FACIAL RECOGNITION TECHNOLOGY AND THE GROWING POWER OF ARTIFICIAL INTELLIGENCE

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pat Kelly, Chair

FACIAL RECOGNITION TECHNOLOGY AND THE GROWING POWER OF ARTIFICIAL INTELLIGENCE

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pat Kelly
Chair

OCTOBER 2022

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

To assist the reader:
A list of abbreviations used in this report is available on page ix

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Pat Kelly

VICE-CHAIRS

Iqra Khalid

René Villemure

MEMBERS

Parm Bains

James Bezan

Hon. Greg Fergus

Matthew Green

Lisa Hepfner

Damien C. Kurek

Ya'ara Saks

Ryan Williams

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Richard Bragdon

Iqwinder Gaheer

Jean-Denis Garon

Leah Gazan

Majid Jowhari

Arielle Kayabaga

Jennifer O'Connell

Brad Redekopp

Francesco Sorbara

Joanne Thompson

Anita Vandenbeld

Dominique Vien

Cathay Wagantall

CLERK OF THE COMMITTEE

Nancy Vohl

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Sabrina Charland, Analyst

Alexandra Savoie, Analyst

THE STANDING COMMITTEE ON
ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

SIXTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h), the committee has studied the use and impact of facial recognition technology and has agreed to report the following:

TABLE OF CONTENTS

LIST OF ACRONYMS

ACLU	American Civil Liberties Union
AI	Artificial Intelligence
AIA	Algorithmic Impact Assessment
BIPA	*Biometric Information Privacy Act*
CAI	Commission d'accès à l'information du Québec
CBSA	Canada Border Services Agency
CCLA	Canadian Civil Liberties Association
CIPPIC	Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
CSIS	Canadian Security Intelligence Service
FR	Facial Recognition
FRT	Facial Recognition Technology
ICLMG	International Civil Liberties Monitoring Group
NCCM	National Council of Canadian Muslims
NCECC	National Child Exploitation Crime Centre
NIST	National Institute of Standards and Technology
NTOP	National Technologies Onboarding Program
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	*Personal Information Protection and Electronic Documents Act*
RCMP	Royal Canadian Mounted Police

TPS   Toronto Police Service

TPSB   Toronto Police Services Board

SUMMARY

The rise of artificial intelligence (AI) and the growing use of facial recognition technology (FRT), as well as recent investigations by the Office of the Privacy Commissioner (OPC) into FRT, led the Committee to study FRT and the growing power of AI.

This report looks at the benefits and risks of FRT and its use in specific contexts, such as law enforcement. It explores other AI governance issues, such as procurement and public investment in this area. It also looks at legislative and other solutions to reassure Canadians that the use of FRT or other AI tools in Canada is done responsibly and respects their rights.

Taking into account witness testimony, the Committee makes several recommendations to improve the federal legislative framework that applies to FRT and AI technologies, including the recommendation to impose a moratorium on the use of FRT in Canada, as recommended by a majority of witnesses.

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

FACIAL RECOGNITION TECHNOLOGY AND THE GROWING POWER OF ARTIFICIAL INTELLIGENCE

INTRODUCTION

Background

Artificial intelligence (AI) is omnipresent in society now. Facial recognition technology (FRT), which relies on AI, is also becoming more popular. In Canada, FRT was recently the subject of a joint investigation by the Office of the Privacy Commissioner of Canada (OPC) and its provincial counterparts in Alberta, British Columbia and Quebec in a case involving Clearview AI.

In February 2021, the OPC released the report of its joint investigation in which it concluded that Clearview AI had failed to comply with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by engaging in the mass collection of images without consent and for inappropriate purposes.[1]

The OPC also conducted an investigation into the use of Clearview AI technology by the Royal Canadian Mounted Police (RCMP). In its special report to Parliament, released in June 2021, the OPC concluded that the RCMP had failed to comply with the *Privacy Act* by collecting personal information from a third party (Clearview AI) who illegally collected it.[2]

In light of the above, in December 2021 the Committee unanimously adopted a motion to study the use and impacts of FRT and the growing power of AI.

---

1   Office of the Privacy Commissioner of Canada (OPC), *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, 2 February 2021 [*OPC Report on Clearview AI*]. The OPC concluded that Clearview AI was not exempt from obtaining consent under the PIPEDA's "publicly available" personal information exemption, which is limited to publicly available personal information identified in the *Regulations Specifying Publicly Available Information*.

2   OPC, *Police use of Facial Recognition Technology in Canada and the way forward*, Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology, 10 June 2021 [*Special Report on the RCMP*]. The RCMP challenged the OPC's findings (see Chapter 2 of this report).

The Committee held nine public meetings and heard 33 witnesses. It also received eight briefs. The Committee thanks all those who participated in the study.

Structure of the Report

The report is divided into four chapters. Chapter 1 explains what FRT is and its presence in the market and provides an overview of its benefits and risks. Chapter 2 focuses on specific uses of FRT, including by law enforcement. Chapter 3 discusses stakeholder accountability with respect to using and developing FRT and AI and issues related to AI procurement and public investment. Finally, Chapter 4 focuses on the regulation of FRT and AI.

CHAPTER 1: FACIAL RECOGNITION TECHNOLOGY

> "Like all technologies, FRT can, if used responsibly, offer significant benefits to society. However, it can also be extremely intrusive, enable widespread surveillance, provide biased results and erode human rights, including the right to participate freely, without surveillance, in democratic life."
>
> Daniel Therrien, Privacy Commissioner of Canada, who appeared before the Committee on 2 May 2022.

Facial Recognition Technology: What It Is and How It Works

Carole Piovesan, a managing partner at INQ Law, said that FRT uses highly sensitive biometric facial data to identify and verify an individual. Brenda McPhail, director of the privacy, technology and surveillance program at the Canadian Civil Liberties Association (CCLA), said FRT can be thought of as facial fingerprinting.

Facial recognition (FR) is the process of identifying a face from a digital image or video. FRT can be deployed in real time or on static images. It uses computer pattern recognition to find commonalities in images depicting human faces. FRT can be used to confirm the identity of a known person, or to identify an unknown person. It can also allow for the categorization and profiling of a person over time based on their facial

information.[3] In other words, FRT can be used for verification, identification and categorization/characterization purposes.[4]

In general, however, FRT systems fall under two categories: those used to verify a person's identity (one-to-one) and those used to identify an individual (one-to-many).

> A one-to-one system compares a user's image to multiple images of a single person to authenticate or verify a person's known identity. A one-to-many system compares an image to a database of different faces (such as a terrorist watchlist or mugshot database) to uniquely identify an individual among a group of people, often in live or real-time settings.[5]

Elizabeth Anne Watkins, a postdoctoral research associate at Princeton University, described facial verification as follows:

> Whereas facial recognition is a 1:n system, which means it both finds and identifies individuals from camera feeds typically viewing large numbers of faces, usually without the knowledge of those individuals, facial verification, on the other hand, while built on similar recognition technology, is distinct in how it's used. Facial verification is a 1:1 matching system, much more intimate and up close where a person's face, directly in front of the camera, is matched to the face already associated with the device or digital account they're logging in to. If the system can see your face and predict that it's a match to the face already associated with the device or account, then you're permitted to log in. If this match cannot be verified, then you'll remain locked out. If you use Face ID on an iPhone, for example, you've already used facial verification.

