technology, maintaining reference datasets with updated information can improve accuracy.[16]

Since facial recognition systems are comparing facial templates, when working within one facial recognition system it is sufficient to retain facial templates rather than facial images.[17] As there is not a universal standard for creating facial templates, different systems will have different templates that may not be compatible with other facial recognition systems. Maintaining a reference dataset of facial templates rather than facial images is more secure. Even if compromised, the facial templates would be less likely to be able to be repurposed than if facial images were stored.

Reference data storage can be centralized or decentralized.[18] A centralized system means all the information is stored together on a server rather than a decentralized approach where information would be stored on an individual user's device. For example, biometric passports where facial images are stored on individual's passports are an example of a decentralized reference dataset. Since 2008, the International Civil Aviation Organization has established

[13] Ibid, 17-20.
[14] Ibid, 6-10.
[15] Ibid, 11.
[16] Ibid, 14.
[17] Ibid, 12-13.
[18] Ibid, 6-10.

criteria for including facial recognition compatible images on the contact-less radio frequency identification memory chip of compliant passports.[19] Canada has issued electronic passports that are complaint with ICAO facial images criteria since 2013. A centralized system is at greater risk for data security breaches and repurposing of information.[20] If data stored centrally is compromised, there would potentially be access to the entire collection of information allowing for compromise at a systematic rather than individual level. Additionally, without the knowledge or consent of individuals, information in a centralized system can be more easily repurposed or aggregated with other biometrically enabled databases than if individuals held their own information.

1.2 One-to-one vs. one-to-many systems

Facial recognition technology can be used to verify the identity of a specific individual (one-to-one system) or to automate identification of an individual (one-to-many system).[21] In a one-to-one system, an image taken of an individual is compared only to a previous image that is presumed to be of the same individual to verify identity. This form of facial recognition technology may be used to unlock cellphones. It can also be used when an individual is seeking to get a new government identification card such as a driver's license where facial recognition software can compare the newly taken image of the individual against the previously stored image of the individual to ensure it is the same person. If on the other hand, facial recognition software is used to compare the newly taken image of an individual to images of all individuals in the database, this is a one-to-many system.

A one-to-many system is when a photo of an individual is compared to all photos in a database.[22] This can be used to either verify identity (like a one-to-one system) or to try and identify unknown individuals. Such systems may more commonly be used by police when comparing a photo of an unknown individual to a database consisting of mugshots. Outside of law enforcement, in Ontario, casinos have adopted a one-to-many system for a voluntary self-exclusion program for those with a gambling addiction who have asked to be removed from casinos if they enter.[23] Since a one-to-many system involves running many more comparisons

[19] Ibid, 6-7.
[20] Ibid, 9-10.
[21] Ibid, 26-30.
[22] Ibid, 26-30.
[23] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors*, 4, March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf.

with the information of all individuals stored in a database, it raises more concerns than a one-to-one system.[24] Conducting high levels of comparisons for any individual search can result in larger error rates. Reducing the size of the reference dataset may increase effectiveness of facial recognition systems.

1.3 What Probe photos are used?

The selection of probe photos can raise concerns surrounding privacy and equality rights. First, regarding the collection of probe photos, whether there is meaningful consent for facial images being captured implicates privacy rights. Furthermore, the quality of probe photos used can impact accuracy levels for facial recognition technology by varying degrees for different populations. Differences in the accuracy of facial recognition technology in real world applications compared to industry reports may emerge because of variation in the images used for testing and actually used in practice. The issues relating to image quality for probe photos has been briefly discussed and will be elaborated on in the quality control section. In short, testing on highly standardized images with forward-facing subjects that are racially homogenous will likely result in higher accuracy ratings than can be expected in practical use of facial recognition technology.[25] That is why requirements for standards of image quality to be used should be adopted to avoid further reductions in accuracy of facial recognition technology and disproportionate impacts on certain demographic groups such as racialized minorities and/or women.

When high quality photos are not available, there is a concern that photos will be edited in ways not strictly intended to improve photo quality, but rather to try and facilitate a match. For example, in "Garbage In, Garbage Out", it is reported that photos are often edited by local police forces before submitting for searches.[26] These edits go beyond lighting adjustments and may include replacing facial features in a probe photo inputted into a facial recognition system to more closely resemble mugshots. For example, it was reported in a NYPD presentation that to remove facial expression, such as replacing an open mouth with a closed mouth, images of lips found through "a Google search for Black Male Model" were pasted into a probe image.

---

[24] Supra note 1 "Facial Recognition at a Crossroads", 29-30.
[25] Ibid, 17-20.
[26] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, May 16, 2019, https://www.flawedfacedata.com/#art-or-science.

It is also highly concerning that at least half a dozen police departments across the United States allow police departments to conduct facial recognition searches using forensic sketches as the probe photo.[27] Companies providing facial recognition systems to police departments in the United States including Rekognition by Amazon Web Services, Cognitec and Vigilant solutions market their facial recognition systems as appropriate for use with sketches. However, sketches do not accurately capture facial features precisely because they rely on eyewitness memory, the ability of an eyewitness to communicate this memory and the ability of an artist to accurately translate a description into an image. As this is a subjective process with many chances for error, sketches are poor inputs into a facial recognition system and should not be used. Commercial systems are not designed to match sketches to photographs—a study of the Cognitec algorithm found that using sketches as the input only retrieved the correct image in the top 200 possible matches 4.1-6.7% of the time, about 1 out of every 20 searches.

1.4 What Reference Dataset is used?

Different facial recognition systems may draw on different sources of images for their reference data set. Whether individuals consent to their images being enrolled in a reference dataset is an important concern. In Canada, images in the passport database were re-purposed for fraud detection in passport applications so new passport applications are compared to past passport images to determine if individuals are applying under different names.[28] Additionally, when a facial recognition system is required for holding a passport, it cannot truly be considered voluntary. The voluntary self-exclusion program from casinos is an example of a truly voluntary enrollment in a reference dataset.

In the private sector, Clearview AI illegally scraped images from Facebook, Twitter, YouTube and other websites in violation of the terms of use of these platforms and without the consent of individuals.[29] Facebook settled a class action under Illinois biometric privacy law for creating facial templates without meaningful consent after it re-purposed user images and included them in facial recognition databases.[30]

Conclusion

[27] Ibid.
[28] Supra note 1 “Facial Recognition at a Crossroads”, 52-57.
[29] Ibid, 124-125.
[30] Ibid, 54.

The current processes of developing facial recognition technology and its applications raises serious concerns for privacy and equality. The remaining sections of this report will examine how existing frameworks provide insufficient protection for privacy and equality rights. Following consideration of examples of facial recognition technology adopted in Canada within the public and private sector, suggestions for regulations drawing from other jurisdictions are discussed.

2. Quality Control: The Risks of Misidentification

Facial recognition technology offers, ostensibly, the ability to either classify or identify an individual on the basis of an image of their face. While this ability raises concerns regarding the collection of personal information and the privacy and security of individuals who are identified via that personal information, there is a separate set of concerns regarding the possibility of *misidentification*. The possibility of being falsely identified carries significant risk, especially where FRT is in use by law enforcement, since false identification can lead to arrest and detention.[31] Moreover, if people are more or less likely to be misidentified based on their demographic characteristics such as race or gender, the use of FRT may lead to discriminatory practices.

In order to understand the impact of the increasingly widespread use of FRT, then, we must understand how accurate the facial recognition (FR) tools actually in use are likely to be, and what the typical sources of error are. A survey of the existing literature yields the following conclusions:

- The ability of FRT to accurately identify or classify images of individuals depends on the individuals' race, gender and age, meaning that there are systematic biases affecting FRT accuracy.[32]
- The ability of FRT to accurately identify or classify images of individuals depends significantly on the quality of the input (or 'probe') image used.[33]

---

[31]See Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. For this reason, the Washington Post Editorial Board has called for a nationwide moratorium on FRT use: "Unregulated facial recognition must stop before more Black men are wrongfully arrested," January 4, 2021, https://www.washingtonpost.com/opinions/unregulated-facial-recognition-must-stop-before-more-black-men-are-wrongfully-arrested/2020/12/31/dabe319a-4ac7-11eb-839a-cf4ba7b7c48c_story.html.

[32] Joy Buolamwini, Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, 81:1–15, 2018; Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*," December 2019, https://doi.org/10.6028/NIST.IR.8280; Krishnapriya K.S. et al., "Characterizing the Variability in Face Recognition Accuracy Relative to Race," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2019.

[33] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, May 16, 2019, https://www.flawedfacedata.com/#art-or-science.

- Some law enforcement agencies in the United States have used celebrity look-alike photos, digitally edited photos, or forensic sketches as probe photos. The use of forensic sketches was even encouraged by a few FRT vendors.[34]
- There are more than one hundred commercially available FR algorithms,[35] and there is a significant range in reported accuracy across facial recognition algorithms.[36] There are also well-known open-source tools for developing such algorithms, significantly reducing barriers to entry.[37]

The discussion that follows will examine these issues in further detail. Section 2.1 details how the accuracy of FRT is measured. Sections 2.2–2.3 examine different sources of error for FRT: section 2.2 looks at the effect that race, gender and age have on FRT accuracy, and section 2.3 looks at the impact of the quality of the probe image used. Section 2.4 considers the state of the FR market in the absence of industry regulation.

2.1 How is accuracy measured?

Facial recognition algorithms, whether they involve 1:1 (one-to-one) or 1:N (one-to-many) comparisons,[38] produce outputs on the basis of similarity scores for pairs of images (for e.g. the probe image and an image from the database). The similarity scores are then measured against a 'confidence threshold'; if the score exceeds the threshold, the pair of images are treated as a match (or a possible match).

---

[34] *ibid*.
[35] Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*," December 2019, https://doi.org/10.6028/NIST.IR.8280.
[36] National Institute of Standards and Technology *FRVT 1:N Leaderboard*. https://pages.nist.gov/frvt/html/frvt1N.html.
[37] See Adam Geitgey, "Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning," *Medium*, https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78. See also *OpenFace: Free and open source face recognition with deep neural networks*, https://cmusatyalab.github.io/openface/; Florian Schroff, Dmitry Kalenichenko, James Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.
[38] In the NIST Vendor Test report, 1:1 algorithms are referred to as "verification" algorithms (since they verify the identity of the person in the probe photo by comparing it to a photo already labeled with that identity), whereas 1:N algorithms are referred to as "identification" algorithms (since they identify individuals by comparing a probe photo with a searchable database of many labeled photos). See Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*," December 2019, https://doi.org/10.6028/NIST.IR.8280, pp. 4–5.

The accuracy of a FR algorithm is therefore usually expressed in terms of the rates of either *false positives* or *false negatives*, where a false positive occurs any time the algorithm matches (on the basis of the similarity scores) two images of different people, and a false negative any time the algorithm fails to match two images of the same person. While a perfect FR algorithm would produce neither false positives nor false negatives, in practice these types of errors must be balanced against one another by deciding on an appropriate confidence threshold: setting a higher confidence threshold will, all else being equal, produce fewer false positives, but will produce many more false negatives, whereas setting a lower similarity threshold will have the opposite effect.[39]

The most recent and largest-scale audit of commercially available FR algorithms is the ongoing Facial Recognition Vendor Test (FRVT) performed by the U.S. Department of Commerce's National Institute of Standards and Technology.[40] This audit examines hundreds of distinct FR algorithms. According to the data from the FRVT, the most accurate commercially available 1:N FR algorithms produce false negatives between 2–3 times in 1,000 when the confidence threshold is set to allow 3 false positives for every 1,000 matches.[41] NEC, whose FR software was licensed to the Toronto Police Services, had algorithms that had the 3rd and 4th lowest error scores as part of the NIST audit; Cognitec and Vigilant Solutions, two FRT developers frequently mentioned in the context of American law enforcement FRT, were found to have error rates roughly 20 times higher than NEC's.[42]

When 1:N searches are used by law enforcement to produce investigatory leads, however, the output is often a collection of possible matches ranked based on their similarity score, rather than a single match (provided their similarity scores reach a set threshold). Human verification is then required as a second step: someone must review the set of possible matches to determine whether they present viable leads or not.[43] In these cases, where a number of non-matches are included in the output by design, the algorithm's accuracy rate is evaluated in terms of either the the false positive identification rate for the top-ranked result (FPIR), or the false negative

---

[39] Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders & Beyond.* Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, September 2020, pp. 31–32.
[40] National Institute of Standards and Technology, *NIST Face Recognition Vendor Test (FVRT) Ongoing.* https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing.
[41] *ibid*.
[42] *ibid*.
[43] Patrick Grother, et al., "Face Recognition Vender Test (FRVT) Part 2: Identification, *NISTIR 8271 Draft Supplement*," December 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

identification rate (FNIR), calculated as the percentage of searches for which there was a match in the database that the algorithm failed to rank above a certain threshold.[44]

It is important to note, however, that the FRVT found that algorithm accuracy depends to a high degree on the quality of the images used. Where mugshots are used as the probe image, and compared to a database of mugshots, the top-performing algorithms find matches (when present in the database) with an FNIR of roughly 0.1%.[45] Where such high-quality images are not used—including cases where "wild" images (photos taken in uncontrolled settings) were used—error rates can exceed 20%.[46] There is also a considerable range in accuracy scores across all the audited algorithms.[47]

2.2 Systematic biases: race, gender and age

As part of the FRVT, the NIST studied the relationship between the demographic characteristics of pictured individuals and the accuracy of FR algorithms in matching them against the database of images. Unfortunately, they found what other researchers have increasingly documented: FR algorithms are significantly poorer at distinguishing, classifying and identifying darker-skinned faces than lighter-skinned faces, do worse with female faces than with male faces, and do worse with the faces of the elderly or young people than with those who are middle-aged.[48]

In particular, the NIST report found that searches using images of West and East African people or of East Asian people resulted in an FPIR roughly 100 times higher than when using images of Eastern Europeans. Using images pulled from domestic (U.S.) law enforcement, "the highest false positives are in American Indians, with elevated rates in African American and

---

[44] *Ibid*., p. 21. Because the FRVT is conducted as an "open-set search," it is not predetermined that every search will have a match for the probe image in the dataset (which is meant to mimic real-world investigatory experience, where a suspect may have no prior criminal record, for e.g.). In the case where there is no matching image in the database, the correct result for the algorithm is to fail to produce any matches with similarity scores above the threshold. See discussion on p. 14. See also Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders & Beyond.* Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, September 2020, pp. 34–35.
[45] Patrick Grother, et al., "Face Recognition Vender Test (FRVT) Part 2: Identification, *NISTIR 8271 Draft Supplement*," p. 3.
[46] *Ibid*., p. 3.
[47] *Ibid*., p. 38; see also *NIST FRVT 1:N Leaderboard*. https://pages.nist.gov/frvt/html/frvt1N.html.
[48] Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*," pp. 2–3.

Asian populations; the relative ordering depends on sex and varies with algorithm."[49] The same study found that the FPIR was higher with female as opposed to male faces, though this effect was less pronounced than the racial bias.[50] Similarly, there were higher FPIRs when using images of elderly people or children.[51] It is worth noting here that the NIST study did not use "wild" images taken either from the internet or from surveillance footage, meaning that the false-positive effects they found were present when using very high-quality images.[52] These results agree with a growing body of academic literature regarding the impact that demographic characteristics—race and gender, in particular—have on the accuracy and effectiveness of FRT.[53]

The problem of racial bias in facial analytic software extends to more broadly familiar territory: both Google[54] and Twitter[55] have recently been found to employ facial analytic tools that fail to accurately identify non-white faces.

While it is broadly hypothesized that some of these effects are determined by the racial and gender composition of the image databases on which the FR algorithms are trained,[56] there is also increasingly evidence that the way in which cameras capture images of darker-skinned faces plays an important role in determining the efficacy and accuracy of FR algorithms (by systematically producing images that FR algorithms are worse at handling).[57]

---

[49] *Ibid*., p. 2.
[50] *Ibid*., p. 2.
[51] *Ibid.*, p. 2.
[52] *Ibid.,* p. 9.
[53] See, for e.g., Joy Buolamwini, Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification"; Krishnapriya K.S. et al., "Characterizing the Variability in Face Recognition Accuracy Relative to Race," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2019; Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition In America*, October 18, 2016, https://www.perpetuallineup.org/.
[54] Jana Kasperkevic, "Google says sorry for racist auto-tag in photo app," *The Guardian*, July 1, 2015. https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app.
[55] Alex Hern, "Twitter apologises for 'racist' image-cropping algorithm," *The Guardian*, September 21, 2020. https://www.theguardian.com/technology/2020/sep/21/twitter-apologises-for-racist-image-cropping-algorithm.
[56] See Joy Buolamwini, "When the Robot Doesn't See Dark Skin," *New York Times*, June 21, 2018. https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html. See also Steve Lohr, "Facial Recognition is Accurate, If You're a White Guy," *New York Times*, Feb. 9, 2018. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html; Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders & Beyond*, p. 41. It is also noted in Patrick Grother, et al., "Face Recognition Vender Test (FRVT) Part 2: Identification, *NISTIR 8271 Draft Supplement*," that with FR algorithms developed in China, the race-based effects were reversed and the algorithms performed better with East Asian faces (p. 2).
[57] Cynthia M. Cook et al., "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, Jan. 2019, pp. 32–41; Sarah Lewis, "The Racial Bias Built into Photography," *New York Times*, April 25, 2019. https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html. This has also become an issue in schools during the Covid-19 pandemic, as facial analytic software is being used in some cases to help conduct online examinations. See Joe Friesen, "Use of surveillance software to crack down on

One group of researchers, including Joy Buolamwini (a leading scholar on AI ethics)[58], however, have raised the concern in a recent paper that relying on audits like the NIST's FRVT to help regulate which FR algorithms can be used either by private or public organizations introduces new ethical problems.[59] One such problem concerns the commercial response to published audits: the authors argue that commercial FR vendors may "overfit" their algorithms to the specific tasks performed as part of the audit rather than addressing the fundamental biases at work, noting that, in a study conducted for their paper, Amazon and Microsoft performed significantly better on the task of gender classification on which they had been previously audited by Buolamwini and Gebru, but performed poorly on related but distinct tasks.[60] One other problem concerns the collection of representative image datasets (or 'benchmarks'): since one likely cause of racial biases in FRT is the under-representation of dark-skinned faces in the datasets used to train FR algorithms, there is a need to supplement existing datasets with images of members of marginalized communities. Attempts to do so, however, introduce new risks of privacy violations (since it is personal information that is being collected at large scales) and exploitation.[61] For example, a FR company based in China signed a deal with the government of Zimbabwe to "harvest the faces of millions of citizens through unprecedented access to their CCTV cameras, smart financial systems, airport, railway, and bust station security, and a national facial database,"[62] partly in order to get access to more dark-skinned faces on which its FR algorithms could be trained to eliminate racial bias.[63]

---

exam cheating has unintended consequences," *Globe and Mail*, December 16, 2020. https://www.theglobeandmail.com/canada/article-use-of-surveillance-software-to-crack-down-on-exam-cheating-has/.

[58] Joy Buolamwini is the founder of the Algorithmic Justice League, an organization aimed at raising awareness of the ways in which AI can harm marginalized groups: https://www.ajl.org/. In addition to authoring and co-authoring studies on racial bias in FRT, cited in this report, she has also given testimony to the House Committee on Oversight and Reform during a hearing on the impact FRT has on Americans' civil liberties: https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

[59] Inioluwa Deborah Raji et al., "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing," Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. February 2020, pp. 145–151. https://dl.acm.org/doi/10.1145/3375627.3375820.

[60] *Ibid*., p. 147. See also Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."

[61] Julia Carrie Wong, "Google reportedly targeted people with 'dark skin' to improve facial recognition," *The Guardian*, October 3, 2019. https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color

[62] Raji et al., "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing," p. 147.

[63] Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, July 24, 2018. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

2.3 Quality of Input Image (editing, using sketches, "wild" photos)

In addition to the documented race, gender and age-based biases affecting the accuracy of FRT, the quality of the input or probe image has a significant impact on accuracy. For instance, the NIST's FRVT found that using images captured by kiosks not originally designed for facial recognition—where the faces captured were frequently cropped at the edges or at a significant downward pitch relative to the camera—led to a 20% higher error rate relative to searches run with mugshots.[64] We should therefore expect higher error rates in general where FR algorithms are using probe images taken from the "wild," or are searching a database of such images, in addition to the privacy concerns such searches present (as was the case with Clearview AI).

Clare Garvie's report *Garbage In, Garbage Out*, however, finds evidence in the context of American policing of investigators using either digitally edited images, forensic or composite sketches, or celebrity look-alike photos as the probe images in FR searches when higher-quality images of suspects are not available.[65] At least three FRT vendors—Amazon, Cognitec and Vigilant Solutions—currently advertise, or have done so in the past, that their FR algorithms work with forensic or composite sketches used as inputs.[66] Despite these claims, a study conducted in 2013 found that the *success* rate when conducting searches using sketches as probe images ranged between 4.1–6.7%.[67] Accordingly, Garvie concludes: "The most likely outcome of using a forensic sketch as a probe photo is that the system fails to find a match… But this practice also introduces the possibility of misidentification."[68]

The use of digitally altered images and celebrity look-alike photos in the place of high-quality unedited images raises the same general concern as does the use of sketches: in all of these cases, investigators may be drawing conclusions with high degrees of certainty about the identity of a suspect on the basis of information that is only loosely connected to them. For this

---

[64] Patrick Grother, et al., "Face Recognition Vender Test (FRVT) Part 2: Identification, *NISTIR 8271 Draft Supplement*," p. 3.
[65] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, May 16, 2019, https://www.flawedfacedata.com/#art-or-science.
[66] *ibid.*
[67] S. Klum, H. Han, A. K. Jain and B. Klare, "Sketch based face recognition: Forensic vs. composite sketches," *2013 International Conference on Biometrics (ICB)*, Madrid, 2013, p. 6.
[68] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*.

reason, police services typically state that FR matches are to be used only as investigative leads, not as positive identification.[69]

In practice, however, FR search results have been transformed from an investigative lead into a positive identification with insufficient rigour. In January 2020, a Detroit man, Robert Julian-Borchak Williams, was arrested for a robbery in October 2018 on the basis of a FR match: Michigan state police ran a FR search using a still from a surveillance video against Michigan's facial recognition database using software purchased from DataWorks Plus, and Mr. Williams' image was included in the results. When these results were sent to Detroit police, Mr. Williams' image was packaged as part of a 6-person photo lineup, and he was identified as the suspect by the loss-prevention contractor who had originally sent the probe image to the Michigan police, solely on the basis of their having seen the surveillance video. Mr. Williams was then arrested, interrogated and held overnight before being released and eventually having the case dismissed.[70]

2.4 Absence of Regulation and Low Barriers to Entry

While it is difficult to arrive at a precise number, there are likely more than one hundred vendors of FRT at present producing algorithms of varying quality.[71] Organizations that purchase FRT, whether public or private, thus face the need to determine the accuracy and sources of error that pertain to the system they plan to use. As the NIST's FRVT study of demographic effects concludes,

> Operational implementations usually employ a single face recognition algorithm. Given algorithm-specific variation, it is incumbent upon the system owner to know their algorithm. While publicly available test data from NIST and elsewhere can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data, perhaps employing a biometrics testing laboratory to assist.[72]

---

[69] *ibid*.
[70] Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
[71] The NIST's FRVT study on demographic effects, conducted in 2019, studied algorithms provided by 99 developers; more have likely arisen since then. See Patrick Grother et al., "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*," p. 1.
[72] *Ibid*., p. 3.

This, however, places a significant and perhaps unrealistic demand on organizations employing FRT, at least absent any regulations or oversight enforcing such a standard.

Moreover, the publicly available test data provided by NIST and others will struggle to provide information on all of the commercially available tools, as it has become increasingly easy to develop FR algorithms. While there are incentives for larger firms with long track records in FR to participate (so that they might advertise their successful results), those same incentives likely do not exist for smaller developers. The risk posed by the proliferation of FR tools is thus that there may be an increasing number of FRT vendors who do not take part in algorithm audits, making their claims regarding the accuracy of their software consequently difficult to evaluate.

The ease with which FR algorithms can now be developed is partly a consequence of the fact that code that was developed for facial recognition purposes is available as an open source resource. The most well-known and widely used such resource is likely FaceNet, a FR system developed by three researchers at Google in 2015,[73] though there is now a variety of open source tools available.[74] When the Office of the Privacy Commissioner of Canada (OPC) released its report on the FRT employed by Cadillac Fairview Corp. Ltd., for instance, it was revealed that the vendor that Cadillac Fairview had purchased facial analytics services from was a firm called Mappedin, who provide interactive mapping services to malls and other public spaces and who had built their facial analytics software on the basis of the FaceNet code.[75]

Conclusion

Despite the significant advances in classification and identification accuracy in recent years, and the proliferation of FRT developers (driven in part by the availability of open source

---

[73] Florian Schroff, Dmitry Kalenichenko, James Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.

[74] See, for e.g., dlib's facial recognition code: http://dlib.net/dnn_face_recognition_ex.cpp.html; see, too, OpenFace, open source software based on FaceNet: https://cmusatyalab.github.io/openface/; see, finally, Adam Geitgey's facial recognition tool, https://github.com/ageitgey/face_recognition, and tutorial, "Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning," *Medium*, https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78.

[75] PIPEDA Report of Findings #2020-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

code), there remain significant concerns regarding the possibility of misidentification. Absent industry regulation (or regulations governing the use of FRT by public and private organizations in Canada), the onus is on those using FRT to a) ensure that the tools they employ are being used in keeping with best practices, and b) understand the sources and likelihood of error associated with the FR system they use, lest the security of all Canadians, but especially those belonging to already marginalized groups, be put at risk.

3. Privacy Concerns Regarding Facial Recognition Technologies in Canada

Introduction:

With the increasing awareness of facial recognition technologies utilized by police forces nationwide, along with the ease of accessing these tools, privacy has once again sprung up as an area of increasing concern. The aim of this section is to provide an overview of the current privacy concerns regarding facial recognition technologies in Canada. A reasonable expectation of privacy will be briefly examined along with current Canadian privacy laws relating to the protection, and security of personal information. The consequences of the collection of private information without consent will be reviewed using the example of the Cadillac Fairview case, in which sensitive biometric data was obtained illegally. The Self Exclusion program administered by the Ontario Lottery and Gaming Corporation (OLG), provides an example of collecting personal information with consent. Finally, an exploration of the private and public sector sharing of facial recognition data with police forces will be examined through the Insurance Corporation of British Columbia (ICBC), use of facial recognition technologies after a riot caused by a hockey game occurred in 2011.[76]

3.1 Reasonable Expectation of Privacy

For decades now, the law has drawn a not-so-clear line between instances where these rights apply and are legally protected and instances where they are not. The reasonable expectation of privacy is the test applied by courts to determine whether or not this line has been crossed and have elected only to intervene where such expectations can reasonably exist. While one would have a reasonable expectation of privacy in terms of their personal finances, they are not to expect the same type of privacy to arise at an airport or other public spaces. It is noteworthy that this seemingly arbitrary distinction has not arisen from the lack of interest for greater privacy protection from the legislature but more as a matter of pragmatism as comprehensive privacy laws have proven particularly elusive and difficult to maintain. That said, as personalized marketing proves more and more lucrative, corporations such as Cadillac Fairview have found unique and innovative ways to try and skirt the privacy laws as they

[76] Office of the Information and Privacy Commissioner for British Columbia, *Investigation into the use of Facial Recognition Technology by the Insurance Corporation of British Columbia,* February 16, 2012. https://www.oipc.bc.ca/investigation-reports/1245

currently exist to capture their consumers' attention. Police forces are also looking for ways to stay ahead of criminals and have resorted to similar high-tech methods such as facial recognition to spot persons of interest. That being said, consent should be at the forefront of most individuals' concerns when it comes to privacy and the collection of their personal information.

3.2 Protection of Individual Privacy

Facial recognition technologies were initially developed as a tool for use in the public sector by government security agencies and law enforcement.[77] Today, the applications of facial recognition technologies seem endless, which naturally raises privacy concerns. In Canada, these technologies are mainly used by provincial licensing and gaming organizations to prevent fraudulent activities, and at the federal level, when issuing passports and other forms of legal identification[78] . All Canadians are protected under two federal laws, which are enforced by the Office of the Privacy Commissioner of Canada, the first being PIPEDA, the Personal Information Protection and Electronic Documents Act.[79] This act applies to the use of personal information as it pertains to commercial activities within the private sector. [80] Commercial activities are defined as "any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.".[81] Organizations that fall within the scope of PIPEDA, have to adhere to many guidelines in relation to the collection of personal information. This includes, but is not limited to, obtaining consent from individuals when their personal information is being collected, used, or disclosed.[82] PIPEDA requires these organizations to provide access to individuals to this information and also allow them to challenge its legitimate

---

[77] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors*, 4-6, March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf.
[78] *Ibid*.
[79] Office of the Privacy Commissioner of Canada, PIPEDA in brief, May 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/; Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada, January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/
[80] Office of the Privacy Commissioner of Canada, PIPEDA in brief, May 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/
[81] *Ibid*.
[82] *Ibid*.

use if they wish.[83] If an organization intends to use the personal information for reasons other than the ones initially described, they are required to obtain consent.[84] PIPEDA also covers all federally regulated businesses within Canada (i.e. banks, airports, telecommunications companies, etc.) which also extend to the territories.[85]

The second federal law that protects Canadians' personal information is *The Privacy Act,* which applies strictly to federal government institutions and the personal information they have acquired.[86] All provinces and territories have their own privacy laws that apply to the handling of private information as it pertains to governmental agencies within their jurisdiction.[87] Three provinces (Quebec, Alberta, and British Columbia) have their own privacy laws for the private sector that apply in place of PIPEDA.[88] To further add complexity to the application of privacy laws, the existence of provincial privacy laws does not exclude the application of PIPEDA within that jurisdiction.

How are these privacy laws applied to facial recognition?

Both PIPEDA and *The Privacy Act* fail to outline appropriate uses of facial recognition. These laws are specific to Canadian companies and private sector organizations, meaning that they may not be able to protect Canadians privacy as intended when companies operate outside of the country which is increasingly the case as the internet has made the necessity of a physical location within a specific territory unnecessary and difficult to ascertain.[89]

3.3 Security of Personal information

The *Privacy Act* covers the use of biometric data by the federal government while PIPEDA deals with the collection, use, and disclosure of personal information as it relates to biometric data for private organizations.[90] The term biometric has evolved gradually over time

---

[83] *Ibid*.
[84] *Ibid*.
[85] *Ibid*.
[86] Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada, January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/
[87] *Ibid*.
[88] *Ibid*.
[89] Hackl, Micheal. "Clearer rules needed for facial recognition technology, " *rabble.ca,* August 6, 2020. https://rabble.ca/columnists/2020/02/clearer-rules-needed-facial-recognition-technology
[90] Office of the Privacy Commissioner of Canada, *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/.

and is currently defined as "... a range of techniques, devices and systems that enable machines to recognize individuals, or confirm or authenticate their identities " by the Office of the Privacy Commissioner of Canada (OPC). [91] Biometric systems have the capacity to quantify and examine individuals behavioural and physical characteristics, which can be stored as data.[92] Biometric information can be gathered from a variety of sources, such as one's facial features, fingerprints, and so on.[93]

The OPC is currently working with the provinces and territories to develop new regulations surrounding the use and collections of biometric data.[94] One key concern related to facial recognition is the covert collection of biometric data, as was the case in the Cadillac Fairview controversy mentioned previously.[95] Faces are a form of biometric data that is publicly available--that is, our faces are visible for the most part when we move through public and private spaces--which makes its collection easy to obtain without the knowledge of the targeted party.[96] The relative ease by which this data is obtained raises subsequent and related issues of 'cross-matching' and the use of information for a secondary purpose. Cross-matching biometric data (i.e. a photo) occurs when the data gathered is compared against an existing database without the consent of that individual.[97] Secondary information collection is the harvesting of biometric data for one purpose (often with consent), and using that information to make inferences beyond its initial purpose.[98] These concerns have been narrowed down to three privacy principles, which are:[99]

1. Individuals should know that their personal information is being collected;
2. Collection of biometric information should only be used for its original purpose as described to the individual; and
3. Biometric information should only be collected if the reasoning for it is clearly defined.