Angelina Wang, a graduate researcher in computer science at Princeton University, explained that, from a technical standpoint, FRT is a machine-learning model. Rather than applying hand-coded rules, the model is given a very large dataset of faces with annotations, from which it learns.[6] These annotations include labels noting which images are the same person, and the location of the face in each image.

Ms. Wang said data for these models is typically collected through crowdsourcing on platforms like Amazon Mechanical Turk, which she said is known for having

---

3   Centre for Media, Technology and Democracy and Cybersecure Policy Exchange, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 1 June 2022, p. 2 [*CMTD and CPE Brief*].

4   Christelle Tessono, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 4 May 2022, p. 2 [*Tessono Brief*].

5   CMTD and CPE Brief, p. 2.

6   Angelina Wang gave the example of a hand-coded rule saying that two people are more likely to be the same if they have the same coloured eyes.

homogeneous worker populations and unfavourable working conditions, or simply scraped off the Internet, from websites like Flickr.[7] These datasets vary in size, from 10,000 images up to millions of images.

Facial Recognition Technology in 2022

Many witnesses said that FRT is increasingly present in the market and in society.

For example, Ms. Piovesan said that FRT is becoming much more extensively used by public and private sectors alike. She said that, according to a 2020 study published by Grand Review Research, the global market size of FRT is expected to reach US$12 billion by 2028.[8] She said this expansion is due to considerable investments and advancements in the use of FRT around the world. She added that, while discussions about FRT tend to focus on security and surveillance, various other sectors are using this technology, including retail and e-commerce, telecommunications and information technology, and health care. This presents a growing economic opportunity for developers and users.

Nestor Maslej, a research associate at the Institute for Human-Centered Artificial Intelligence at Stanford University, shared the following statistics from the Institute's 2022 AI Index Report.[9]

> In 2021, 18 of 24 U.S. government agencies used these technologies: 16 departments for digital access or cybersecurity, six for creating leads in criminal investigations, and five for physical security. Moreover, 10 departments noted that they hoped to broaden its use. These figures are admittedly U.S.-centric, but they paint a picture of how widely governments use these tools and towards what end.

> Since 2017, there has also been a total of $7.5 billion U.S. invested globally in funding start-ups dedicated to facial recognition. However, only $1.6 million of that investment has gone towards Canadian FRT start-ups. In the same time period, the amount invested in FRT technologies has increased 105%, which suggests that business interest in FRT is

---

7   For example, Nestor Maslej, a research associate at the Institute for Human-Centered Artificial Intelligence at Stanford University, explained that a résumé-screening system developed by Amazon using machine learning was found to be discriminatory because the system was trained on data from résumés Amazon had already received, the overwhelming majority of which were from men. The system was never used to make hiring decisions.

8   Grand View Research, Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analytics), by Application (Access Control, Security & Surveillance), by End-use, by Region, and Segment Forecasts, 2021 - 2028.

9   Stanford University, Human-Centered Artificial Intelligence Institute, Artificial Intelligence Index Report 2022; See also: Nestor Maslej, Brief to ETHI Committee – Study on the Use and Impact of Facial Recognition Technology, 9 June 2022.

also growing. Our estimates also show that FRT is the 12th-most funded area out of 25 AI focus areas.

Several other witnesses mentioned the already widespread use of FRT. For example, Dr. Watkins said that FR is used on Uber drivers, Amazon delivery drivers and home care providers to electronically verify each visit. Many police departments across the United States are using FRT, except in cities with bans or moratoriums on it. Ms. Wang said FRT is used by interviewing platforms like HireVue. Rob Jenkins, a professor of psychology at the University of York in the United Kingdom, said that a number of countries use FRT at border controls and in other processes, like passport renewal. Specific uses of FRT in Canada will be discussed in Chapter 2 of this report.

Diane Poitras, president of the Commission d'accès à l'information du Québec (CAI), said that, in addition to identity verification, the term FR is sometimes used to designate derivatives of the technology, which can be used for corporate purposes, in shopping centres for example, where the goal is not to identify individuals but rather their characteristics, like age, sex or time spent window-shopping.[10]

Sanjay Khanna, a strategic advisor and foresight expert, for his part, alluded to a future in which FRT could be used for sentiment analysis, for example for commercial manipulation purposes, or embedded into security robots or gambling. However, Ms. Wang said the following with respect to that type of FRT:

> It's worth noting here that there is also lots of pseudoscience on other kinds of facial recognition tasks, such as gender prediction, emotion prediction, and even sexual orientation prediction and criminality prediction. There has been warranted backlash and criticism of this work, because it's all about predicting attributes that are not visually discernible.

Benefits of Facial Recognition Technology

Many witnesses acknowledged that some uses of FRT could benefit society.[11] For example, Ms. Piovesan said that FRT can facilitate quick and secure payment at checkout, or help save a patient's life. She said that FRT is used in health care to monitor patients and make sure their condition does not change. She said that FRT can be useful

---

10   ETHI, *Evidence*, Diane Poitras.

11   ETHI, *Evidence*, Alex LaPlante; ETHI, *Evidence*, Carole Piovesan; ETHI, *Evidence*, Françoys Labonté; ETHI, *Evidence*, Daniel Therrien; ETHI, *Evidence*, Sanjay Khanna; ETHI, *Evidence*, Owen Larter; ETHI, *Evidence*, Rob Jenkins.

for verifying a person's identity to access their bank or their phone. FRT can also be useful for conducting financial transactions.

Françoys Labonté, chief executive officer of the Computer Research Institute of Montréal, said that, generally speaking, "people are in favour of using facial recognition technology for specific clearly-stated applications when it's easy to understand the benefits and how the data will be used."

Ms. McPhail mentioned the convenient and widespread use of facial verification to unlock phones, which, with appropriate built-in protections, may pose relatively little privacy risk.

Owen Larter, director responsible for artificial intelligence public policy at Microsoft, said that FRT can have a lot of benefits. Among these, he too mentioned identity verification using FR for a person's phone or computer. He noted the beneficial applications of FRT in the accessibility context, stating that some organizations are doing research on how to use FR to help people who are blind or with low vision better understand and interact with the world around them. One such project, called Project Tokyo, uses a headset so that an individual who is blind can scan a room and identify people who have consented to be part of their FR system, enabling them to identify that person and start a conversation. Mr. Larter also mentioned an application that aims to help people with Alzheimer's or similar diseases recognize friends and loved ones.[12]

Mr. Khanna said that FRT can be beneficial when used to prevent industrial accidents, for example by preventing employees from falling asleep or not being alert to a lack of attention.

Dubi Kanengisser, senior advisor in strategic analysis and governance for the Toronto Police Services Board (TPSB), said that FR can be another tool used by law enforcement to carry out their duties of identifying perpetrators and victims.

Daniel Therrien, former privacy commissioner of Canada, said that FR can be used for serious crimes, such as missing children, and for other compelling state purposes, such as in the border context to ensure that people of concern can be identified without impeding the flow of travellers into the country.

Kristen Thomasen, a law professor at the University of British Columbia, emphasized, however, that privacy is a social good that benefits everyone. That includes women and children who are often cited in the narrative that one of the beneficial uses of FR is to

---

12   Microsoft, Project Tokyo.

protect marginalized or victimized groups in certain contexts such as human trafficking or child abuse. She agreed that these beneficial uses of FRT should be acknowledged while nuancing that narrative considerably, as the erosion of privacy as a social good will also harm women and children. She stated that FRT consolidates and perfects surveillance, and that more perfect surveillance means greater privacy harm and inequity.