To protect the personal privacy of individuals, the OPC has established Privacy Impact Assessments (PIAs) and conducts privacy audits when a complaint is brought against a government agency, or other organization when it relates to biometric data collection.[100] PIAs

---

[91] *Ibid*.
[92] *Ibid*.
[93] *Ibid*.
[94] *Ibid*.
[95] *Ibid*.
[96] *Ibid*.
[97] *Ibid*.
[98] *Ibid*.
[99] *Ibid*.
[100] *Ibid*.

examine the implications a program, service, or policy has on individuals' privacy, which is a valuable tool when personal information is being gathered.[101] As of April 1, 2010 a PIA is mandatory as per the Treasury Board of Canada Secretariat's (TBS) *Directive on Privacy Impact Assessment* by government agencies if the use of personal information is required.[102] A PIA is a requirement of all government agencies in which there is a potential to impact an individuals' privacy rights, as per the *PIA Directive,* and publication of the results is mandatory.[103] The PIA is a tool used to assess risk and tries to mitigate potential issues as they relate to the collection of personal information.[104] It attempts to aid in the development of solutions to securely store personal (biometric) data, establishing security clauses as they pertain to the transfer of personal data between entities, and determining appropriate levels of security, etc. [105]

3.4 What access do Facial Recognition Technology (FRT) providers have to public searches and information?

Facial recognition providers have the ability to gather data from a variety of sources to build their databases. In regards to the private sector, companies providing FRT claim that they can access information that is publicly available on the Internet.[106] Companies such as Clearview AI search the open web and pull all the available images and compare them to a customer's photo.[107] In a similar fashion, law enforcement agencies claim the ability to gather images from social media profiles such as Facebook and even have the capacity to obtain photos from dating sites.[108] In addition to this capability, they have established administrative databases with high quality images from various governmental agencies that provide legal documentation (i.e. passports, drivers licenses). Globally, the expansion of databases that store images used for the purpose of facial recognition has experienced massive growth. With this growth privacy concerns regarding these large databases have risen, as the photos in these databases are not restricted to individuals

[101] *Ibid*.
[102] Office of the Privacy Commissioner of Canada,Privacy Impact Assessments: Frequently asked questions, December, 2011. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_33/
[103] Office of the Privacy Commissioner of Canada. Expectations: OPC's Guide to the Privacy Impact Assessment Process, March 2020. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/
[104] *Ibid.*
[105] *Ibid.*
[106] Clearview AI. *Computer Vision for a Safer World*. 2020. https://clearview.ai/
[107] *Ibid.*
[108] Smith, Marcus, Mann, Monique., & Urbas, Gregor. 2018. *Biometrics, crime and security*. London: Routledge, Taylor & Francis Group.

who have had encounters with the criminal justice system.[109] and increased awareness of potential privacy concerns regarding the legality of obtaining biometric data of citizens, especially those who are not part of the criminal justice system.[110] Law enforcement agencies have expanded their databases by combining both publicly available images of individuals and photos used for legal documentation purposes .[111] In Canada, there is no law that explicitly prohibits facial recognition companies from gathering images from public search engines but the privacy risks suggest that a societal conversation about what it means for an image to be "public" is overdue.

3.5 Collection of Personal Information without Consent

Section 5(3) of *PIPEDA* outlines what requirements must be met in order to obtain consent. It states that "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances".[112] This definition does not directly reference facial recognition technologies and leaves room for interpretation, which is why it is meant to be a guiding principle for the courts in conjunction with part one of PIPEDA and with the application of the 'reasonable person lens'.[113] Organizations must provide a reason as to why private information is being gathered, insofar that the collection of it would be determined appropriate considering the situation by a reasonable individual.[114] It is important to note that even if an organization's purpose satisfies the requirements set out in section 5(3), they still have to fulfil other sections of the *Act* to ensure the proper protection of private information.[115] As it pertains to the collection of private information, PIPEDA has outlined six reasons for collection of personal information that they describe as 'no-go' zones, based on experience, and current privacy laws. Taken directly from their website are as follows:[116]

1. Collection, or use or disclosure is otherwise unlawful;
2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law;

[109] *Ibid.*
[110]
[111] *Ibid.*
[112] Office of the Privacy Commissioner of Canada. Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), May 2018. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/
[113] *Ibid.*
[114] *Ibid.*
[115] *Ibid.*
[116] *Ibid.*

3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual;
4. Publishing personal information with the intended purpose of charging individuals for its removal;
5. Requiring passwords to social media accounts for the purpose of employee screening; and
6. Surveillance by an organization through audio or video functionality of the individual's own device

3.6 Example of Collection of Private Information without Consent

Cadillac Fairview Corporation Limited (CFCL) Case

CFCL embedded cameras into their digital directory kiosks in 12 Canadian malls, which harvested biometric information of their patrons.[117] The CFCL case will be examined as it relates to privacy issues, a more in-depth analysis is provided in section four of this report. A joint investigation was launched by the Alberta, BC, and Federal Privacy commissioners, which discovered that customer information was being unlawfully obtained.[118] PIPEDA, British Columbia's *Personal Information Protection Act* (PIPA BC), and Alberta's' *Personal Information Protection Act* (PIPA AB), were applied to this investigation when determining if CFCL was complied with privacy laws.[119] The investigators found that customers were not properly advised of the company's privacy policy, which Cadillac Fairview claimed was posted on decals at all entry points across the mall.[120] These privacy policy postings were deemed as insufficient and that CFCL should have obtained expressed opt-in consent from patrons.[121] It was also discovered the privacy policy was placed in the middle of a 5,000 word document, which mall patrons could not easily access when using the directory, additionally the language used within the privacy policy was deemed to be excessively broad.[122] The investigators concluded that the privacy policy did not warrant sufficient consent for the practices carried out by CFCL, or Anonymous Video Analytics (AVA).[123]

---

[117] Office of the Privacy Commissioner of Canada, *Cadillac Fairview collected 5 million shoppers' images,* October 29, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/
[118] *Ibid.*
[119] PIPEDA Report of Findings #2020-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.
[120] *Ibid.*
[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*

The report also uncovered that sensitive biometric data gathered from these images was being stored in another database by third party software, even though CFCL would delete them from their own servers, an activity which CFCL claimed they had no knowledge of.[124] The CFCL stated they only wanted to gather information on the gender and age of their patrons, and had no intention of using the data collected to identify customers. [125]The investigation revealed additional concerns relating to the accessibility of the collected information by third-parties.The investigation determined that the stored biometric information posed a great risks to customers personal privacy as this data is vulnerable to being accessed by and potentially misused if not maintained securely.[126]

3.7 Examples of Collections of Private Information with Consent

Casinos in Ontario – Use of Biometric Data:

The Ontario Lottery and Gaming Corporation (OLG) created a program known as *Self-Exclusion* to assist individuals with gambling addictions in Ontario.[127]. The OLG, iViewSystems, a provider of facial recognition technologies, and iTrak, a risk management system reached an agreement on April 18, 2011.[128] Individuals who enrol in the program make a written commitment to avoid Ontario gaming facilities, which is meant to assist them with their gambling issues.[129] During the enrolment phase, biometric features are extracted from images captured and uploaded into iView's iGWatch Facial Recognition System.[130] This facial recognition software converts captured images into biometric data to compare to stored information within the iTrak platform in real time.[131] A colour-coded alert is produced by the iGWatch Facial Recognition System, which notifies the operator of when a potential match is found based on the match confidence level.[132] If a match is found the operator is presented with

---

[124] *Ibid.*
[125] *Ibid.*
[126] *Ibid.*
[127] iView Systems, and Ontario Lottery and Gaming Corporation. *IView Systems Awarded Province Wide Contract for Incident Reporting and Facial Recognition*. April, 18, 2011. www.globenewswire.com/news-release/2011/04/18/1358580/0/en/iView-Systems-Awarded-Province-Wide-Contract-for-Incident-Reporting-and-Facial-Recognition.html.
[128] *Ibid.*
[129] *Ibid.*
[130] *Ibid.*
[131] *Ibid.*
[132] *Ibid.*

the individual's photo along with the one in the database, and from there they make the final identification decision.[133]

The OLG Self-Exclusion program is the first real-life application of biometric encryption for a 1:many system.[134] Biometric encryption has emerged as a method to protect sensitive information with the increased awareness of privacy issues that accompany biometric technologies, which does not store any images or templates generated during the data gathering process.[135] This technology can be applied in a variety of ways, but for the purpose of this analysis two methods will be examined. The first, is the attachment of a digital key that corresponds to the biometric data and secondly, the creation of a digital key that is based on the biometric data.[136] In addition to the secure biometric encryption system, the self-exclusion database uses advanced IT techniques such as secure communications and conventional cryptography in an effort to advance system security and privacy.[137] These layers of security, along with the application of a hybrid model make it more difficult to link personal information to other databases without consent from the individual.[138]

The use of a hybrid model, which is the creation of a biometric encryption model to be used within the context of a watch-list, was determined to be the ideal option as provided the OLG self-exclusion program, with the greatest security benefits.[139] A 1:many biometric system is more complex and requires additional processing capabilities.[140] The group of individuals who have registered with the self-exclusion program have their biometric data securely uploaded to a watch-list.[141] A watch-list has a small percentage of a population's biometric data registered and once patrons enter an OLG facility their biometric data is automatically scanned and tested against the database of biometrics on the watch-list. [142] During

[133] iView Systems, and Ontario Lottery and Gaming Corporation. *IView Systems Awarded Province Wide Contract for Incident Reporting and Facial Recognition*. April, 18, 2011. www.globenewswire.com/news-release/2011/04/18/1358580/0/en/iView-Systems-Awarded-Province-Wide-Contract-for-Incident-Reporting-and-Facial-Recognition.html; Information and Privacy Commissioner Ontario. *Privacy by Design Solutions for Biometric One-to-Many Identification Systems.* June 2014. https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf

[134] Information and Privacy Commissioner Ontario. *Privacy by Design Solutions for Biometric One-to-Many Identification Systems.* June 2014. https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf

[135] *Ibid*.

[136] *Ibid*.

[137] *Ibid*.

[138] *Ibid*.

[139] *Ibid*.

[140] *Ibid*.

[141] *Ibid*.

[142] *Ibid*.

the enrollment phase the individual is required to provide a facial image and is assigned a unique enrollee ID, which does not reveal personal information about the member, via a process known as biometric encryption (discussed below).[143] A record of an extracted member's facial features is stored in a vendor-supplied database which then applies a unique biometrically encrypted template to the data (known as 'helper data').[144] When testing the OLG facial recognition technology the correct identification rate reached a maximum of 91% and BE did not significantly reduce the efficiency of facial recognition, but the correct identification rate reduced by less than 1% while the false acceptance rate decreased by 30% to 50%.[145]

3.8 Private/Public Sector Sharing of Information with Police

The Insurance Corporation of British Columbia (ICBC)

The ICBC used facial recognition software to help the Vancouver police department identify rioters after a June 2011 hockey game.[146] This use of FRT was brought to the British Columbia Privacy Commissioner and was determined to be an unlawful use of the ICBC's facial recognition software as it did not meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA), BC's legislation which outlines citizens' privacy rights.[147] The BC Privacy Commissioner determined that the ICBC must immediately stop assisting police with any requests to use their facial recognition technology with a goal of identifying an individual(s) without previously obtaining a court order, subpoena, or warrant.[148]

At the time of the investigation, the ICBC database contained approximately 455,00 British Columbia Identification Cards (BCID) and 3.1 million active drivers licenses images, along with a total of 4.4 million facial recognition templates.[149]

The ICBC gathers its facial recognition data through the *enrolment process*, which occurs when a digital image is captured and specialized software is used to take measurements of the face, along with an analysis of the subjects skin texture.[150] These measurements are converted into an

---

[143] *Ibid*.
[144] *Ibid*.
[145] *Ibid*.
[146] Office of the Information and Privacy Commissioner for British Columbia, *Investigation into the use of Facial Recognition Technology by the Insurance Corporation of British Columbia,* February 16, 2012. https://www.oipc.bc.ca/investigation-reports/1245
[147] *Ibid*.
[148] *Ibid*.
[149] *Ibid*.
[150] *Ibid*.

algorithm and then a binary code which is known as a facial recognition template.[151] The second step of this process is *storage* in which the facial recognition template is uploaded to ICBC's database.[152] The final step of the facial recognition process is *matching,* which occurs when an individual needs to renew or replace an identification card.[153] ICBC will create a new facial recognition template of the individual and compare it to their old template in the system to try and generate a match, therefore using a 1:1 comparison.[154] The assumption is that the facial recognition templates will match if the individual is telling the truth about their identity.[155] During this stage the facial recognition software will assign a score to an individual's template, the higher the score, the greater the likelihood of a match to a template already in the system.[156] In order to ensure the individual does not have multiple identities the ICBC also completes a 1:many comparison.[157]

Privacy issues relating to this case when considering the use of biometric data are the use of individual's bodies as identification tools, and function creep.[158] Collection of biometric data is significant as it impacts our ability to maintain our privacy and control information about ourselves.[159] As facial recognition databases become more interoperable, the potential for the occurrence of a function creep is greater than ever before.[160]

---

[151] *Ibid*.
[152] *Ibid*.
[153] *Ibid*.
[154] *Ibid*.
[155] *Ibid*.
[156] *Ibid*.
[157] *Ibid*.
[158] *Ibid*.
[159] Ibid.
[160] Ibid.

4. Facial Recognition Technology within the Public Sector

Facial recognition technology has been adopted within the public sector by a variety of organizations including those involved in law enforcement and agencies providing identification cards such as passports and driver's licenses.[161] Additionally, it has also been introduced in some casinos by provincial gaming commissions to support voluntary self-exclusion programs for individuals who have identified themselves as having a gaming addiction and requested to be excluded from casinos. The implementation of facial recognition technology by organizations within the public sector is not always transparent which raises serious privacy and accountability concerns. Even after adoption, for most examples of facial recognition technology being used in the public sector, there are not publicly available policies to indicate what safeguards are in place to protect privacy and ensure the technology is being used for limited means. The lack of information regarding the process of deciding to introduce facial recognition technology and policy governing its use once adopted is concerning.

Facial recognition technology is invasive to privacy and therefore whether it is required should depend on an analysis of whether it is reasonable given the circumstances. A report by the Office of the Privacy Commissioner suggested that any institution contemplating using facial recognition technology would need to be able to justify the privacy intrusion and suggested consideration of the following questions: [162]

1) Is the measure demonstrably necessary to meet a specific need?
2) Is it likely to be effective in meeting that need?
3) Would the loss of privacy be proportionate to the benefit gained?
4) Is there a less privacy-invasive way of achieving the same end?

Without sufficient information on why facial recognition was necessary to adopt and limitations on its use once adopted, it is impossible for the public to make an informed decision on whether the use of facial recognition technology is reasonably required in the situation, and if so, whether it is being conducted in an appropriate manner. Without the information to answer these questions, there will continue to be a lack of accountability for public sector organizations choosing to use facial recognition technology.

---

[161] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors*, 4-6, March 2013, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf.
[162] Ibid, 6.

4.1 Law Enforcement

ClearviewAI

Law enforcement agencies including at the municipal, provincial and national level had adopted facial recognition technology. A major concern with the introduction of facial recognition technology by law enforcement agencies is the lack of transparency. This was captured by the use of ClearviewAI by many police forces. ClearviewAI has a reference dataset of about 3 billion facial images that it has collected by unlawfully scraping images from social networking sites without notice or consent.[163]A number of law enforcement agencies such as the Ontario Provincial Police and the RCMP eventually admitted to using ClearviewAI after first denying its use.[164] (A table of the list of law enforcement agencies reported to have used Clearview AI is included below.) Officials in charge of various municipal police forces (e.g. Calgary, Edmonton, Toronto, etc.) had indicated they were unaware that their own officers were using ClearviewAI as many officers had gotten access to a free trial of ClearviewAI at a conference. The fact that officers felt they were able to use this facial recognition technology without explicit permission highlights the lack of transparency and accountability that exists. While after the use was revealed, various chiefs of police forces ordered their officers to stop using ClearviewAI, the absence of enforcement of clear policy that prohibits use of facial recognition technology that has not been officially approved puts citizens at risk of having their rights violated until mistakes are uncovered by journalists.