Prof. Thomasen stressed that FRT is not inevitable and that pointing to some beneficial use cases should not be sufficient to limit thinking around the potential harms that can arise from more widespread use of the technology. Ana Brandusescu, an artificial intelligence governance expert, and Ms. Poitras also cautioned against trivializing the risks that FRT poses because of its popularity or because it is convenient.

Concerns About Facial Recognition Technology

Misidentification and Algorithmic Bias

The biggest concern with the use of FRT is the potential for misidentification. For example, Cynthia Khoo, a research fellow at the Center on Privacy and Technology at Georgetown Law School in Washington, D.C., and with the Citizen Lab at the University of Toronto, said that researchers have found that FRT is up to 100 times more likely to misidentify Black and Asian individuals. It misidentifies more than one in three darker-skinned women, but is 99% accurate for white men. However, Ms. Wang noted that although models developed in Asia also have lots of biases "[t]hey are just a different set of biases than models that have been developed by Canadians or Americans".

Ms. Brandusescu presented statistics similar to those provided by Ms. Khoo:

> FRT is better at distinguishing white male faces than Black, brown, indigenous and trans faces. We know this from groundbreaking work by scholars like Joy Buolamwini and Timnit Gebru. Their study found that:
>
> … darker skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter-skinned males is 0.8%.

Witnesses referred to a study conducted by the U.S. National Institute of Standards and Technology (NIST), which found that some algorithms perform worse for certain

demographic groups.[13] The report found that, for algorithms developed in the U.S., false positive rates are highest for Asians and African Americans compared to Caucasians. For domestic law enforcement images, the highest false positive rates were for Indigenous peoples. The report also found false positive rates to be higher for women than men, and higher for the elderly and for children.

Ms. Piovesan also raised concerns about accuracy and bias in system outputs, unlawful and indiscriminate surveillance and black box technology that is inaccessible to lawmakers, restricting freedom and putting at risk fundamental values as enshrined in the *Canadian Charter of Rights and Freedoms*. Alex LaPlante, senior director of product and business development at Borealis AI, made similar comments, stating:

> [I]f we don't take care to adequately assess the application, development and governance of AI, it can have adverse effects on end-users, perpetuate and even amplify discrimination and bias towards racialized communities and women, and lead to unethical usage of data and breaches of privacy rights.

Dr. Watkins said that technologies such as AI, machine learning and algorithmic technologies based on data gathered over years and decades reflect human biases like institutional racism and sexism. These processes are "very conservative and very old-fashioned, and they are perpetuating the biases that we, as a society, ought to figure out how to…get past."

However, some witnesses said that FRT has come a long way. For example, Prof. Jenkins said that impressive progress has been made in the past five years in how well these systems can identify faces. Mr. Maslej noted:

> In 2017, some of the top-performing facial recognition algorithms had error rates anywhere from roughly 20% to 50% on certain FRVT [Facial Recognition Vendor Test] datasets. As of 2021, none has posted an error rate greater than 3%, with the top-performing models registering an error rate of 0.1%, meaning that for every one thousand faces, these models correctly identify 999.

Despite any progress, a few witnesses said that FRT would still raise concerns, even if it worked optimally.[14] For example, Ms. Khoo said that, even if FRT worked perfectly, it

---

13   ETHI, *Evidence*, Alex LaPlante; International Civil Liberties Monitoring Group, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 13 April 2022 [*ICLMG Brief*], p. 4; National Institute for Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, December 2019.

14   ETHI, *Evidence*, Kristen Thomasen; ETHI, *Evidence*, Tim McSorley; ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Angelina Wang.

might be used to the detriment of social groups that fall along historical lines of systemic oppression. Ms. McPhail made similar comments:

> [I]f the technology is fixed and if it becomes more accurate on all faces across the spectrums of gender and race, it may become even more dangerous. Why? It's because we know that in law enforcement contexts, the surveillance gaze disproportionately falls on those same people. We know who often suffers discrimination in private sector applications. Again, it's those same people. In both cases, a perfect identification of these groups or members of these groups who already experience systemic discrimination because of who they are and what they look like carries the potential to facilitate simply more perfectly targeted discriminatory actions.

Prof. Thomasen said that facial surveillance must be considered within its historical trajectory, which emerged from eugenics and white supremacist ideologies. She also cautioned that personal use of facial surveillance can be damaging with respect to harassment, doxing and other forms of technology-facilitated violence.

From a technical perspective, Ms. Wang explained that, because machine learning models try to identify patterns in data, they frequently amplify biases that exist in that data. She illustrated this point using the following example:

> [I]n predictive policing, if communities of colour and different neighbourhoods with higher proportions of Black citizens may have higher levels of crime, then predictive policing models may over-report those communities in the future to be more likely to have crime, even if that is not true, and will over-amplify this compared to the base rate of what the correlation actually is.

She also pointed out that, even if bias problems across demographic groups were resolved, two problems would remain: brittleness (known ways that bad actors can manipulate FR models to circumvent and trick them) and interpretability: it is extremely difficult to discover the precise set of rules the model is using to make these decisions.[15]

Other Concerns

Tim McSorley, national coordinator of the International Civil Liberties Monitoring Group (ICLMG), raised three main concerns about FRT: biased and inaccurate algorithms reinforce systemic racism and racial profiling; facial recognition allows for indiscriminate and warrantless mass surveillance; and the lack of regulation, transparency and accountability from law enforcement and intelligence agencies in Canada.[16]

---

15   ETHI, *Evidence*, Angelina Wang.

16   See also: ICLMG Brief.

Patricia Kosseim, Ontario's Information and Privacy Commissioner, said that, with respect to the use of FRT, the greatest concern of commissioners across Canada is mass surveillance, whether done by a third-party private sector company on behalf of the police or by the police service itself. Ms. McPhail noted that in addition to equality rights:

> [T]ools that could allow ubiquitous identification would have negative impacts on a full range of rights protected by our Canadian Charter of Rights and Freedoms and other laws, including freedom of association and assembly, freedom of expression, the right to be free from unreasonable search and seizure by the state, the presumption of innocence … and ultimately rights to liberty and security of the person.

Another concern with FRT is that people are not always aware that their face is part of a dataset used by FRT. The Clearview AI case is an example of such a situation. Ms. Wang said that the "individuals whose faces are included in this dataset generally do not know their images were used for such a purpose, and may consider this to be a privacy violation."

According to Prof. Jenkins, when an image is included in FRT algorithms, it becomes impossible to eliminate the influence of that image on the algorithm. He also explained the concept of intrapersonal variability: each of us has one face, which has its own appearance that constantly varies. This principle is an important factor in facial recognition since it involves not only the natural aging of the face, but also factors such as the angle, lighting, or a person's facial expression. Intrapersonal variability causes a lot of variation, which is difficult to overcome when using FRT.

Prof. Jenkins also noted that human oversight can catch egregious errors. However, he said that human face recognition is not infallible and can therefore also introduce errors into the system.[17]

Ms. Poitras brought up the privacy risks of biometric databases, noting that databases created for one purpose may be used for other purposes without an individual's knowledge or an adequate assessment of the risks associated with those other purposes. Witnesses also raised concerns about security weaknesses and data breaches.[18]

---

17   See also: Rob Jenkins, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 4 April 2022.

18   Ligue des droits et libertés, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 15 April 2022, p. 6 [*Ligue des droits et libertés Brief*]; Tessono Brief, p. 6.

Finally, for many witnesses, the fact that facial traits are permanent, and cannot be changed like passwords, makes FRT particularly invasive.[19]

CHAPTER 2: USES AND RELATED RISKS

> "**[Facial recognition technology] cannot bear the legal and moral responsibility that humans might otherwise abdicate to it over vulnerable people's lives and freedom.**"
>
> Cynthia Khoo, research fellow,
> who appeared before the Committee on 21 March 2022 as an individual.

Beyond general observations with regards to FRT, witnesses also commented on specific uses of FRT.

Dr. Watkins said that the use of FRT by government organizations, such as police agencies, border authorities and the government in general, is high risk. She said that, not only are these technologies unreliable, but they also presume that social constructs, like race and gender, are machine-readable in a person's face which, which in her opinion, "is simply untrue." She added that AI technologies, like Clearview AI, are not yet accurate enough and should not be used in high-risk scenarios, where lives and livelihoods are on the line.

One high-risk scenario discussed by witnesses was the use of FRT by police forces.

Use of Facial Recognition by Police Forces

Criticism

According to Ms. Khoo, one of the key problems with law enforcement use of FRT is the lack of transparency. The public often learns about the technology's use through media, leaked documents and freedom of information requests. Mr. McSorley and Ms. McPhail also noted the lack of transparency from law enforcement in Canada. Ms. McPhail described the situation in Canada as "a real crisis of accountability when it comes to police use of these technologies."

---

19   ETHI, *Evidence*, Angelina Wang; ETHI, *Evidence*, Daniel Therrien; ETHI, *Evidence*, Diane Poitras.

Prof. Jenkins criticized the reliability of FRT. He compared other identification methods used by police forces, such as fingerprinting, to FR to demonstrate the existence of more reliable techniques, in certain circumstances. He explained that other more traditional methods do not have the same number of technical problems that FRT presents: changes in facial appearance, lighting conditions, the distance from the face to the camera lens, and so on.

Prof. Jenkins said "[o]ne of the main concerns is mistaken identity and just the idea that an innocent person could be apprehended, accused and even sentenced for a crime they did not commit." He also recognized that it is important to "avoid the opposite error of failing to apprehend someone who could be a great danger to other people."

Ms. Khoo, Ms. Brandusescu, Ms. McPhail and Ms. Wang each mentioned cases of misidentification of Black men in the U.S. that led to wrongful arrests. Ms. Khoo gave Robert Williams, Nijeer Parks and Michael Olivier as examples:

> All three are Black men who were wrongfully arrested by police relying on facial recognition technology. They have endured lost jobs, traumatized children and broken relationships, not to mention the blow to personal dignity. These are the human costs of false confidence in, and unconstitutional uses of, facial recognition technology.

However, Ms. McPhail said that she was not aware of any examples where the misidentification of an individual led to criminal charges in Canada. She said that this is because police forces in Canada have been cautious and measured in adopting this technology and are using it in relatively limited ways.

Ms. Khoo said that racial justice activists, whom she and her colleagues talked to in the context of the research conducted for the Citizen Lab report, consider the use of algorithmic technologies by police to be 21st-century state violence: before it was done with pen and paper, now it is done with computers and algorithms.[20]

Ms. Brandusescu said that there is systemic racism in policing in Canada, noting that this was acknowledged by the House of Commons Standing Committee on Public Safety and National Security in a 2021 report.[21] In her view, FRT exacerbates systemic racism.

---

20   The Citizen Lab, Kate Robertson, Cynthia Khoo and Yolanda Song, *To Surveil and Predict – A Human Rights Analysis of Algorithmic Policing in Canada*, 1 September 2020.

21   Standing Committee on Public Safety and National Security (SECU), *Systemic Racism in Policing in Canada*, June 2021.

Ms. McPhail said that police use of FRT with mugshot databases is inherently problematic since they have their own issues of bias and discrimination. The ICLMG made similar comments.[22]

Sharon Polsky, president of the Privacy and Access Council of Canada, consulted with police forces on the use of FR and believes that police officers, like most Canadians, do not really understand compliance requirements or what FRT can actually do.[23]

Risk of Mass Surveillance by Police Forces

Some witnesses raised the possibility that police activities lead to mass surveillance.[24] Mr. McSorley gave the specific example of the RCMP:

> For example, the RCMP scrape information about individuals online and keep those in databases. We know they have been doing that. This is beyond facial recognition, but they would argue they have a right to collect that information, whereas others have been challenging it as we have, saying that it's a form of mass surveillance that needs to be regulated.

Gordon Sage, director general of the RCMP's Sensitive and Specialized Investigative Services, said that he does not believe that the mere use of FRT constitutes mass surveillance, even with respect to the use of Clearview AI's technology, which matched images against a database of three billion publicly sourced images.

Paul Boudreau, acting deputy commissioner of the RCMP's Specialized Policing Services, said that the RCMP does not use FRT for active surveillance or the capturing of mass protests. However, Mustafa Farooq, president and CEO of the National Council of Canadian Muslims (NCCM), said his organization gets calls all the time from people undergoing surveillance by the Canadian Security Intelligence Service (CSIS) or the RCMP at rallies or protests. Mr. Sage of the RCMP denied this allegation, assuring the Committee that the RCMP does not use any FRT for mass surveillance. He added that the only FRT used by the RCMP was Clearview AI's, but that this use stopped in July 2020.

---

22   ICLMG Brief, p. 4.

23   See also: Privacy and Access Council of Canada. Facial Recognition Use by Law Enforcement in Canada: Realities, Reservations, and Recommendations, 15 October 2021.

24   ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Tim McSorley.

Mr. Therrien said that he had no reason to doubt the RCMP's statement that it does not conduct mass surveillance or use FRT to do so, although he found their definition of the circumstances under which they use it rather ambiguous.

Colin Stairs, chief information officer of the Toronto Police Service (TPS), assured the Committee that the TPS does not conduct mass surveillance, does not take photos of protesters as a practice, and therefore does not run these types of photos through FR. He added that the TPS uses FRT as an investigative tool, not as a surveillance or reconnaissance tool that would infringe on privacy. For example, he explained the TPS' use of FR:

> What we are doing is taking crime scene photos gathered from cameras that would be recording the street regardless, taking a still from that and comparing it to the mug shot database, which is very similar to witnesses giving testimony. This is not a significant change.

Similarly, Dr. Kanengisser said that anything that falls under "mass surveillance" is an unreasonable use of FRT. For example, tracking people en masse indiscriminately would be unacceptable to the TPSB, as would the use of any technology that can be shown to be inaccurate, leading to significant misidentification and potential harm. For example a person getting arrested because they were misidentified by a software and that was not confirmed by a human would be unacceptable.

The following sections further discuss the use of FRT by the RCMP and TPS, including the use of Clearview AI's FRT.

Use by the Royal Canadian Mounted Police

According to Mr. McSorley, the RCMP has used different forms of FR over the past 20 years without any public acknowledgement, debate or clear oversight. Mr. Boudreau said, "We've been using facial recognition within the organization [the RCMP] for a very long time" but that, when it comes to new FRT "such as Clearview, we are not using that type of technology." Mr. Sage also said that the RCMP does not currently use FRT. The

RCMP clarified its testimony regarding its use of FRT in a letter to the Committee in July 2022.[25]

However, the RCMP has admitted to using Clearview AI's FRT in the past. Mr. Sage and Mr. Boudreau confirmed that two licences were purchased in October 2019 and used until July 2020, when Clearview AI withdrew from the Canadian market.