Law Enforcement using Clearview AI

Alberta	**Calgary Police Service** In February 2020, it was revealed that two officers in the Calgary Police Service had used Clearview AI.[165] While the Calgary Police Service stated they do not use Clearview AI in an official capacity, two officers tried the system to explore its potential usefulness for investigations. The Calgary
	Edmonton Police Service

[163] Tamir Israel, "Facial Recognition at a Crossroads: Transformation at our Borders and Beyond." *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC),* 124-5, (2020).
[164] Catharine Tunney, "RCMP denied using facial recognition technology - then said it had been using it for months," *CBC News*, March 4, 2020, https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266.
[165] Robson Fletcher, "Calgary police now admit 2 officers used controversial Clearview AI facial-recognition software," *CBC News*, February 28, 2020, https://www.cbc.ca/news/canada/calgary/calgary-police-admit-using-clearview-ai-facial-recognition-software-1.5480803.

	Police Service indicated the software had not been used in active investigations and the individuals were told to delete their accounts.
	In February 2020 it was reported that three "fairly senior" officers within the Edmonton Police Service had used Clearview AI.[166] These officers within a specialized investigation unit had signed up for Clearview AI in December 2019 after learning about it at a conference. Supt. Warren Driechel, head of the Edmonton Police Service indicated it was only used once in a "limited capacity" during an auto-theft investigation. Chief Dale McFee has directed members of the force to stop any use of Clearview AI. The Edmonton Police Service launched an internal investigation into the use of Clearview AI and a review of policies that guide FRT use.
British Columbia	**Vancouver Police Department** The CBC reported in January 2020 that the Vancouver Police Department stated it had never used Clearview AI and that it had no intention of using it.[167] In early March 2020, spokesperson for the Vancouver Police Department, Sergeant Aaron Roed, confirmed Clearview AI had been used by a detective in the Internet Child Exploitation team.[168] The detective had created a free 30-day trial Clearview AI police-only account following a workshop in Ontario. Roed said only one search was conducted during the child abuse investigation which was unsuccessful following which the account was cancelled.
Nova Scotia	**Halifax Police** Halifax police confirmed a specialized investigator had used Clearview AI but stated they are no longer use Clearview AI.[169] A free trial of the app was tested by an officer on open source data searches.
Ontario	**Durham Region** Durham Regional Police have confirmed officers used trial version of Clearview AI and have directed officers to stop use.[170]

[166] "Officers used Clearview AI facial recognition technology, Edmonton Police Service admits," *CBC News*, February 28, 2020, https://www.cbc.ca/news/canada/edmonton/edmonton-police-artificial-intelligence-facial-recognition-1.5480680.
[167] "Toronto police admit using secretive facial recognition technology Clearview AI," *CBC News*, February 13, 2020, https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785.
[168] "The end of anonymity? Facial recognition app used by police raises serious concerns, say privacy advocates," *CBC News*, January 21, 2020, https://www.cbc.ca/radio/thecurrent/the-current-for-jan-21-2020-1.5434328/the-end-of-anonymity-facial-recognition-app-used-by-police-raises-serious-concerns-say-privacy-advocates-1.5435278.
[169] Zane Woodford, "Halifax police used controversial facial recognition technology," *The Chronicle Herald*, February 28, 2020, https://www.thechronicleherald.ca/salt/halifax-police-used-controversial-facial-recognition-technology-417130/.
[170] Wendy Gillis and Kate Allen, "OPP confirms use of controversial facial recognition tool Clearview AI," *Toronto Star*, March 1, 2020, https://www.thestar.com/news/canada/2020/03/01/opp-confirms-use-of-controversial-facial-recognition-tool-clearview-ai.html.

	Halton Police In February 2020, the CBC reported that the Halton police had been utilising a free trial of Clearview AI since October 2019.[171] Constable Ryan Anderson indicated that following the expiration of the free trial, they are conducting an internal evaluation of the app.
	Hamilton Police Although the initial response from the Hamilton Police to a freedom of information request indicated they did not use Clearview AI or have related marketing materials, a revised letter within a month from the Hamilton Police Service freedom of information branch indicated that through a trial period, the Hamilton Police Service had been given access to Clearview AI.[172] Officers obtained log-in credentials for a trial after attending a law enforcement convention. Deputy Chief Frank Bergen directed members to stop use of the app. The letter indicates the tool was not used for investigative purposes. Officers were reportedly looking at the app to understand it's capacities. Bergen stated that other than the Clearview AI trial, Hamilton Service does not use FRT.
	Niagara Regional Police Like many other municipal police services, after initially denying use of Clearview AI, the Niagara police released a corrected statement indicated they had receive free access to Clearview AI for a trial.[173] Stephanie Sabourin, spokesperson for Niagara officers indicated that Clearview AI was researched by officers to understand the capabilities and limitations and used in a limited capacity. She indicated that trial use was suspended once the issue of its lawfulness were brought up and it is no longer in use by members of the service.
	Ottawa Police In March 2020, after discovering members of the force's Internet Child Exploitation Unit had Clearview AI accounts, the Ottawa Police Service launched a poll of all members to determine how many had signed up.[174]
	Peel Regional Police Service In February 2020, the CBC reported that Peel Regional Police said they were provided with a demo version of Clearview AI for testing purposes but that the Chief has instructed testing be stopped until an assessment by

[171] Kelly Bennett, "Hamilton police tested controversial facial recognition technology Clearview AI," *CBC News*, February 20, 2020, https://www.cbc.ca/news/canada/hamilton/the-service-says-it-has-not-used-the-tool-for-any-investigative-purposes-1.5470359.
[172] Ibid.
[173] Ibid.
[174] Wendy Gillis and Kate Allen, "OPP confirms use of controversial facial recognition tool Clearview AI," *Toronto Star*, March 1, 2020, https://www.thestar.com/news/canada/2020/03/01/opp-confirms-use-of-controversial-facial-recognition-tool-clearview-ai.html.

	the province's privacy commissioner's office is completed to ensure use of the FRT complies with privacy legislation.[175] Ontario Privacy Commissioner Brian Beamish stated he would be consulting with Peel Regional Police to examine its use of FRT and use by other forces.
	Toronto Police Service In February 2020 it was revealed members of the Toronto police had used Clearview AI. This announcement came after the Toronto Police had denied using Clearview AI just the month before in January.[176] Spokesperson for the Toronto Police, Meaghan Gray indicated in February 2020 that members of the Toronto Police had used Clearview AI since October 2019.[177] Details regarding how often it was used or for what purposes were not revealed. She stated that upon becoming aware of its use on 5 February 2020, Chief Mark Saunders ordered officers to stop using the app. No indication as to who had originally approved officers using the app or how Chief Saunders became aware of its use was given. The Toronto Police Services Board said they were not aware members of the force were using Clearview AI.[178] Buzzfeed reported that despite using free trials, the Toronto Police Service ran over 3,400 searches on more than 150 accounts.[179] Gray stated that the Toronto Police have asked the Ontario Information and Privacy Commissioner if Clearview AI is an appropriate investigative tool and will not utilise Clearview AI until a review of the project is completed.[180]
	York Regional Police Despite denying claims of use of Clearview AI on 12 February 2020, on 28 February 2020, York regional police admitted that some York police officers had used a free trial of the app without the knowledge or authorization of leadership.[181] Sergeant Andy Pattenden stated upon learning officers were using Clearview AI, they were directed to stop using the trial version immediately. He indicated there is an internal inquiry to identify how many officers used Clearview AI and in what units. He also said York Regional Police is waiting to hear from the Ontario Information and Privacy Commission for further directions. Until
Ontario Provincial Police	

[175] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[176] Supra note 168 "The end of anonymity?"
[177] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[178] Ibid.
[179] Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," *Buzzfeed News*, February 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[180] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[181] Jeremy Grimaldi, "York police officers used facial recognition technology without permission: YRP spokesperson," *York Region*, February 28, 2020, https://www.yorkregion.com/news-story/9869682-york-police-officers-used-facial-recognition-technology-without-permission-yrp-spokesperson/.

	receiving further information from the Privacy Commission, he stated all members have been told to cease use of any facial recognition technology.
	The CBC reported in January 2020 when asked, the Ontario Provincial Police said they used facial recognition technology but refused to specify the tools they used.[182] After repeated inquiries from The Star as to whether the OPP uses Clearview AI, the OPP launched an internal review in February 2020.[183] In March 2020, CBC reported that the Ontario Provincial Police had been using a free online trial of Clearview AI since December 2019.[184] A free trial was obtained by officers attending a conference and thus did not go through the normal evaluation process the OPP uses when introducing a new software. [185] It was used by officers in four units: child sexual exploitation, anti-human trafficking, digital forensics and cybercrime. Clearview AI helped identify victims and assisted in an investigation that identified and charged a suspect. The OPP has directed officers to stop using Clearview AI and is in contact with the Office of the Information and Privacy Commissioner of Ontario.[186]
National	**Royal Canadian Mounted Police** The Ottawa Citizen reported that the RCMP refused to answer whether it had used Clearview AI—the statement by the RCMP indicated the RCMP would not comment on specific investigative tools or techniques.[187] The CBC reported on 4 March 2020, that despite denying use of FRT on 17 January 2020, the RCMP had in fact been using FRT for months.[188] Following a hack of Clearview AI's client list, the RCMP stated it had used Clearview AI technology for at least four months. Buzzfeed reported that the Royal Canadian Mounted Police was a paying customer of Clearview AI, unlike many other law enforcement agencies in Canada that although using Clearview AI used free trials.[189] Clearview AI was confirmed to be used by the child exploitation unit as well as to "enhance criminal investigations" in a few other units, details unspecified. It has been used in at least 15 child exploitation investigations.[190] Spokesperson Catherine Fortin indicated the RCMP headquarters was looking into which units had been using Clearview AI. She emphasized the RCMP was only using Clearview AI within ongoing criminal investigations, primarily for victim identification and not on members of the public.

[182] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[183] Supra note 170 "OPP confirms use of controversial facial recognition tool."
[184] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[185] Supra note 170 "OPP confirms use of controversial facial recognition tool."
[186] Supra note 167 ""Toronto police admit using secretive facial recognition technology."
[187] Shaamini Yogaretnam, "Ottawa police piloted controversial facial recognition software last year," *Ottawa Citizen*, February 14, 2020, https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-last-year.
[188] Supra note 167 "Toronto police admit using secretive facial recognition technology."
[189] Supra note 179 "Clearview's Facial Recognition App."
[190] Supra note 167 ""Toronto police admit using secretive facial recognition technology."

	The federal Office of the Privacy Commissioner has opened an investigation into RCMP use of FRT to determine if use violates federal privacy laws.[191] The RCMP has said it will collaborate with the federal Privacy Commissioner regarding guidelines for FRT use under Canadian law.

NeoFace Reveal

Beyond ClearviewAI, three municipal police forces have indicated use of NeoFace Reveal, an FR tool developed by NEC Corporation. First adopted by the Calgary Police Service, it has also been used by the Toronto Police Service and tested by the Ottawa Police Service. In comparison the ClearviewAI, the NeoFace Reveal system was used to compare images to a mugshot database rather than a database scraped from the internet. While this addresses some privacy concerns as the systems are used on lawfully obtained photos, there remains concerns about the use of the facial recognition technology as grounds for arrest or harassment, and about the nature of mugshot databases, grounded in over-policing of racialized minorities. For example, the Toronto Police indicated facial recognition technology is used to identify potential candidates but arrests are only made after further evidence is collected; without sufficient accountability mechanisms, this remains a serious concern.[192]

Calgary Police Service

In 2014 the Calgary Police Service was the first police force to begin using the NeoFace Reveal Facial recognition system from NEC Corporation of America.[193] It purchased the FRT as an investigative tool to compare photos and videos from video surveillance against the internal mugshot database which contained roughly 300,000 as of 2019.[194] Staff Sergeant Gordon MacDonald with Calgary's criminal identification unit indicated FRT helps save officers time in matching a suspect to a mugshot.[195] He noted that there are strict rules for using the system—it

[191] Ibid.

[192] Kate Allen and Wendy Gillis, "Toronto police have been using facial recognition technology for more than a year," *Toronto Star*, May 28, 2019, https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html?rf.

[193] "Facial recognition software to aid Calgary police in future investigations," *CBC News*, November 3, 2014, https://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1 .2822592.

[194] Supra note 192 "Toronto police have been using facial recognition technology for more than a year."

[195] David Burke, "Use of facial recognition technology by police growing in Canada, as privacy laws lag," *CBC News*, February 10, 2020, https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749.

can only be used to compare images to mugshots. The current mugshot database is just for Calgary and has roughly 300,000 images. MacDonald also suggested a national database of mugshots would be useful, a move which would create cascading concerns; even without such a database however there is a risk police departments will informally share information resulting in a de facto national database.

Toronto Police Service

The Toronto Police have adopted facial recognition technology provided by the NEC system. The Toronto Police purchased a facial recognition system in March of 2018 for $451,718 plus annual maintenance and support costs.[196] After the 12 month warranty expired, a maintenance and support contract was put in place for 5 years until 2023.[197] The Toronto Police said the use of FRT was to compare images of potential suspects from public or private cameras to an internal database of approximately 1.5 million mugshots. Searches return a series of candidate photos which a trained analyst then manually reviews to determine if the person matches the candidate photo. Prior to adoption of the system, between September 2014 and September 2015 a pilot project was conducted where the team using the facial recognition system received training at the FBI's Criminal Justice Information Services. During the pilot project, over 1000 suspect images were processed but about 400 could not be searched due to poor photo quality. Of the remaining images, it was reported 281 potential matches were identified which helped lead to identification and arrests in a number of major and violent criminal offences.

The Privacy Impact Assessment reports that service investigators do not require a search warrant to request a facial recognition search.[198] Only the six individuals trained by the FBI have access to the secure system and it is only used for searches on the lawfully obtained mugshot database. In his report, Chief Saunders noted that facial recognition is used as a tool to identify potential candidates but that arrests are only made after further evidence is collected through additional investigation (unlike fingerprint matches). Therefore, an exact estimate on the number of arrests resulting from use of facial recognition technology is not available. Between March and December 2018, 1,516 facial recognition searches were conducted with about 5000 still and video images. The system found potential mugshot matches for about 60% of the images with

[196] Supra note 192 "Toronto police have been using facial recognition technology for more than a year."
[197] Toronto Police Services Board, *Public Meeting Agenda*, 244-247, May 30, 2019.
[198] Ibid.

about 80% of these matches leading to identification of offenders. Saunders reported that FRT helped conclude multiple investigations including four homicides, sexual assaults, armed robberies and gang related crimes. Saunders and Staff Inspector Stephen Harris, Forensic Identification Services emphasized Toronto police does not use real-time facial recognition technology and lacked legal authority to do so. Images captured through police body-worn cameras could only be used if a suspect was caught committing a criminal offence on camera and investigators would be required to seek a court's permission before using the FRT.[199]

Ottawa Police Service

The Ottawa Police Service tested NeoFace Reveal, but are reported to no longer be using it.[200] The Ottawa Citizen reported that Ottawa Police had tested FRT in a pilot project ending in March 2019.[201] The Ottawa Police Service used FRT to compare photographs of persons of interest in criminal investigations to an existing database. Deputy Chief Uday Jaswal indicated the pilot program was intended to examine whether the FRT could assist in criminal investigations and to identify technological and procedural challenges as well as privacy and ethical challenges that would come with utilising FRT. No indication has been given as to whether the FRT pilot program led to arrests or charges was given.

Police Services in the Process of Securing Facial Recognition Technology

Some police services are reported to be in the process of securing facial recognition technology. The Edmonton Police Service has indicated they are looking into purchasing facial recognition technology and the Alberta's privacy commissioner is encouraging them to seek oversight in the form of a privacy review to ensure the program complies with privacy law.[202] Edmonton Police has indicated they have not yet secured a licensing agreement with a company and that they are not looking into Clearview AI. Additionally, York Regional Police have demonstrated interest in investing resources in securing FRT. In 2019, $1.68 million was allocated for a "Facial Recognition and Automated Palm and Fingerprint Identification system"

[199] Supra note 192 "Toronto police have been using facial recognition technology for more than a year."
[200] Supra note 167 "Toronto police admit using secretive facial recognition technology."
[201] Supra note 187 "Ottawa police piloted controversial facial recognition software."
[202] Jordan Omstead, "Caution urged as Edmonton police explore facial recognition technology," *CBC News*, February 5, 2020, https://www.cbc.ca/news/canada/edmonton/caution-urged-as-edmonton-police-explore-facial-recognition-technology-1.5451823.

in the York Regional Police budget.[203] According to a York Police spokesperson, they are in the process of purchasing FRT with the intention of comparing images and videos within the lawful possession of York Regional Police and that are connected to specific investigations.[204] Motorola solutions Canada Inc., VERITONE, AIH Technology Inc., and Morpho Canada Inc. are listed as the companies who have submitted bids to supply York Regional police with FRT.[205] Finally, at the provincial level, Surete du Quebec recently finalized a contract at the end of August 2020 with IDEMIA Identity & Security Canada Inc for $4.4 million—this is the Canadian subsidiary of a French company with facial recognition technology software.[206]

4.2 Federal Agencies

On a national level, a number of federal agencies utilise facial recognition technology. Again, there is limited publicly available information on what facial recognition technologies are used and for what specific purposes.

Canada Border Services Agency

Primary Inspection kiosks are used at border control checkpoints.[207] Individuals with a machine readable biometric passport can scan their passport at the Kiosk which will extract the relevant facial and identifying information. The kiosk then takes a static digital photograph of the individual. This new static digital photograph of the individual is compared to the passport using facial recognition technology to verify identify. Additionally, Canada and the US have discussed using FRT with databases of images from both countries as part of the perimeter security initiative.[208]

---

[203] Regional Municipality of York Police Services Board, *Revised Agenda Public Session*, November 7, 2018, http://www.yrpsb.ca/usercontent/meetings/2018/nov/Merged_Agenda_Package_-_Public_Board_Meeting_Nov07_2018.pdf.
[204] Nathan Munn, "Police Forces in Canada Are Quietly Adopting Facial Recognition Tech," *Vice News*, June 23, 2020, https://www.vice.com/en/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech.
[205]"Facial Recognition Software Bid," York Regional Police, https://web.archive.org/web/20200618131043/https://yrp.bidsandtenders.ca/Module/Tenders/en/Tender/Detail/14d004d2-1270-4cbd-89cd-a13d58a5bf27.
[206] Kevin Dougherty, "Quebec lawmakers raise the alarm over police use of facial recognition," *iPolitics*, September 22, 2020, https://ipolitics.ca/2020/09/22/quebec-lawmakers-raise-the-alarm-over-police-use-of-facial-recognition/.
[207] Tamir Israel, "Facial Recognition at a Crossroads: Transformation at our Borders and Beyond." *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC),* 1-16, (2020).
[208] Supra note 1, "Automated Facial Recognition."

Passport Canada's Facial Recognition Project

Passport Canada uses FRT to detect fraud among passport applicants such as if an individual applies for passports under multiple names.[209] The Facial Recognition Project was first piloted in 2004 and currently operated by IRCC. Initially, a one-to-many system was used to generate 10 of the most likely matches and a human operator would make a final decision of whether any image matched the applicant. The Office of the Privacy Commissioner made a series of recommendations to mitigate risks of the program some of which have been adopted.[210]

4.3 Provincial Agencies Outside of Law Enforcement

Driver's Licenses

A number of provinces use FRT when issuing driver's licenses and photo identification cards to combat identify theft or people from securing multiple ID cards. In 2013, the Office of the Privacy Commissioner reported provinces including Ontario, British Columbia and Manitoba use FRT to detect fraud in driver's licenses.[211] In 2016, facial recognition software was introduced in Saskatchewan by SGI Canada while issuing driver's licenses and photo identification cards.[212] The President and CEO of SGI stated FRT would enhance security for customers as the FRT would protect residents from identity theft. When a photo is input in the facial recognition system, the template of the photo created is compared to the individual's previous photo (if they had a previous driver's license on file) and then to all other photos in the database to confirm the photo is not linked to other customers. The contract for incorporating FRT into driver's licenses in Saskatchewan was awarded to Veridos Canada Inc who began producing driver's licenses for the province in April 2016.

In Atlantic Canada, provinces including Nova Scotia, Prince Edward Island and Newfoundland and Labrador also use FRT to confirm the identity of individuals when producing drivers licenses or government issued photo ID cards.[213] The picture of the individual taken is compared to previous pictures of the individual on file and to other pictures in the database to verify identity. These measures are intended to reduce identity theft and prevent suspended

[209] Ibid.
[210] Ibid.
[211] Ibid.
[212] "Facial recognition will go live on Aug. 24," Saskatchewan Government Insurance, last modified August 17, 2016, https://www.sgi.sk.ca/news?title=facial-recognition-will-go-live-on-aug--24.
[213] "The Facts about Facial Recognition," New Brunswick Ombudsperson, https://www.ombudnb.ca/site/latest-news/the-facts-about-facial-recognition.

drivers from seeking a driver's license. The Information and Privacy Commissioners for Nova Scotia, Prince Edward Island and Newfoundland and Labrador have questioned the safeguards in place to protect information and have committed to monitoring the programs.

Casinos

Facial recognition technology has been used in casinos since the early 2000s. An investigation by the Office of the Information and Privacy Commissioner examined the use of facial recognition technology in Ontario casinos by the OPP in 2001.[214] The Biometrica Systems, Inc system provided a database that included known or suspected casino cheats and allowed casinos within North America to send information to each other. The Alcohol and Gaming Commission of Ontario (AGCO) is responsible for ensuring there is no criminal activity in Ontario casinos. To use the system, an officer must have had a reasonable suspicion an individual is engaged in criminal activity. The officer could then use the system to determine if the individual is a known or suspected casino cheat based on 1) the database of 800 faced provided by Biometrica Systems, Inc or 2) the OPP's own database of individuals convicted or being investigated for cheating in casinos.

Every time the system is used, officers are required to compile an incident report and the facial scan is only retained if the investigation found illegal activity. The OPP was reported to not send facial scans they conducted to law enforcement agencies or casinos in other jurisdictions or to Biometrica Systems, Inc. The investigation stated the OPP does not scan all casino patrons (about 5 scans/million patrons). As part of the conclusions of the investigation, the Office of the Information and Privacy Commissioner found that the AGCO should provide proper notice of the collection of personal information (i.e. that facial recognition technology was being used in the casinos). In the report's recommendations it is suggested that *"all government institutions, including law enforcement agencies should consult with the Office of the Information and Privacy Commissioner before launching any initiative or program that involves the use of biometric technology"*.

[214] Information and Privacy Commissioner Ontario, *The Use of Biometric Face Recognition Technology in Ontario Casinos*, February 26, 2001, https://www.canlii.org/en/on/onipc/doc/2001/2001canlii26269/2001canlii26269.html?searchUrlHash=AAAAAQATZmFjaWFsIHJlY29nbml0aW9uIAAAAAAB&resultIndex=1.

More recently, a 2013 report by the Office of the Privacy Commissioner of Canada reported FRT continues to be used in casinos to detect known criminals but also in a voluntary self-exclusion program offered by provinces including Ontario and British Columbia to identify individuals who have asked to be denied entry because of gambling addictions.[215] For example, in Ontario images of people who enter a casino are compared to a database of self-identified gamblers who have been asked to be denied entry. Images that do not match the database are discarded. This program was approved by the Ontario Privacy Commissioner, with its design, e.g. biometric encryption, meant to protect privacy.

Conclusion

A number of organizations within the public sector have adopted facial recognition technology within and outside law enforcement. In many cases, there is currently a lack of transparency regarding the reasoning for adopting facial recognition technology in the first place and the existence of safeguards regarding its use. This prevents a complete analysis of whether facial recognition is reasonably required in a given context when considering the specific need for facial recognition technology against the loss of privacy and whether there are alternative solutions that are less privacy invasive.

[215] Supra note 1, "Automated Facial Recognition."

5. Facial Recognition Technology within the Private Sector

To date, there have been only two investigations announced into private firms for either using or operating FRT. First, in October 2020, the Office of the Privacy Commissioner of Canada (OPC), in connection with the Information and Privacy Commissioners of Alberta and British Columbia, released an investigative report into the use of FRT by the Cadillac Fairview Corporation Limited in several of the malls it owns and operates throughout the country.[216] Second, there is an ongoing investigation, launched in February 2020, into the activities of Clearview AI being conducted jointly by the OPC and the privacy protection authorities of British Columbia, Alberta and Quebec.[217] Because there are no rights to access information from private entities, the information available on private sector FRT use is limited to what has been reported on publicly, what has been announced by firms themselves, and what has been revealed through OPC investigations or the like.

From what information is available, we can draw the following conclusions:

- FRT has been in use in the private sector, and specifically in the retail sector, since at least 2010.[218]
- Private sector FRT use is principally directed towards security (by, for instance, recognizing faces of previously apprehended shoplifters) and sales/marketing (by tracking and analyzing consumer behaviour).[219]

---

[216] PIPEDA Report of Findings #2020-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

[217] OPC Announcement: "Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology," February 21, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/.

[218] *Planet Biometrics*, "Biometric CCTV system success at Canadian Tire," October 1, 2010. https://www.planetbiometrics.com/article-details/i/285/

[219] "From facial recognition to extra staff: High and low tech tools used to combat shoplifting in Winnipeg," *CTV Winnipeg*, February 21, 2019. https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648; Chris Frey, "Revealed: how facial recognition has invaded shops — and your privacy," *The Guardian*, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto; Esther Fung, "Shopping Centers Exploring Facial Recognition in Brave New World of Retail," *Wall Street Journal*, July 2, 2019. https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802.

- Firms using FRT may try to argue that their use does not involve the collection of personal information if photographs of identifiable individuals are not stored, either temporarily or permanently.[220]
- Under existing privacy law, however, biometric *templates* (i.e., not just images of identifiable individuals) have been regarded as personal information.[221]
- The private sector use of FRT almost certainly exceeds what has been publicly reported.[222]

In November, 2020, however, the federal government introduced Bill C-11, legislation that would replace PIPEDA as the federal privacy law governing the private sector. Daniel Therrien, the Privacy Commissioner of Canada, released a statement addressing the proposed changes, making some pointed criticisms:

> Bill C-11 opens the door to new commercial uses of personal information without consent, but does not specify that such uses are conditional on privacy rights being respected. […] In fact, the new purpose clause places even greater emphasis on the importance of the use of personal information for economic activity… The government states its refusal to adopt a rights-based approach is based on constitutional grounds. It says only the provinces have jurisdiction to legislate civil rights matters and the federal Parliament's jurisdiction is limited to trade and commerce.[223]

While an evaluation of the full impact of this change to Canadian privacy law requires further analysis outside the scope of this report, it is worth noting that expanded exemptions to consent

---

[220] Sarah Rieger, "At least two malls are using facial recognition technology to track shoppers' ages and genders without telling," *CBC News*, July 26, 2018. https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964.

[221] PIPEDA Report of Findings #2020-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

[222] See, for instance, Ryan Mac, Caroline Haskins, Logan McDonald, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," *Buzzfeed News*, February 27, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement, which refers to Canada as Clearview AI's "largest market" outside of the US, and that "company logs show access to its app has been given to both public and private entities"; see also Kate Allen, Wendy Gillis, Alex Boutilier, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known," *Toronto Star*, February 27, 2020. 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.

[223] Office of the Privacy Commissioner of Canada, Statement from the Privacy Commissioner of Canada following the tabling of Bill C-11, November 19, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/s-d_201119/.

requirements for private sector collection of personal information would bear directly on Canada's handling of FRT under privacy law, since one of the principal issues is the large-scale, automated collection of personal information that is often essential to FRT.

The discussion that follows will examine the private sector use of FRT in further detail. Section 5.1 gives an account of Cadillac Fairview's use of FRT and the OPC's decision regarding the resulting privacy violations, the only such decision to date. Section 5.2 then considers other known uses of FRT by private sector organizations in Canada.

5.1 Case Study: Cadillac Fairview

The details of the OPC report following their investigation of Cadillac Fairview's use of FRT are especially valuable because this is the only OPC ruling that explicitly comments on the relationship between FRT and Canadian privacy law (governing either the public or private sectors). While Bill C-11 is expected to replace PIPEDA as the governing private sector privacy law, OPC's analysis of the FRT employed in this case and the way in which Cadillac Fairview was determined to have collected personal information without prior consent likely still offers valuable insights regarding future private sector use of FRT.

Background

Cadillac Fairview Corporation Limited (CFCL) is a commercial real estate company that owns and manages malls and other commercial properties across Canada. Following a test period in 2017, CFCL contracted a third-party company, Mappedin, to install and operate "anonymous video analytics" (AVA) software in 12 of its Canadian malls between May and July 2018.[224] The AVA software, described by CFCL in correspondence with the OPC as "facial detection software," used concealed cameras contained in "digital wayfinding directories" to detect the faces of shoppers within the camera's field of view. When a human face was detected, the AVA software would attempt to classify the face according to gender and age range brackets, so that Mappedin could provide CFCL with aggregate demographic information about traffic patterns in

[224] PIPEDA Report of Findings #2020-004, para. 26.

its malls. Because the data collected by the AVA software was, according to CFCL, anonymous, and because, again according to CFCL, the software never collected personal information, including but not limited to images of shoppers' faces, the company claimed that use of the AVA software did not violate privacy laws.[225]

In short, CFCL asserted that at no time did it

1. identify individuals based on images of their faces (CFCL claimed that the AVA software was only capable of performing facial analytics, not facial *recognition*), or
2. collect and/or store shoppers' personal information.

On the basis of these claims, CFCL challenged OPC's jurisdiction, arguing that CFCL's use of AVA software could not have run afoul of PIPEDA's restrictions on the collection of personal information (since no such information was collected).

The OPC's investigation into the AVA software in question, however, revealed some complicating details. First: because shoppers' faces were needed as inputs in order to generate demographic estimates (gender and age classifications), once a face passed in front of the camera and was detected, the AVA software "generated a bounding box around the face, and captured the image therein for conversion and processing. This "capture" resulted in an actual digital image – or photograph – of the face being retained for a period of a few milliseconds."[226] While these captured images were not stored for long, the software also encoded the captured images of faces through numerical representations based on measurements of each face[227] so that the software could track and distinguish between faces within the camera's view (that is, so that while a shopper remained in view of the camera, their face would not be registered as a new face to track every moment). Mappedin, on behalf of CFCL, collected over five million such encoded numerical representations.[228]

Biometric templates and personal information

[225] *Ibid*., para. 30.
[226] *Ibid*., para. 40.
[227] *Ibid*., para. 44.
[228] *Ibid*., para. 52.

One issue relevant to future FRT use that is discussed in the OPC investigation, then, is the question of whether the numerical representations of faces collected by CFCL should be regarded as personal information, as understood in Canadian privacy law. More broadly: is a biometric template produced through an analysis of an individual's face considered personal information about that individual?

On the narrow question regarding Mappedin's numerical representations, the OPC reached an unambiguous conclusion:

> In particular, we are of the view that the embedding process, which results in the creation of a unique numerical representation of a particular face, constitutes a collection of biometric information, because that information is uniquely derived from a particular identifiable individual, and could be used, and is used in the context of the AVA technology in this case, to distinguish between different individuals.[229]

The OPC reached its conclusion in this case based on its understanding of the underlying technology: Mappedin's AVA software was built on top of FaceNet, an open source facial recognition tool developed by researchers at Google in 2015.[230] OPC determined that the numerical representations were created using FaceNet software "to identify a number of facial features, which would normally enable the software to recognize specific individuals."[231]

This conclusion was consistent, as the OPC report notes, with both the OPC's guidance on biometrics[232] as well as prior decisions by both the OPC and Alberta's Office of the Information and Privacy Commissioner that determined that biometric templates (including templates derived from palm prints, voice prints, palm-vein scans and fingerprints) were personal information in the context of privacy law.[233]

---

[229] *Ibid*., para. 65.
[230] Florian Schroff, Dmitry Kalenichenko, James Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682. See discussion in section 2.4 of this report.
[231] PIPEDA Report of Findings #2020-004, para. 65.
[232] Office of the Privacy Commissioner of Canada, *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/.
[233] See PIPEDA Case Summary #2004-281, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-281/; PIPEDA Case Summary #2010-007, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2010/pipeda-2010-007/; Information and Privacy Commissioner of Alberta, Investigation Report P2008-IR-005, https://www.oipc.ab.ca/media/127899/P2008-005IR.pdf; Information and Privacy Commissioner of Alberta, Investigation Report F2008-IR-001, https://www.oipc.ab.ca/media/127902/F2008-001IR.pdf.