Mr. Sage said that he believed that a licence was first obtained by an investigator working for the National Child Exploitation Crime Centre (NCECC). He added that the director general at the time was not aware of the purchase when it was made. He also noted that the employee in question was never investigated. Mr. Boudreau also confirmed that no RCMP officer was reprimanded regarding the use of Clearview AI's FRT.

Mr. Boudreau explained that the RCMP is constantly looking at new technologies, whether it is FR or other types of technologies, so different divisions look at and evaluate new technologies. However, he said that, when the RCMP learned that a limited number of RCMP programs and services had begun using Clearview AI, an internal investigation was launched.

Mr. Sage said that because no policy was in effect at the time the licence was obtained, "members on the ground were able to obtain licences as they saw fit." Mr. Sage added that no analysis of the technology's compliance with the Charter took place at the time. The RCMP also confirmed that no ethics review was done before using Clearview AI's FRT.[26] Roch Séguin, director of the Strategic Services Branch, Technical Operations, said that the RCMP had approached the Department of Justice regarding the use of FRTs in its investigations only once, but it was internal to the RCMP.

Mr. Sage explained that Clearview AI's FRT was tested by a lot of RCMP members, using either their own photos, from profiles and social media, or photos of celebrities. They

---

25   Royal Mounted Police of Canada, *Letter to the Committee*, 21 July 2022. The letter clarifies the RCMP's testimony on the use of Facial Recognition Technology (FRT). It indicates that the RCMP uses certain FRT that had not previously been highlighted as such, namely Spotlight and Traffic Jam. Both tools use facial recognition, and other components, to help law enforcement identify victims of sexual exploitation, human trafficking and missing persons who are at risk of exploitation, by conducting searches on open websites. None of these tools have yet been evaluated by the National Technologies Onboarding Program. The letter also provides a list of RCMP use of FRT, a list of likely future use of new technologies and describes the approval process for purchasing licences from Clearview AI.

26   Royal Canadian Mounted Police, *Confidential letter to the Committee*, 3 June 2022.

found that the technology was not always effective and had some identification problems. As a result, it became one of many tools requiring human intervention.

Mr. Sage said that FRT was used in RCMP investigations on only three occasions: the NCECC used it on two occasions to identify victims of serious crime and provide safeguards to protect the victims who were located in Canada. It was used on a third occasion to track a fugitive abroad in cooperation with other police forces. He assured the Committee that the RCMP's use of FRT has never resulted in prosecutions in Canada.[27] Mr. Boudreau also said that human intervention must always be used when analyzing results.

However, the OPC report on the use of Clearview AI's FRT found that only 6% of the searches by Clearview AI appeared to be linked to NCECC victim identification, and approximately 85% were not accounted for at all by the RCMP.[28] According to Mr. Sage, 6% of the searches were for the three cases mentioned above, while the remaining 85% were used to test the technology.

Mr. Therrien explained that, as a result of his investigation, the OPC found that the RCMP had not taken any measures to verify the legality of Clearview AI's collection of information and lacked any system to ensure that new technologies were deployed lawfully. The OPC ultimately determined that Clearview AI's use of FRT was unlawful because it relied on the illegal collection and use of facial images by its business partner.

The OPC also found that there were "serious and systemic failings by the RCMP to ensure compliance with the Act before it collected information from Clearview and, more broadly, before novel collection of personal information in general."[29] Mr. Therrien noted that the words used in the report refer to the fact that at the time of the investigation the RCMP did not have a verification and approval process in place to ensure that, when new technology is used by its officers, the technology respects the law and privacy rights.

Mr. Therrien explained that the RCMP disagreed with the OPC's findings that it had failed to comply with section 4 of the *Privacy Act* by using Clearview AI technology. He noted that the RCMP argued that the section does not explicitly require a government

---

27   For example, Gordon Sage said that FRT was successful in identifying and finding a child who was a victim of sexual exploitation when traditional methods over the past 9–10 years had failed.

28   *Special OPC report on the RCMP*, para. 18.

29   Ibid., para. 87.

institution to verify the legality of its business partner's practices before the public sector uses the information.[30]

Mr. Therrien agreed that the above requirement is not explicit, but said that it exists implicitly under section 4 of the *Privacy Act*. Otherwise, a federal institution could, through contracting with the private sector, engage in practices it cannot engage in directly. He recommended that the ambiguity in the *Privacy Act* be removed by explicitly requiring all government institutions to ensure that what they are buying is lawful when they contract with the private sector.

Mr. Boudreau and Mr. Sage confirmed that the RCMP does not agree with all of the findings of the OPC's report, but supports its recommendations.

Mr. Therrien noted that, despite the RCMP's position, it was making good progress, in cooperation with the OPC, to have a better verification system for new technologies, be it FR or other new technologies. During his appearance, he said that the RCMP was unlikely to be able to implement all of the OPC's recommendations by the recommended 12-month deadline but said he believed the RCMP was making a genuine effort.

Mr. Séguin said that the OPC's recommendations led to a national technologies onboarding strategy in March 2021: the National Technologies Onboarding Program (NTOP). Since then, the RCMP has made significant progress in implementing the NTOP to ensure that technologies are assessed before being used in any operation or investigation. He said that the NTOP was expected to be in place by June 2022, within the 12 months recommended by the OPC, but that staff training may not have been given by that time.[31]

Mr. Séguin described the key pillars of the NTOP:

> With regard to the key pillars for the national technology onboarding program, or stakeholder outreach and partnership, which includes the training, obviously there's a policy review in development to identify all gaps with existing policy and to modify and update new ones. There's a technology assessment portion, where we built a full intake process through a series of questionnaires. Also, we're implementing a technology

---

30   Clearview AI challenged the OPC's findings and the orders made by the provincial commissioners. The federal commissioner does not have the power to make orders. See: ETHI, *Evidence*, Brenda McPhail; and ETHI, *Evidence*, Diane Poitras. In Quebec, Clearview AI is challenging the decision of the Commission d'accès à l'information du Québec (CAI) in court, including the CAI's jurisdiction over a U.S. company.

31   Royal Mounted Police of Canada, *Letter to the Committee*, 21 July 2022, p. 3. As of 21 July 2022, 31 new technologies had been submitted for review by the National Technologies Onboarding Program (NTOP), which is in its preliminary operational state. The letter describes the NTOP in more details.

inventory for awareness oversight. The last component is going to be public awareness and transparency.

Mr. Boudreau said that the NTOP provides an opportunity to look at all new technologies from a legal, ethical and privacy perspective. He added that the RCMP believes that the use of FR "must be targeted, time-limited and subject to verification by trained experts" and "should not be used to confirm an identity, but rather only be considered as an investigational aid where the results must be confirmed, again, by human intervention."

According to RCMP officials, the RCMP's partners will have to follow its policies.[32] Mr. Séguin also assured the Committee that "[f]rom a public awareness and transparency piece, it is built in as part of our communications strategy to relieve the categories of technology that the RCMP will be leveraging in the future."