Biometric templates and consent

Since biometric templates like the numerical representations produced by Mappedin's AVA software are treated as personal information, the collection and use of such biometric templates is governed by Canadian privacy law. According to the OPC's *Guidelines for obtaining meaningful consent*,[234] in circumstances where the collection of personal information is not otherwise a privacy violation, the *express* (as opposed to implicit) consent of the individuals whose information is being collected is required if that information is considered "sensitive".[235] Biometric information, including biometric templates, the report states,

> …is sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual. Within the category of biometric information, there are degrees of sensitivity. Facial biometric information is more sensitive since possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance.[236]

According to the OPC's guidelines, express consent is also required when the collection of personal information exceeds what a person would "reasonably expect" would be collected in the circumstances. In this case, the OPC determined that an individual in one of the CFCL malls would not reasonably expect either that their image was being captured and used (given the fact that the camera was concealed in a wayfinder kiosk) or that their image would be used to create a biometric template.[237] Based on the *Guidelines* and Principle 4.3 of Schedule 1 of PIPEDA, the report concludes,

> …in order to comply with the Acts, and conduct its practices in accordance with the Guidelines as reinforced by the Supreme Court of Canada, CFCL should have obtained express opt-in consent. That consent should have been obtained at the

---

[234] Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent*, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.
[235] The OPC report cites as support the Supreme Court of Canada decision *Royal Bank of Canada v. Trang*, 2016 SCC 50 paras 23 & 34.
[236] PIPEDA Report of Findings #2020-004, para. 79.
[237] *Ibid*., para. 80.

> time of the visitor's engagement with the map, before *CFCL captured and processed their image* via the AVA technology.[238]

While Bill C-11 does not adopt the OPC's guidelines in their entirety, it does adopt the language of express consent, as noted by the Privacy Commissioner's statement regarding the tabling of the bill.[239] Subsection 15(4) states that

> Consent must be expressly obtained, unless the organization establishes that it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed.[240]

As the Privacy Commissioner notes in his statement, Bill C-11 expands the exemptions from the consent requirements that exist under PIPEDA. The exemption for "business activities" given under subsection 18(1) states:

> An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for a business activity described in subsection (2) and
>
> (a) a reasonable person would expect such a collection or use for that activity; and
>
> (b)the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.[241]

The OPC decision regarding CFCL's violations of PIPEDA's consent requirements, especially regarding their determination of whether the creation of biometric templates for the purposes of facial recognition could be 'reasonably expected,' may therefore have continued relevance in evaluating the privacy implications of FRT use in the private sector.[242]

---

[238] *Ibid*., para. 81.

[239] Statement from the Privacy Commissioner of Canada following the tabling of Bill C-11, Office of the Privacy Commissioner of Canada, November 19, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/s-d_201119/.

[240] House of Commons of Canada, *Bill C-11*, https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

[241] *ibid*.

[242] Under section 40 of C-11, organizations would also be exempt from the consent requirement if they are collecting and/or using personal information "for purposes related to investigating a breach of an agreement or a contravention of federal or provincial law," and if collection with the individual's knowledge and consent would "compromise the availability or the accuracy of the information" (*ibid*.). This aligns with PIPEDA paragraph 7(1)(b), which allows for the same exemption. Thus, where FRT is used by an organization for security purposes, consent would presumably not be required. In PIPEDA Report of Findings # 2013-016, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-016/, however, OPC notes that "[c]ollections of personal information shall be limited to that which is necessary for the purposes identified by the organization." In that case, an organization was found to be in violation of PIPEDA

5.2 Other Known Uses in Canada

In addition to CFCL's use of FRT provided by Mappedin, it has been reported that the following organizations may have used FRT at some point:

Canadian Tire

It was reported in October of 2010 that two Canadian Tire locations had, through their security provider, Razko Security Limited, contracted Cognitec, a well-known FRT developer,[243] to provide an early version of its FaceVACS Video Scan System[244] to be operated in connection with the CCTV cameras located in the stores in an effort to prevent theft. The system would scan surveillance footage for faces of known shoplifters, sending the security team an alert when a match was made.

In 2016, a report published by *The Guardian*[245] included a document prepared by 3VR,[246] detailing the FR services they had provided the Canadian retail chain. Today, Canadian Tire is known to use FRT in roughly 15% of its locations nationwide,[247] though it is not known who provides the FR services at present.

Rexall

As part of the reporting on Clearview AI in the Toronto Star in February 2020, it was revealed that the pharmacy chain Rexall had received a trial version of Clearview AI's software

---

because it conducted a large-scale, indiscriminate collection of sensitive personal information for the purposes of preventing theft, and that it therefore collected "more information than necessary for its identified purpose."

[243] Cognitec's most recent FR algorithms were included in the NIST FRVT audit discussed in section 2.1.

[244] FaceVACS is still offered by Cognitec: see https://www.cognitec.com/facevacs-videoscan.html.

[245] Chris Frey, "Revealed: how facial recognition has invaded shops — and your privacy," *The Guardian*, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto

[246] Now known as "Identiv": https://www.identiv.com/3vr/.

[247] "From facial recognition to extra staff: High and low tech tools used to combat shoplifting in Winnipeg," *CTV Winnipeg*, February 21, 2019. https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648

from Toronto Police. When asked by the Star, Rexall confirmed that one employee had used the FR software to search seven suspected shoplifters, but that the company has discontinued the use of Clearview's software. Nevertheless, the Star reported that Rexall was listed in private Clearview AI data obtained by Buzzfeed News and shared with the Star.[248]

Saks' Fifth Avenue

The Guardian's 2016 article on FRT use in retail also alleged that Saks' Fifth Avenue has used FRT in its stores, reporting that the senior manager of asset protection for Hudson's Bay Company (HBC), the parent company of Saks' Fifth Avenue, had given an internal presentation on HBC's use of FRT for security purposes. A representative for Saks' Fifth Avenue declined to comment on whether the company uses FRT.[249]

Foody Mart

In November 2019, it was reported by the *National Post* that Foody Mart, a grocery chain with stores in Ontario and B.C., was looking to introduce FRT into its stores as a payment method. The payment system would allow customers to pay by scanning their face, which would be associated in an internal database with their account and billing details.[250]

---

[248] Kate Allen, Wendy Gillis, Alex Boutilier, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known," *Toronto Star*, February 27, 2020. 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.

[249] Chris Frey, "Revealed: how facial recognition has invaded shops — and your privacy," *The Guardian*, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto

[250] Tom Blackwell, "Businessman with Beijing ties looks to bring face-recognition tech to Canadian stores," *National Post*, November 12, 2019, https://nationalpost.com/news/pay-with-your-face-ontario-grocery-chain-looks-at-paying-via-facial-recognition.

6. Existing Policies and Regulations (Jurisdictional Scan)

6.1 Municipal Bans and Moratoriums in the United States

As facial recognition technology (FRT) comes under greater public scrutiny, understanding the policy responses that have been pursued in response is becoming increasingly necessary. Furthermore, given that both the United States and Canada have federal political systems and lack specific and comprehensive national legislation on facial recognition, examining American policy in particular would appear to have the potential to offer substantial insights.[251]

This indeed proves to be the case: Many American policymakers have recognized the potential dangers of facial recognition and have put forward substantive, meaningful policy interventions in response. Of note in this respect is the growing prevalence of moratoriums/bans on the use of FRT in American cities. At the time of writing, approximately 15 cities comprising over 3 million people have, in some form, implemented this type of policy response. These cities include Portland, Oregon; Portland, Maine; Springfield, Massachusetts; Somerville, Massachusetts; Brookline, Massachusetts; Northampton, Massachusetts; Cambridge, Massachusetts; Boston, Massachusetts; Easthampton, Massachusetts; San Francisco, California; Berkeley, California; Oakland, California; Alameda, California; New Orleans, Louisiana; and Jackson, Mississippi.

It is worth noting that there is a considerable degree of macro-level policy variation across cities, particularly in respect to scope. Most of the aforementioned cities have bans that apply only at the public level, meaning the municipal government and its associated agencies cannot use facial recognition technology. This is the case with the bans in San Francisco; Brookline; Alameda; Northampton; Cambridge; Boston; Somerville; Easthampton; Berkeley; New Orleans; Oakland; and Portland, Maine.[252] In contrast, Jackson's ban only applies to the local police force.[253] Meanwhile, the ban Portland, Oregon has adopted applies at both the public

---

[251] Raquel Aragon and Michael Whitener, "How should we regulate facial-recognition technology?" *International Association of Privacy Professionals,* January 29, 2019, https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/.

[252] To see the individual references for each city in this list, consult 1) in the Appendix.

[253] Kayode Crown, "Jackson Bans Facial Recognition Tech; New Airport Academy, Sewer Repairs," *Jackson Free Press*, August 20, 2020, https://www.jacksonfreepress.com/news/2020/aug/20/jackson-bans-facial-recognition-tech-new-airport-a/.

and private level—meaning that private businesses and the municipal government alike cannot utilize FRT.[254] Then there is Springfield: The city has adopted a moratorium against police use of FRT, which will not be lifted "until the Springfield Police Department develops a policy for using facial recognition technology that is approved by the [city] council."[255]

There are also more subtle policy differences across these bans/moratoriums that could meaningfully alter the usage of FRT within these jurisdictions. For example, the ordinances in some cities—specifically Portland, Oregon; Boston; San Francisco; Oakland; Easthampton; Somerville; and Cambridge—also explicitly prohibit city governments from using data or information extracted from FRT.[256] With that said, Boston's ordinance does allow Boston police or officials to use evidence extracted from FRT when it relates to the "investigation of a specific crime...so long as such evidence was not generated by or at the request of Boston or any official."[257] New Orleans and Alameda's respective ordinances also have a similar provision.[258] Finally, the bans in Portland, Oregon and Portland, Maine are distinct because they outline explicit penalties for violations. In Portland, Maine, private citizens that are subjected to a facial recognition scan in a manner that contravenes the ordinance are entitled to $1,000 at minimum, and municipal employees that violate this ordinance can be terminated or suspended.[259] In Portland, Oregon, businesses that violate the ban could pay fines of up to $1,000 per day.[260]

6.2 Policy Alternatives: Community Control Over Police Surveillance (CCOPS) Legislation

This patchwork of bans and moratoriums in American cities has been complemented with alternative, less absolute forms of regulation. So-called Community Control Over Police

[254] City of Portland, "Prohibit the acquisition and use of Face Recognition Technologies by City Bureaus (Ordinance)," 2020, https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868276/703_Sep_9_2TC_TW_E_Ord_BPS_1.pdf; City of Portland, "Prohibit the use of Face Recognition Technologies by private entities in places of public accomodation in the City", 2020, https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868277/704_Sep_9_2TC_TW_Ord_BPS_2__1_.pdf.

[255] Paul Tuthill, "Springfield Passes Moratorium On Face Surveillance Technology," *WAMC Northeast Public Radio*, February 25, 2020, https://www.wamc.org/post/springfield-passes-moratorium-face-surveillance-technology.

[256] To see the individual references for the cities in this list, consult 2) i n the Appendix.

[257] Boston City Council, "Ordinance Banning Face Surveillance Technology in Boston," 2020, 4, https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html.

[258] Michael Isaac Stein, "New Orleans City Council bans facial recognition, predictive policing and other surveillance tech," *The Lens*; Peter Hegarty, "East Bay city becomes latest to ban use of facial recognition technology," *The Mercury News.*

[259] Russell Brandom, "Portland, Maine has voted to ban facial recognition," *The Verge*.

[260] Mariella Moon, "Portland officials pass strict ban on facial recognition systems," *Engagdget*, September 9, 2020, https://www.engadget.com/portland-facial-recognition-ban-035952590.html.

Surveillance (CCOPS) legislation has been one such alternative. Advocated for by the American Civil Liberties Union (ACLU), CCOPS legislation is focused on ensuring that "local residents, through their city council representatives, are empowered to decide if and how surveillance technologies are used."[261] According to the ACLU, 17 jurisdictions comprising 14 million people have adopted CCOPS laws in some form.[262]

One of the key strengths of CCOPS legislation is its versatility. In some cases, CCOPS legislation actually includes facial recognition bans. San Francisco's public ban on FRT, for example, was passed as part of a wider CCOPS law.[263] Similarly, Somerville's facial recognition ban was also a byproduct of the ACLU's CCOPS campaign.[264] But CCOPS legislation can also introduce alternative measures that can serve as precursors to, or otherwise complement, specific bans and moratoriums. This is perhaps most clear in Cambridge, Massachusetts, which adopted a CCOPS ordinance in 2018 that "mandates that surveillance technologies cannot be funded, acquired, or used without express City Council approval."[265] Additionally, the ordinance requires municipal departments to acquire City Council approval if they want to utilize already-acquired surveillance technology in a novel way.[266]

Crucially, CCOPS legislation can also provide critical safeguards against the potential abuses of FRT in cities without a ban or moratorium. New York City is a clear example of this: It does not yet have a facial recognition ban or moratorium, but it does have CCOPS legislation called the Public Oversight of Surveillance Technology (POST) Act.[267] Instead of applying broadly to the municipal government in general (as is the case with Cambridge's CCOPS ordinance), New York's CCOPS legislation specifically applies to the New York Police Department (NYPD), and it requires the NYPD to be significantly more transparent with its

---

[261] American Civil Liberties Union (ACLU), "Community Control Over Police Surveillance (CCOPS)," 2020, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance#map.
[262] *Ibid*.
[263] *Ibid.*
[264] American Civil Liberties Union (ACLU), "Somerville Becomes First East Coast City To Ban Government Use Of Face Recognition Technology," June 28, 2019, https://www.aclu.org/press-releases/somerville-becomes-first-east-coast-city-ban-government-use-face-recognition.
[265] Jenna Fisher, "Cambridge Passes Law To Regulate Police Surveillance," *Patch Media*, December 11, 2020, https://patch.com/massachusetts/cambridge/cambridge-passes-law-regulate-police-surveillance; ACLU Massachusetts, "Cambridge Passes Law Requiring Community Control of Police Surveillance," December 10, 2018, https://www.aclum.org/en/news/cambridge-passes-law-requiring-community-control-police-surveillance.
[266] ACLU Massachusetts, "Cambridge Passes Law Requiring Community Control of Police Surveillance."
[267] Lauren Feiner, "NYC lawmakers pass bill requiring police to disclose surveillance technology," *CNBC*, June 18, 2020, https://www.cnbc.com/2020/06/18/nyc-passes-bill-requiring-police-to-disclose-surveillance-technology.html.

surveillance capabilities. More specifically, the NYPD is required under this law to provide "impact and use policies" on the types of surveillance technology it utilizes.[268] This means the NYPD must disclose the kind of surveillance technology it uses, the capabilities of its technology, the rules and processes that govern how these tools are used, and the safeguards used to protect the data collected by these surveillance tools.[269] The law also necessitates that the Commissioner of the NYPD must perform annual audits of these impact and use policies in order to ensure regulatory and legal compliance.[270]

Like New York City, Seattle currently lacks a ban or moratorium on FRT but it does have CCOPS legislation in the form of the Surveillance Technology Ordinance it adopted in 2017. Unlike New York's POST Act, which is clearly focused on improving transparency on the use of surveillance technology, this ordinance focuses on increasing community feedback by necessitating public input on the procurement of *any* surveillance tool by the Seattle Police Department (SPD).[271] According to Shahid Buttar, an activist and civil rights lawyer, Seattle's ordinance represents an "example of regulating local police surveillance through public process, as opposed to legislatively specifying substantive limits on the use of a particular device."[272] In this regard, CCOPS legislation can be understood as offering policymakers another discrete method of addressing some of the quandaries surrounding FRT.

6.3 State Laws on Facial Recognition Technology

State laws on facial recognition and surveillance technology further complicate this patchwork of municipal policies and regulations. One notable example is Illinois's Biometric Information Privacy Act (BIPA), which was passed in 2008. BIPA is particularly noteworthy due to the fact that it explicitly defines facial scans as a biometric identifier and, in turn, only allows a private entity (i.e., a private business) to obtain an individual's biometric identifier(s) if the following conditions are met: 1) A written notice of collection must be provided to said

---

[268] New York City Council, "Public Oversight of Surveillance Technology (POST) Act (Int. No. 487-A)," February 14, 2018, 1, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.
[269] *Ibid*, 1–3.
[270] *Ibid*, 3,
[271] Shahid Buttar, "West Coast Jurisdictions Advance Community Oversight of Police Surveillance," *Electronic Frontier Foundation*, August 7, 2017, https://www.eff.org/deeplinks/2017/08/west-coast-jurisdictions-advance-community-oversight-police-surveillance.
[272] *Ibid*.

individual, 2) the individual must be informed of why and for how long their biometric identifier is going to be collected, and 3) the company must receive a "written release" by the individual.[273] In practise, these conditions mean the law "requires affirmative consent for companies to collect biometric markers from their customers, including fingerprints and facial recognition models."[274] Texas also has its own biometric law called the Statute on the Capture or Use of Biometric Identifier, and it contains similar provisions.[275]

Both BIPA and Texas's biometric law have already created obstacles for companies offering facial recognition-related services. Google and Facebook have both been sued for violating BIPA due to the facial recognition features in their respective photo storage services.[276] Additionally, in 2018, Google refrained from making its Arts & Culture app available in Illinois and Texas. Google chose to do this out of an abundance of caution; it had added a feature that utilizes facial recognition, so the company chose to not make the app available in these states "for fear of violating the strict biometrics privacy laws on the books."[277] These are clearly just small examples of biometric laws affecting the implementation and use of facial recognition, but they do nonetheless demonstrate the impact that these kinds of laws can have.

Other state laws affecting the use of FRT offer additional safeguards but do not appear to be as powerful as laws like BIPA. This is especially apparent with California's A.B. 1215 and New York's Bill A6787-D/S5140-B. A.B. 1215, which Governor Newsom signed into law in 2019, establishes a three-year moratorium on the use of facial recognition in police body-worn cameras.[278] Meanwhile, New York's Bill A6787-D/S5140-B, which Governor Cuomo signed into law in December 2020, establishes a statewide moratorium on the use of biometric

---

[273] Illinois General Assembly, "(740 ILCS 14/) Biometric Information Privacy Act," 2008, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
[274] Russell Brandom, "Crucial biometric privacy law survives Illinois court fight," *The Verge*, January 26, 2019, https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition.
[275] John G. Browning, "The Battle Over Biometrics," *State Bar of Texas*, October 2018, 676, https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm.
[276] Ally Marotti, "Facebook could be forced to pay billions of dollars over alleged violations of Illinois biometrics law," *Chicago Tribune*, April 17, 2018, https://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html; Christopher Zara, "Google Gets Sued Over Face Recognition, Joining Facebook and Shutterfly In Battle Over Biometric Privacy in Illinois," *International Business Times*, March 4, 2016, https://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278.
[277] John G. Browning, "The Battle Over Biometrics," 676.
[278] Matthew Guariglia, "Victory! California Governor Signs A.B. 1215," *Electronic Frontier Foundation*, October 9, 2019, https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215.

technology, including FRT, in schools.[279] This moratorium is supposed to last until at least July 1, 2022 or until a study into the use of biometric technology in schools is completed and the State Education Commissioner allows their use in these institutions; whichever comes later will serve as the effective end date of the moratorium.[280] While A.B. 1215 and New York's moratorium clearly do not share the broad scope of a law like BIPA, they do represent more targeted policy interventions that further suggest there are multiple paths available for policymakers to regulate facial recognition technology.

6.4 Is America's Patchwork of Regulations for Facial Recognition Technology Effective?

The potential downsides of America's complex patchwork of municipal regulations and state biometric laws for FRT are fairly obvious. Primarily, this patchwork approach leaves a significant number of people vulnerable to the potential harms associated with the use of FRT. In other words, individuals in jurisdictions with regulations would be afforded some level of protection, but those who do not live in these areas would be more susceptible to the issues associated with current facial recognition use—whether that is the inaccurate identification of persons of colour (as described in Section 2 of this report), the infringement of privacy rights, or a lack of transparency with procurement and usage of facial recognition tools. This dynamic is plainly apparent in the United States: For cities like Portland, there are places like Plano, Texas, which "has enthusiastically adopted facial recognition technology with little public oversight."[281] This lack of oversight offers little in the way of safeguards against any potential abuses.

However, there are some that contend that this patchwork does offer some benefit, at least in the short term. Chief among them is Harvard professor and author Susan Crawford, who argues that "we should be glad to have all these local takes on the ethics of biometric data use."[282] Crawford takes this position for a few reasons. She cites Supreme Court Justice Louis Brandeis's well-known idea of states serving as laboratories for policy experimentation, pointing

---

[279] Governor's Press Office, "Legislation (A6787-D/S5140-B) Directs the Study of Whether Facial Recognition and Other Kinds of Biometric Technology Should be Used in Schools; Suspends Their Use Until Properly Reviewed," December 22, 2020, https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-suspending-use-and-directing-study-facial-recognition.

[280] *Ibid*.

[281] Susan Crawford, "Facial Recognition Laws Are (Literally) All Over the Map," *Wired*, December 16, 2019, wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

[282] *Ibid*.

to how patchwork legal environments have helped encourage the proliferation of electrical power grids and the development of policies like the Affordable Care Act.[283] However, her most salient argument has to do with how a patchwork legal environment "makes compliance difficult and drives up production costs" for companies, an assertion supported by empirical evidence in other sectors.[284] To this point, the International Federation of Accountants finds that patchworks are expensive: For the financial sector alone, global regulatory divergence (i.e., where different countries have different regulatory systems) costs $780 billion a year.[285] (Given the nascent nature of the facial recognition sector, this figure is almost certainly lower for facial recognition vendors, but the point nonetheless remains: Patchworks can saddle businesses with real costs). Per Crawford, the costs borne out of regulatory divergence in the facial recognition sector in the United States will incentive vendors to negotiate with federal regulators and offer concessions that would ensure the creation of uniform federal laws(s)—which would naturally reduce the regulatory costs faced by these companies.[286] To this point, the fact that technology companies explicitly lobbied Congress in 2020 for a nationwide law on facial recognition suggests that this incentive is indeed already present and that there is substantive merit to Crawford's argument in general.[287]

6.5 Evolution in the Canadian Legal and Regulatory Environment

Overall, the legal and regulatory environment for facial recognition in Canada is, in relation to the United States, comparatively underdeveloped. As mentioned earlier, Canada—like the U.S.—lacks thorough national-scale legislation that applies specifically to facial recognition. But, unlike the U.S., there is a conspicuous lack of provincial laws and local bans/moratoriums in place to fill the legal and regulatory gap. This disparity raises a key question: Should the American patchwork of municipal bans and state laws serve as a sort of policy roadmap for regulating facial recognition technology in Canada?

It is not the aim of this report to provide a final answer to this question, but there are indicators that the Canadian legal and regulatory environment vis-a-vis facial recognition

---

[283] *Ibid*.
[284] *Ibid*.
[285] International Federation of Accountants, "Regulatory Divergence: Costs, Risks, Impacts," 2018, pp. 4, https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf.
[286] Crawford, "Facial Recognition Laws Are (Literally) All Over the Map."
[287] Brian Fung, "Tech companies push for nationwide facial recognition law. Now comes the hard part," *CNN*, June 13, 2020, https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html.

technology is indeed slowly evolving to more resemble the patchwork of the United States. For one, there appears to be growing interest on the part of municipal policymakers in ordinances that provide safeguards against the use of FRT. For example, in 2020, Montreal City Councillor Marvin Rotrand introduced a motion reminiscent of facial recognition ordinances adopted by American municipalities in that it would require "city police to obtain city council approval before buying, renting, deploying or using facial recognition technology," among other surveillance tools.[288] On the provincial level, Ontario's provincial government appears to be considering introducing a new provincial privacy law for the private sector, as evidenced by Ontario's Ministry of Government and Consumer Services (MGCS) launching a consultation session on such a topic in August 2020.[289] While FRT is not explicitly mentioned, the discussion paper for the consultation session intriguingly acknowledges that improving or otherwise clarifying transparency and consent requirements for the collection of personal information are "key areas for reform."[290] This is especially promising, as it suggests that any potential new privacy law would in some way address these two legal areas, which this report has identified as being clearly pertinent to the use of FRT.

Regardless of their position on the use of FRT, policymakers and external stakeholders should observe how these policy developments on the municipal and provincial level play out. Are they harbingers of a legal and regulatory patchwork to come, or are they isolated efforts of a small policy window? Whatever the answer may turn out to be, it may very well signal what direction the regulation of facial recognition technology in Canada will take.

---

[288] Jacob Serebin, "Montreal should restrict police use of facial recognition technology: councillor," *National Post*, September 18, 2020, https://nationalpost.com/pmn/news-pmn/canada-news-pmn/montreal-should-restrict-police-use-of-facial-recognition-technology-councillor.

[289] Ministry of Government and Consumer Services, "Public Consultation - Reforming Privacy in Ontario's Private Sector," *Ontario's Regulatory Registry,* August 13, 2020, https://www.ontariocanada.com/registry/view.do?language=en&postingId=33967.

[290] Ministry of Government and Consumer Services, "Ontario Private Sector Privacy Reform Discussion Paper," 2020, pp. 4, https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45716.

Appendix

1)

Alameda, California: Peter Hegarty, "East Bay city becomes latest to ban use of facial recognition technology," *The Mercury News*, December 18, 2019, https://www.mercurynews.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology/.

Berkeley, California: Levi Sumagaysay, "Berkeley bans facial recognition," *The Mercury News*, October 16, 2019, https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

Oakland, California: Sarah Ravani, "Oakland bans use of facial recognition technology, citing bias concerns," *San Francisco Chronicle*, July 7, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

San Francisco, California: Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Brookline, Massachusetts: Nik DeCosta-Klipa, "Brookline becomes 2nd Massachusetts community to ban facial recognition," *Boston Globe Media Partners*, December 12, 2019, https://www.boston.com/news/local-news/2019/12/12/brookline-facial-recognition.

Northampton, Massachusetts: City of Northampton, "An Ordinance Prohibiting the Use of Face Surveillance Systems," 2019, https://www.northamptonma.gov/AgendaCenter/ViewFile/Item/13774?fileID=130290.

Cambridge, Massachusetts: Nik DeCosta-Klipa, "Cambridge becomes the largest Massachusetts city to ban facial recognition," *Boston Globe Media Partners*, January 14, 2020, https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition.

Boston, Massachusetts: Boston City Council, "Ordinance Banning Face Surveillance Technology in Boston," 2020, 3–4, https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html.

Somerville, Massachusetts: City of Somerville, "Ordinance Number 2019-16 Ban on Facial Recognition Technology," June 27, 2019, http://somervillecityma.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=12917.

Easthampton, Massachusetts: Michael Connors, "Easthampton bans facial recognition technology," *Daily Hampshire Gazette*, July 3, 2020, https://www.gazettenet.com/Easthampton-City-Council-passes-ordinance-banning-facial-recognition-survaillance-technology-35048140.

New Orleans, Louisiana: Michael Isaac Stein, "New Orleans City Council bans facial recognition, predictive policing and other surveillance tech," *The Lens*, December 18, 2020, https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech.

Portland, Maine: Russell Brandom, "Portland, Maine has voted to ban facial recognition," *The Verge*, November 4, 2020, https://www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance.

2)

Portland, Oregon: City of Portland, "Prohibit the acquisition and use of Face Recognition Technologies by City Bureaus (Ordinance)."

San Francisco, California: Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times.*

Oakland, California: Sarah Ravani, "Oakland bans use of facial recognition technology, citing bias concerns," *San Francisco Chronicle*.

Boston, Massachusetts: Boston City Council, "Ordinance Banning Face Surveillance Technology in Boston," 3–4.

Easthampton, Massachusetts: Michael Connors, "Easthampton bans facial recognition technology," *Daily Hampshire Gazette*.

Somerville, Massachusetts: City of Somerville, "Ordinance Number 2019-16 Ban on Facial Recognition Technology."

Cambridge, Massachusetts: Nik DeCosta-Klipa, "Cambridge becomes the largest Massachusetts city to ban facial recognition," *Boston Globe Media Partners*.

Bibliography

Algorithmic Justice League. https://www.ajl.org/.

Allen, Kate, and Wendy Gillis. "Toronto police have been using facial recognition technology for more than a year." *Toronto Star*, May 28, 2019. https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html?rf.

American Civil Liberties Union (ACLU). "Community Control Over Police Surveillance (CCOPS)." 2020. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance#map.

American Civil Liberties Union (ACLU). "Somerville Becomes First East Coast City To Ban Government Use Of Face Recognition Technology." June 28, 2019. https://www.aclu.org/press-releases/somerville-becomes-first-east-coast-city-ban-government-use-face-recognition.

American Civil Liberties Union (ACLU) Massachusetts. "Cambridge Passes Law Requiring Community Control of Police Surveillance." December 10, 2018. https://www.aclum.org/en/news/cambridge-passes-law-requiring-community-control-police-surveillance.

Amos, Brandon and Bartosz Ludwiczuk and Satyanarayanan, Mahadev, *OpenFace: A general-purpose face recognition library with mobile applications*, CMU-CS-16-118, CMU School of Computer Science, Tech. Rep., 2016. https://cmusatyalab.github.io/openface/

Aragon, Raquel and Whitener, Michael. "How should we regulate facial recognition technology?" *International Association of Privacy Professionals*, January 29, 2019. https://iapp.org/news/a/how-should-we-regulate-facial-recognition-technology/.

Bennett, Kelly. "Hamilton police tested controversial facial recognition technology Clearview AI." *CBC News*, February 20, 2020. https://www.cbc.ca/news/canada/hamilton/the-service-says-it-has-not-used-the-tool-for-any-investigative-purposes-1.5470359.

Blackwell, Tom. "Businessman with Beijing ties looks to bring face-recognition tech to Canadian stores," *National Post*, November 12, 2019,

https://nationalpost.com/news/pay-with-your-face-ontario-grocery-chain-looks-at-paying-via-facial-recognition.

Boston City Council. “Ordinance banning face surveillance Technology in Boston.” 2020. https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html.

Brandom, Russell. “Crucial biometric privacy law survives Illinois court fight.” *The Verge*, January 26, 2019. https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition.

Brandom, Russell. “Portland, Maine has voted to ban facial recognition.” *The Verge*, November 4, 2020. https://www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance.

Browning, John G. “The Battle Over Biometrics.” *State Bar of Texas*, October 2018. https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm.

Buolamwini, Joy and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proceedings of Machine Learning Research*, 81:1–15, 2018.

Buolamwini, Joy. “When the Robot Doesn’t See Dark Skin,” *New York Times*, June 21, 2018. https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

Burke, David. "Use of facial recognition technology by police growing in Canada, as privacy laws lag." *CBC News*, February 10, 2020. https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749.

Buttar, Shahid. “West Coast Jurisdictions Advance Community Oversight of Police Surveillance.” *Electronic Frontier Foundation*, August 7, 2017. https://www.eff.org/deeplinks/2017/08/west-coast-jurisdictions-advance-community-oversight-police-surveillance.

CBC News. "The end of anonymity? Facial recognition app used by police raises serious concerns, say privacy advocates." January 21, 2020. https://www.cbc.ca/radio/thecurrent/the-current-for-jan-21-2020-1.5434328/the-end-of-a

nonymity-facial-recognition-app-used-by-police-raises-serious-concerns-say-privacy-advocates-1.5435278.

CBC News. "Facial recognition software to aid Calgary police in future investigations." November 3, 2014. https://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1.2822592.

CBC News. "Officers used Clearview AI facial recognition technology, Edmonton Police Service admits." February 28, 2020. https://www.cbc.ca/news/canada/edmonton/edmonton-police-artificial-intelligence-facial-recognition-1.5480680.

CBC News. "Toronto police admit using secretive facial recognition technology Clearview AI." February 13, 2020. https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785.