Mr. Sage added that the NTOP assesses the risks and ethical issues of the technology, and includes a privacy assessment. He said that as part of the RCMP's efforts to develop new ways forward, the RCMP has "a member located within [the OPC's] office, and we are asking for one of their employees to be with our office in order to strengthen that knowledge and relationship."

Mr. Boudreau added that, when the RCMP looks at technologies such as FRT, they have to be looked at through the lens of a legal, privacy, gender-based analysis and bias perspective, and have human intervention as well.

As for the future use of FRT by the RCMP, Mr. Sage said it was unfortunate that FRT cannot be used in child exploitation cases to identify victims. He said it is an urgent file. He said he is waiting on a decision from national technical operations, as required by the NTOP process, to do an assessment of the use of FRT. Once the assessment is done, he hopes to have permission to use FRT for victims at risk.

Despite the actions taken by the RCMP, Rizwan Mohammad, an advocacy officer with the NCCM, said that the NCCM is shocked by the blasé attitude the RCMP has taken in approaching the issue of its use of Clearview AI. He noted that the RCMP had initially denied using Clearview AI's FRT but then confirmed it had been using the software, claiming that the use of FRT was not widely known within the RCMP.

The RCMP's use of other FRT was also raised by some witnesses. For example, Mr. McSorley said that the RCMP has contracted with IntelCenter, a U.S.-based private "terrorist facial recognition" system that provides "access to facial recognition tools and

---

32   ETHI, *Evidence*, Gordon Sage; ETHI, *Evidence,* Roch Séguin.

a database of more than 700,000 images of people associated with terrorism." The company says it acquires these images from scraping online, like Clearview AI. He said that law enforcement's use of IntelCenter is of great concern as it adds the extra stigma of saying that they know these people are associated with terrorism, with no oversight in terms of how they came to that determination. That information is then used by law enforcement.

However, Mr. Sage said that the IntelCenter software was acquired by the RCMP on an internal trial basis only. It was not tested or used in any national security investigation or other operational capacity. He added that, in March 2018, when the RCMP learned that the IntelCenter service software was not approved for operational use, "its use by E Division was discontinued."

Lastly, Mr. Sage said that Project Arachnid, a program run by the Canadian Centre for Child Protection in partnership with the NCECC, does not use FRT. It uses a hashtag search, which is the DNA of an image, to crawl the Internet.[33]

Use by the Toronto Police Service

Colin Stairs confirmed that the TPS uses FRT to compare probe photos uncovered in investigations against photos in its Intellibook, the TPS' mugshot database. Mr. Stairs assured the Committee that the body camera images used by the TPS do not go into the mugshot database and that there is "no connection between the body-worn cameras and the Intellibook system, no automated connection." He said the TPS operates under the *Identification of Criminals Act* and therefore uses only mugshots, which come from arrests and processing. Clearview was an anomaly in that regard. The TPS does not use publicly sourced facial images in its facial recognition program.

Mr. Stairs acknowledged that there is a known set of issues around face analysis in different training sets. He explained that the TPS selected the FRT it uses on the basis of minimizing racial bias, while recognizing that there are biases embedded into photographic systems (e.g., biases towards lighter faces compared to darker faces). For that reason, the TPS uses a "hurdle rate" below which the TPS does not consider it a match. A match is not considered an identity: the identity has to be corroborated by other methods.

---

33   Canadian Centre for Child Protection, *Project Arachnid*; See also: ETHI, *Ensuring the Protection of Privacy and Reputation on Platforms such as Pornhub*, June 2021. The report discusses Project Arachnid.

Mr. Stairs said that FRTs can be helpful when an unknown witness or subject is involved in a violent crime or a significant issue. However, their usefulness is limited by the scope of the TPS' mugshot database and the restrictions imposed by the *Criminal Code* and the *Canadian Charter of Rights and Freedoms*.

Mr. Stairs confirmed that the TPS' use of FRT is always accompanied by human analysis by the forensic identification service, stating that "there is a technician who takes the image, runs it into the system and looks at the results." He said he believes that any information related to the TPS' use of FRT in an investigation is shared after an arrest with the court or the defendant.

In February 2022, the TPSB adopted a Use of Artificial Intelligence Technology Policy (AI policy).[34] Dr. Kanengisser explained that, under the AI policy, the use of FRT or other biometric technology is considered "high risk." Considerable reviews in advance of adoption and deployment of the technology are therefore required.[35] Follow-up on the technology is also done over at least two years to examine any impact, including any unintended consequences.

Dr. Kanengisser said that the AI policy includes guiding principles for deciding whether or not a technology should be approved, which include issues of fairness and reliability, the legality of the use, and the requirement for human intervention at all times.

Mr. Stairs said that the TPS is drafting the procedure that will implement the AI policy adopted by the TPSB, and that consultations similar to those conducted to develop the policy will be held with stakeholders. In terms of hoped-for outcomes, he said that part of the problem is "insufficient visibility and guidance to frontline officers on how they should approach new technologies." As a result, the TPS is looking to create a framework that allows it to filter and indicate to the TPSB and the public the types of technologies it intends to use and why.

Mr. Stairs explained that, under the AI policy, the levels of risk for evaluating technologies are extreme risk, high risk, medium risk, low risk, and very low risk. Extreme risk would be banned. He added that a high or extreme risk level must involve human intervention. He said that the AI policy also requires that all technology must be

---

34   Toronto Police Services Board, *Use of Artificial Intelligence Technology Policy*, 22 February 2022.

35   ETHI, *Evidence*, Opening Remarks, Dubi Kanengisser. The Toronto Police Service (TPS) needs to demonstrate a real need and a mitigation plan to address any risks of bias or infringement of privacy or other rights in order to adopt a new "high-risk" tool and ensure a governance structure that allows for effective auditing. The policy also places an emphasis on training for TPS members.

posted and evaluated under the framework, except for low and very low risk technologies. Otherwise, the load on the TPS would be very high.

Ms. Kosseim said that the Office of the Information and Privacy Commissioner of Ontario was consulted on the AI policy. She said that, while not all of her office's recommendations were adopted within the policy, they can be adopted within the procedures that implement it. Vance Lockton, a senior technology and policy advisor in the Commissioner's office, said, for example, that one of the Commissioner's recommendations would be to include in the procedures better definitions of risk levels and how oversight of AI used by the TPS will be exercised.

According to Ms. Thomasen, the TPS' AI policy still has some weaknesses. For example, it still treats algorithmic policing technologies as inevitable—as a net benefit whose risks can be mitigated. She believes that this is not the right framework to address these technologies given the harms they can cause and the social context in which they are introduced.

Use of Facial Recognition by Other Federal Agencies

In 2020, a group of 77 privacy, human rights and civil liberties advocates, including the ICLMG, wrote a letter to the Minister of Public Safety calling on him to ban all use of facial recognition surveillance by federal law enforcement and intelligence agencies.[36] Further to the letter Mr. McSorley attended a listening session with the director of policy in the Minister's office, where he was told that the Canada Border Services Agency (CBSA) does not use real-time FR. Mr. McSorley added that no information was shared about CSIS's use of the technology, and no clear commitment was given from the Minister's office to take further action.

Referring to the patchwork of legislation around FRT, Mr. McSorley said:

> The lack of discussion and the lack of forthcomingness from federal agencies to discuss their use of facial recognition technology is what raises these deep concerns that they could be engaging in forms of surveillance that are unlawful or which otherwise would be considered unlawful, but are doing so because of this patchwork of legislation.