City of Northampton. "An Ordinance Prohibiting the Use of Face Surveillance Systems." 2019. https://www.northamptonma.gov/AgendaCenter/ViewFile/Item/13774?fileID=130290.

City of Portland. "Prohibit the acquisition and use of Face Recognition Technologies by City Bureaus (Ordinance)." 2020. https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868276/703_Sep_9_2TC_TW_E_Ord_BPS_1.pdf.

City of Portland. "Prohibit the use of Face Recognition Technologies by private entities in places of public accomodation in the City." 2020. https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868277/704_Sep_9_2TC_TW_Ord_BPS_2__1_.pdf.

City of Somerville. "Ordinance Number 2019-16 Ban on Facial Recognition Technology." June 27, 2019. http://somervillecityma.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=12917.

Clearview AI. *Computer Vision for a Safer World*. 2020. https://clearview.ai/

Cognitec Systems GmbH. FaceVACS-VideoScan, https://www.cognitec.com/facevacs-videoscan.html.

Connors, Michael. "Easthampton bans facial recognition technology." *Daily Hampshire Gazette*, July 3, 2020.

https://www.gazettenet.com/Easthampton-City-Council-passes-ordinance-banning-facial-recognition-survaillance-technology-35048140.

Cook, Cynthia M. et al., "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, Jan. 2019, pp. 32–41

Conger, Kate, Fausset, Richard, and Kovaleski, Serge F. "San Francisco Bans Facial Recognition Technology." *The New York Times*, May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Crawford, Susan. "Facial Recognition Laws Are (Literally) All Over the Map." *Wired*, December 16, 2019, wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

Crown, Kayode. "Jackson Bans Facial Recognition Tech; New Airport Academy, Sewer Repairs." *Jackson Free Press*, August 20, 2020. https://www.jacksonfreepress.com/news/2020/aug/20/jackson-bans-facial-recognition-tech-new-airport-a/.

CTV Winnipeg. "From facial recognition to extra staff: High and low tech tools used to combat shoplifting in Winnipeg," February 21, 2019. https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648.

DeCosta-Klipa, Nik. "Brookline becomes 2nd Massachusetts community to ban facial recognition." *Boston Globe Media Partners*, December 12, 2019. https://www.boston.com/news/local-news/2019/12/12/brookline-facial-recognition.

DeCosta-Klipa, Nik. "Cambridge becomes the largest Massacussetts city to ban facial recognition." *Boston Globe Media Partners*, January 14, 2020. https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition.

Dlib C++ Library, "High quality face recognition," http://dlib.net/dnn_face_recognition_ex.cpp.html.

Dougherty, Kevin. "Quebec lawmakers raise the alarm over police use of facial recognition." *iPolitics*, September 22, 2020. https://ipolitics.ca/2020/09/22/quebec-lawmakers-raise-the-alarm-over-police-use-of-facial-recognition/.

"Facial Recognition Software Bid." York Regional Police. https://web.archive.org/web/20200618131043/https://yrp.bidsandtenders.ca/Module/Tenders/en/Tender/Detail/14d004d2-1270-4cbd-89cd-a13d58a5bf27.

"Facial recognition will go live on Aug. 24." Saskatchewan Government Insurance. Last modified August 17, 2016. https://www.sgi.sk.ca/news?title=facial-recognition-will-go-live-on-aug--24.

Feiner, Lauren. "NYC lawmakers pass bill requiring police to disclose surveillance technology." *CNBC*, June 18, 2020. https://www.cnbc.com/2020/06/18/nyc-passes-bill-requiring-police-to-disclose-surveillance-technology.html.

Fisher, Jenna. "Cambridge Passes Law To Regulate Police Surveillance." *Patch Media*, December 11, 2020. https://patch.com/massachusetts/cambridge/cambridge-passes-law-regulate-police-surveillance.

Fight for the Future. "Ban Facial Recognition Map." https://www.banfacialrecognition.com/.

"The Facts about Facial Recognition." New Brunswick Ombudsperson. https://www.ombudnb.ca/site/latest-news/the-facts-about-facial-recognition.

Fletcher, Robson. "Calgary police now admit 2 officers used controversial Clearview AI facial-recognition software." *CBC News*, February 28, 2020. https://www.cbc.ca/news/canada/calgary/calgary-police-admit-using-clearview-ai-facial-recognition-software-1.5480803.

Frey, Chris. "Revealed: how facial recognition has invaded shops — and your privacy," *The Guardian*, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto

Friesen, Joe. "Use of surveillance software to crack down on exam cheating has unintended consequences," *Globe and Mail*, December 16, 2020. https://www.theglobeandmail.com/canada/article-use-of-surveillance-software-to-crack-down-on-exam-cheating-has/.

Fung, Brian. "Tech companies push for nationwide facial recognition law. Now comes the hard part." *CNN*, June 13, 2020. https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html.

Fung, Esther. “Shopping Centers Exploring Facial Recognition in Brave New World of Retail,” *Wall Street Journal*, July 2, 2019. https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802.

Garvie, Clare. *Garbage In, Garbage Out: Face Recognition on Flawed Data*. May 16, 2019. https://www.flawedfacedata.com/#art-or-science.

Garvie, Clare, Alvaro Bedoya, Jonathan Frankle. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. October 18, 2016. https://www.perpetuallineup.org/.

Geitgey, Adam. “Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning,” *Medium*, https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78.

Geitgey, Adam. ageitgey/face_recognition. https://github.com/ageitgey/face_recognition#readme

Gillis, Wendy, and Kate Allen. "OPP confirms use of controversial facial recognition tool Clearview AI." *Toronto Star*, March 1, 2020. https://www.thestar.com/news/canada/2020/03/01/opp-confirms-use-of-controversial-facial-recognition-tool-clearview-ai.html.

Governor’s Press Office. “Legislation (A6787-D/S5140-B) Directs the Study of Whether Facial Recognition and Other Kinds of Biometric Technology Should be Used in Schools; Suspends Their Use Until Properly Reviewed.” December 22, 2020. https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-suspending-use-and-directing-study-facial-recognition.

Grimaldi, Jeremy. "York police officers used facial recognition technology without permission: YRP spokesperson." *York Region*, February 28, 2020. https://www.yorkregion.com/news-story/9869682-york-police-officers-used-facial-recognition-technology-without-permission-yrp-spokesperson/.

Grother, Patrick et al., “Face Recognition Vender Test (FRVT) Part 2: Identification, *NISTIR 8271 Draft Supplement*,” December 2020, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

Grother, Patrick. et al., “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, *NISTIR 8280*,” December 2019, https://doi.org/10.6028/NIST.IR.8280.

Guariglia, Matthew. "Victory! California Governor Signs A.B. 1215." *Electronic Frontier Foundation*, October 9, 2019. https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215.

Hackl, Micheal. "Clearer rules needed for facial recognition technology, " *rabble.ca,* August 6, 2020. https://rabble.ca/columnists/2020/02/clearer-rules-needed-facial-recognition-technology

Hawkins, Amy. "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, July 24, 2018. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

Hegarty, Peter. "East Bay city becomes latest to ban use of facial recognition technology." *The Mercury News*, December 18, 2019. https://www.mercurynews.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology/.

Hern, Alex. "Twitter apologises for 'racist' image-cropping algorithm," *The Guardian*, September 21, 2020. https://www.theguardian.com/technology/2020/sep/21/twitter-apologises-for-racist-image-cropping-algorithm.

Hill, Kashmir. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html .

Hill, Kashmir. "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

House Committee on Oversight and Reform, Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties. (video) https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

House of Commons of Canada, *Bill C-11*, https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

Identiv, inc. "3VR Is Now Identiv," https://www.identiv.com/3vr/.

Illinois General Assembly. "740 ILCS 14/) Biometric Information Privacy Act." 2008. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Information and Privacy Commissioner of Alberta, Investigation Report P2008-IR-005, https://www.oipc.ab.ca/media/127899/P2008-005IR.pdf.

Information and Privacy Commissioner of Alberta, Investigation Report F2008-IR-001, https://www.oipc.ab.ca/media/127902/F2008-001IR.pdf.

International Federation of Accountants. "Regulatory Divergence: Costs, Risks, Impacts." 2018, pp 1–16. https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf.

Information and Privacy Commissioner Ontario. *The Use of Biometric Face Recognition Technology in Ontario Casinos*. February 26, 2001. https://www.canlii.org/en/on/onipc/doc/2001/2001canlii26269/2001canlii26269.html?searchUrlHash=AAAAAQATZmFjaWFsIHJlY29nbml0aW9uIAAAAAAB&resultIndex=1.

Information and Privacy Commissioner Ontario. *Privacy by Design Solutions for Biometric One-to-Many Identification Systems.* June 2014. https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf

Israel, Tamir. *Facial Recognition at a Crossroads: Transformation at our Borders & Beyond*. September 2020. https://cippic.ca/uploads/FR_Transforming_Borders.pdf.

iView Systems, and Ontario Lottery and Gaming Corporation. *IView Systems Awarded Province Wide Contract for Incident Reporting and Facial Recognition*. April, 18, 2011. www.globenewswire.com/news-release/2011/04/18/1358580/0/en/iView-Systems-Awarded-Province-Wide-Contract-for-Incident-Reporting-and-Facial-Recognition.html.

Kasperkevic, Jana. "Google says sorry for racist auto-tag in photo app," *The Guardian*, July 1, 2015. https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app.

Klum, S., H. Han, A. K. Jain and B. Klare, "Sketch based face recognition: Forensic vs. composite sketches," *2013 International Conference on Biometrics (ICB)*, Madrid, 2013.

K.S., Krishnapriya et al., "Characterizing the Variability in Face Recognition Accuracy Relative to Race," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2019.

Lewis, Sarah. “The Racial Bias Built into Photography,” *New York Times*, April 25, 2019. https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.

Lohr, Steve. “Facial Recognition is Accurate, If You’re a White Guy,” *New York Times*, Feb. 9, 2018. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Mac, Ryan, Caroline Haskins, and Logan McDonald. "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA." *Buzzfeed News*, February 27, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Marotti, Ally. “Facebook could be forced to pay billions of dollars over alleged violations of Illinois biometrics law.” *Chicago Tribune*, April 17, 2018. https://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html.

Ministry of Government and Consumer Services (MGCS) (Ontario). “Public Consultation - Reforming Privacy in Ontario's Private Sector.” *Ontario’s Regulatory Registry,* August 13, 2020. https://www.ontariocanada.com/registry/view.do?language=en&postingId=33967.

Ministry of Government and Consumer Services (MGCS) (Ontario). “Ontario Private Sector Privacy Reform Discussion Paper.” 2020, pp. 1–9. https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45716.

Moon, Mariella. “Portland officials pass strict ban on facial recognition systems.” *Engagdget*, September 9, 2020. https://www.engadget.com/portland-facial-recognition-ban-035952590.html.

Munn, Nathan. "Police Forces in Canada Are Quietly Adopting Facial Recognition Tech." *Vice News*, June 23, 2020. https://www.vice.com/en/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech.

National Institute of Standards and Technology *FRVT 1:N Leaderboard*. https://pages.nist.gov/frvt/html/frvt1N.html.

National Institute of Standards and Technology, *NIST Face Recognition Vendor Test (FVRT) Ongoing*. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoin.

New York City Council. "Public Oversight of Surveillance Technology (POST) Act (Int. No. 487-A)." February 14, 2018. https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.

Office of the Information and Privacy Commissioner for British Columbia, *Investigation into the use of Facial Recognition Technology by the Insurance Corporation of British Columbia,* February 16, 2012. https://www.oipc.bc.ca/investigation-reports/1245

Office of the Privacy Commissioner of Canada, *Cadillac Fairview collected 5 million shoppers' images,* October 29, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/

Office of the Privacy Commissioner of Canada, *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/.

Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent*, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

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

Office of the Privacy Commissioner of Canada. "Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology," February 21, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/.

Office of the Privacy Commissioner of Canada. Expectations: OPC's Guide to the Privacy Impact Assessment Process, March 2020. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

Office of the Privacy Commissioner of Canada. Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), May 2018. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

Office of the Privacy Commissioner of Canada. PIPEDA in brief, May 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Office of the Privacy Commissioner of Canada,Privacy Impact Assessments: Frequently asked questions, December, 2011. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_33/

Office of the Privacy Commissioner of Canada, Statement from the Privacy Commissioner of Canada following the tabling of Bill C-11, November 19, 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/s-d_201119/.

Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada, January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Omstead, Jordan. "Caution urged as Edmonton police explore facial recognition technology." *CBC News*, February 5, 2020. https://www.cbc.ca/news/canada/edmonton/caution-urged-as-edmonton-police-explore-facial-recognition-technology-1.5451823.

Owen, Taylor, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun, and Kate Gilbert. *Facial Recognition Moratorium Briefing #1*. August 18, 2020.

PIPEDA Report of Findings #2020-004, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

PIPEDA Case Summary #2004-281, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-281/.

PIPEDA Case Summary #2010-007, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2010/pipeda-2010-007/.

PIPEDA Report of Findings # 2013-016, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-016/.

Planet Biometrics, "Biometric CCTV system success at Canadian Tire," October 1, 2010. https://www.planetbiometrics.com/article-details/i/285/.

Raji, Inioluwa Deborah, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, Emily Denton, "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing," Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. February 2020, pp. 145–151. https://dl.acm.org/doi/10.1145/3375627.3375820.

Ravani, Sara. "Oakland bans use of facial recognition technology, citing bias concerns." *San Francisco Chronicle*, July 7, 2019. https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

Regional Municipality of York Police Services Board. *Revised Agenda Public Session*. November 7, 2018. http://www.yrpsb.ca/usercontent/meetings/2018/nov/Merged_Agenda_Package_-_Public_Board_Meeting_Nov07_2018.pdf.

Rieger, Sarah. "At least two malls are using facial recognition technology to track shoppers' ages and genders without telling," *CBC News*, July 26, 2018. https://www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964.

Schroff, Florian, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.

Serebin, Jacob. "Montreal should restrict police use of facial recognition technology: councillor." *National Post*, September 18, 2020. https://nationalpost.com/pmn/news-pmn/canada-news-pmn/montreal-should-restrict-police-use-of-facial-recognition-technology-councillor.

Smith, Marcus, Mann, Monique., &Urbas, Gregor. 2018. *Biometrics, crime and security*. London: Routledge, Taylor & Francis Group.

Stein, Michael Isaac. "New Orleans City council bans facial recognition, predictive policing and other surveillance tech." *The Lens*, December 18, 2020.

https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech.

Sumagaysay, Levi. “Berkeley bans facial recognition.” *The Mercury News*, October 16, 2019. https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

Supreme Court of Canada, *Royal Bank of Canada v. Trang*, 2016. https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/16242/index.do?site_preference=normal&pedisable=true.

Toronto Police Services Board. *Public Meeting Agenda*. May 30, 2019.

Tunney, Catharine. "RCMP denied using facial recognition technology - then said it had been using it for months." *CBC News*, March 4, 2020. https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.548226.

Tuthill, Paul. “Springfield Passes Moratorium On Face Surveillance Technology.” *WAMC Northeast Public Radio*, February 25, 2020. https://www.wamc.org/post/springfield-passes-moratorium-face-surveillance-technology.

Washington Post Editorial Board, “Unregulated facial recognition must stop before more Black men are wrongfully arrested,” *Washington Post*, January 4, 2021, https://www.washingtonpost.com/opinions/unregulated-facial-recognition-must-stop-before-more-black-men-are-wrongfully-arrested/2020/12/31/dabe319a-4ac7-11eb-839a-cf4ba7b7c48c_story.html.

Wong, Julia Carrie. “Google reportedly targeted people with 'dark skin' to improve facial recognition,” *The Guardian*, October 3, 2019. https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color

Woodford, Zane. "Halifax police used controversial facial recognition technology." *The Chronicle Herald*, February 28, 2020. https://www.thechronicleherald.ca/salt/halifax-police-used-controversial-facial-recognition-technology-417130/.

Yogaretnam, Shaamini. "Ottawa police piloted controversial facial recognition software last year." *Ottawa Citizen*, February 14, 2020. https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-last-year.

Zara, Christopher. “Google Gets Sued Over Face Recognition, Joining Facebook and Shutterfly In Battle Over Biometric Privacy in Illinois.” *International Business Times*, March 4, 2016. https://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278.