Mr. McSorley said that CSIS has refused to confirm whether or not it uses FRT in its work, stating that it has no obligation to do so.

---

36   International Civil Liberties Monitoring Group, *Open Letter: Canadian Government Must Ban Use of Facial Recognition by Federal Law Enforcement, Intelligence Agencies*.

Mr. Mohammad said that a number of national security and policing agencies, as well as other government agencies, have said that their use of surveillance was done in ways that were constitutionally sound and proportionate, when that was not the case, as demonstrated by the cases of Maher Arar, Abdullah Almaki and Mohamedou Ould Slahi.[37] He said:

> The same agencies that lied to the Canadian people about surveilling Muslim communities are coming before you now to argue that while mass surveillance will not be happening, FRT can and should be used responsibly.

Mr. Farooq brought up the example of a recent Federal Court decision that criticized CSIS for its habit of trying to mislead the court.[38] He noted that the government is appealing the decision. He added that what is going to be done to challenge national security agencies when they mislead people remains an open question.

Use of Facial Recognition by Border Authorities

In September 2020, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) released a report about FR and its use at the border.[39] Tamir Israel, a lawyer with the CIPPIC, outlined the report's key findings:

> [F]acial recognition is being adopted at the border without due consideration for the harms it would cause, without much external oversight and often without regard to existing policies, such as the Treasury Board's policy on artificial intelligence, where you are supposed to bring in external guidance when adopting intrusive technologies like that.
>
> Then, once it is adopted, it often gets repurposed very quickly for reasons beyond the narrow reasons of the context in which it was developed.

---

37   See: SECU, Review of the Findings and Recommendations of the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Iacobucci Inquiry) and the report from the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (O'Connor Inquiry), June 2009.

38   Canadian Security Intelligence Services Act (CA) (Re), 2020 FC 616 (CanLII), 2020 CF 616 (CanLII). The judge found that the Canadian Security Intelligence Service had breached its duty of candour. The duty of candour is a legal concept that applies in an ex parte warrant application and requires the party making the application to demonstrate utmost good faith in presenting its case for a warrant.

39   Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), Facial Recognition at a Crossroads: Transformation at our Borders & Beyond, September 2020.

> The last one is that it often provides a link between digital and physical presences in ways that allow for automation in the application of many other automated assessment tools, which is problematic in and of itself.

Mr. Israel made the following comment about the emergence of FRT at the borders:

> There are proposals around the world to automate that screening process. You'll walk up to a screen and get a facial recognition scan. There will be an assessment of your profile pulled in digitally, and you'll automatically get channelled through gates to a high-security, medium-security or low-security line.

Mr. Israel said that there are different types of FR systems, but that a decentralized system best describes the technology used for passport control. In a centralized system, all the images are held in one spot, whereas in a decentralized system an encoded digital image, such as a passport photo, is compared to the photo taken by the passport user at the airport. The security of the digital radio device encoded on the passport can be breached, but then only one passport is breached.

Several witnesses said that the use of FRT and other biometric technologies at airports and borders present high risks.[40]

Esha Bhandari, deputy director of the American Civil Liberties Union (ACLU), expressed concern about the expansion of FR and other biometric technology in airports. She explained that the concern is the mandatory requirement to agree to the use of FRT or provide iris scans to access essential services such as going to the airport or crossing the border, in contexts in which it is difficult to opt out due to the coercive nature of the environment. In her view, regulations should provide people with a meaningful opt-out so that they are not forced to provide an iris scan, for example.[41]

Mr. Israel raised the lack of explicit opt-in, saying that "you're not even necessarily aware that you're being subjected to the technology." He gave the example of the customs screening mechanisms at Toronto's Pearson Airport where travellers do not necessarily realize that a FR scan is happening. He said that "requiring, at the very least, an opt-out with very clear notification, and perhaps even an opt-in, would be a useful addition."

---

40   ETHI, *Evidence*, Tamir Israel; ETHI, *Evidence*, Esha Bhandari; ETHI, *Evidence*, Petra Molnar; Refugee Law Lab, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, 25 April 2022 [*Refugee Law Lab Brief*].

41   Refugee Law Lab, p. 8. Iris scans are also used in some refugee camps, for example in Jordan.

Witnesses also raised concerns about discrimination and racial profiling at the borders.[42] For example, Mr. Israel said that no-fly lists are a long-standing problem and that proposals to create FR lists with comparable objectives would be problematic.

Dr. Molnar again pointed out that FRT is highly discriminatory against black and brown faces and that algorithmic decision-making often relies on biased datasets. This is what concerns Prof. Jenkins about the use of FRT at airports, where even a 1% margin of error can be massive. He explained:

> I think around 100,000 passengers per day travel through Heathrow Airport, so, if we had an accuracy of 99% in that context, we'd be talking about 100 misidentifications per day, which soon adds up. It just doesn't seem sustainable to me.

Furthermore, in his research, Prof. Jenkins found that border and law enforcement officials are no better at identifying unfamiliar faces, despite their professional training and many years of experience. He said that the percentage of human errors made by experts, such as passport officers, compared to FRT software errors can vary depending on the specifics of the task. For example, passport staff who are well trained and have many years of experience have error rates of about 10%. For computer-based systems, it is difficult to predict accurate error rates since the results reported by vendors are often based on ideal conditions that allow for reliable analysis, where real-world noise and complexity are not taken into account.

Dr. Molnar also shared her concerns about the use of FRT by border authorities for the purpose of implementing biometric mass surveillance in migration and border management. In her view, to fully understand the impacts of various migration management and border technologies (e.g., AI lie detectors, biometric mass surveillance and various automated decision-making tools), it is important to consider the broader ecosystem in which these technologies develop. It is an ecosystem that is increasingly replete with the criminalization of migration, anti-migrant sentiments, and border practices leading to thousands of deaths, not only in Europe but also at the U.S.–Mexico and U.S.–Canada borders.

Since 2018, Dr. Molnar has visited borders all around the world, most recently the U.S.–Mexico border and the Ukrainian border. She said:

> Borders easily become testing grounds for new technologies, because migration and border enforcement already make up an opaque and discretionary decision-making space, one where life-changing decisions are rendered by decision-makers with little

---

42   ETHI, *Evidence*, Mustafa Farooq; ETHI, *Evidence*, Tamir Israel.

oversight and accountability in a system of vast power differentials between those affected by technology and those wielding it.[43]

In refugee determinations in particular, she said that, if mistakes are made, and if someone is wrongly deported to a country they are fleeing from, the ramifications can be dire.[44] Moreover, Dr. Molnar said that surveillance and smart border technologies do not deter people from making dangerous crossings, but rather force them to change their routes towards less inhabited terrain, leading to loss of life. She gave the example of the family that was found dead at the Manitoba–U.S. border.

Dr. Molnar therefore believes that replacing human decision-makers with automated decision-making and increasing surveillance "just muddies the already very discretionary space of immigration and refugee processing and decision-making." She added that, in border enforcement and immigration decision-making, structures that are underpinned by intersecting systemic racism and historical discrimination against people migrating, technology's impacts on people's human rights are very real.

Witnesses also discussed some specific FRT programs or projects at borders.

For example, Ms. Bhandari said the ACLU is concerned about the expansion of FR in airports, including programs like Nexus. Mr. Israel said that, while FRT programs used at Canadian borders, like Nexus, are still voluntary, the pressure to get through the border is used to encourage travellers to sign up for these types of systems. He also gave the example of the World Economic Forum's Known Traveller Digital Identity program pilot project:

> Canada, for example, piloted a program with the Netherlands, one developed by the World Economic Forum. It's basically a digital identity, housed on your phone, with a lot of your passport information and additional social identity verification program information. The idea was to see if that could be used in replacement of a passport, in order to facilitate border crossings. Facial recognition was the technology built into that system. The end vision of that system—it's very explicit—is getting travellers to voluntarily sign up for it to avoid delays at the border, because it gives you access to faster security processing. However, it later becomes available to banks,

---

43   Dr. Molnar gave the example of what she saw in the Sonoran Desert at the U.S.–Mexico border where various automated and AI-powered surveillance towers are sweeping the desert.

44   Dr. Molnar referred to the following report: The Citizen Lab, Petra Molnar and Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, 26 September 2018.

telecommunication companies and other entities, as well, for similar identity verification programs.[45]

Mr. Israel expressed concern about the Government of Canada's participation in the pilot project, which was interrupted by the pandemic. He said:

> I'm very concerned with the idea of using the pinpoint of the travel experience to encourage people to opt in and create these types of profiles, knowing that they're then going to be used against them, not just in border control contexts, where many marginalized communities are already at a massive disadvantage, but here and abroad, in other countries that end up implementing the same system. It's intended to be a global system. It's also with the idea that these same systems are going to then be used by the private sector for fraud detection or identity management in interactions with private companies.

Dr. Molnar and Mr. Farooq also mentioned the CBSA's pilot project at airports to test a technology called AVATAR—polygraphs that use facial and emotional recognition technologies to discern whether a person is lying and that are already banned in other jurisdictions. While Dr. Molnar questioned how a detector can deal with religious or ethnic differences, such as someone who may be reticent to make eye contact, who may just be nervous or who may have memory trauma, the NCCM expressed concerns about how this technology can be weaponized to profile people for potential terrorism. Dr. Molnar raised the following question:

> Whose priorities really matter when we choose to create AI-powered lie detectors at the border instead of using AI to identify racist border guards?

Lastly, Mr. Israel said that recently "CBSA announced they will try to implement a biometric study hub within their infrastructure," but that not much has been seen going on yet.

Use of Facial Recognition in Public Spaces

Ms. Khoo said that the use of FRT in public violates privacy preserved through anonymity in daily life. She said that this would likely induce chilling effects on freedom of expression such as public protests about injustice. It also promises to exacerbate gender-based violence and abuse by facilitating the stalking of women. Witnesses also reminded

---

45   ETHI, *Evidence*, Tamir Israel; Government of Canada, *The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers*, News release, 25 January 2018.

the Committee that the Supreme Court of Canada ruled that individuals retain a right to privacy even when in a public space.[46]

Dr. Watkins said that the use of FRT in public spaces could affect the right to freedom of movement.

Mr. McSorley said that, even if the significant problems of bias and accuracy were resolved, FR surveillance systems would continue to subject people to intrusive and indiscriminate surveillance, whether it is people walking through a public square or activists at a protest.

Mr. Farooq said his organization has not received any formal human rights complaints related to AI technology, including FRT. He mentioned, however, that the NCCM sometimes hears concerns around people attending peaceful rallies, such as in Vancouver or Hamilton, where pictures are being taken by law enforcement. He specified that the NCCM does not necessarily know what is being done with the collected data, in large part because of lack of disclosure. In his view, the lack of complaints is due to a lack of disclosure.

FRT is also used in semi-public spaces, such as commercial establishments. Mr. Labonté drew a parallel between using FRT in a retail store or shopping centre with e-commerce, where even if users are not connected to an account, cookies nevertheless leave behind traces of that time on the web. These cookies are then used to send targeted advertising on the basis of preferences.

Ms. Bhandari gave the example of U.S. companies, such as Walgreens, that use FRT to pick out a customer's age and gender and show them tailored ads or products. She said that this is an invasive tactic that could lead to concerns about consumers being steered to products based on gender stereotypes, which could further segregate society.

Ms. McPhail mentioned the OPC's investigation of Cadillac Fairview Mall. She said that the investigation revealed a non-consensual private sector use of facial analytics, which was discovered due to a glitch in the technology. In her view, this example shows that "almost every facial recognition vendor advertises that it can help private sector bodies leverage personal data to improve their market, and that's a problem."

---

46   ICLMG Brief, p. 6; Ligue des droits et libertés Brief, p. 4; *R v. Spencer*, 2014 SCC 43.

In its investigation, the OPC found that Cadillac Fairview had collected and used personal information, including sensitive biometric information through anonymous video analytics, without valid consent from visitors to Canadian malls.[47]

The examples given by witnesses show that FRT surveillance can be conducted in public spaces without people's knowledge.

Use of Facial Recognition in the Workplace

Dr. Watkins expressed her concerns with the private industry use of facial verification on workers. She said that "[f]acial verification is increasingly being used in work contexts, in particular gig work or precarious labour."

According to Dr. Watkins, "these systems are often in place to guarantee worker privacy, to prevent fraud and to protect security" but there needs to be alternatives in place to give workers other options. She said that workers should be consulted to better understand what kinds of technology they would prefer to comply with and to provide them with alternatives so that they can opt out of technologies yet still access their means of livelihood. She explained:

> In my research, I've gathered data from workers describing a variety of harms. They're worried about how long their faces are being stored, where they're being stored and with whom they're being shared. In some cases, workers are forced to take photos of themselves over and over again for the system to recognize them as a match. In other cases, they're erroneously forbidden from logging into their account because the system can't match them. They have to spend time visiting customer service centres and then wait, sometimes hours, sometimes days, for human oversight to fix these errors. In other cases still, workers have described being forced to step out of their cars in dark parking lots and crouch in front of their headlights to get enough light for the system to see them. When facial verification breaks, workers are the ones who have to create and maintain the conditions for it to produce judgment.

Dr. Watkins said that ultimately FRT is currently not reliable enough to be used in high-risk scenarios like the workplace. However, she acknowledged that some workers do advocate for FR for various reasons.

---

47   OPC, *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia*, 28 October 2020.

Use of Facial Recognition by Political Parties

According to Ms. McPhail, the use of FR by political parties also poses a risk to democracy. She mentioned the Liberal Party of Canada's recent use of a "similar one-to-one matching facial recognition tool … in its nomination voting process prior to the last federal election." She said that "[i]n that case, it was a much more risky use of a potentially faulty and discriminatory technology because it took place in a process that is at the heart of grassroots democracy."

Committee Observations and Recommendations

The Committee is of the view that RCMP officials were very reluctant to provide complete answers to the Committee's questions. In particular, with respect to the use of Clearview AI technology, many members voiced concern during the RCMP's testimony that witnesses were being evasive in their responses.

Considering the Privacy Commissioner's comments on section 4 of the *Privacy Act* and the many concerns about the use of FRT in the various contexts explored in this chapter, the Committee recommends:

Recommendation 1

That the Government of Canada amend section 4 of the *Privacy Act* to require a government institution to ensure that the practices of any third party from which it obtains personal information are lawful.

Recommendation 2

That the Government of Canada ensure that airports and industries publicly disclose the use of facial recognition technology including with, but not limited to, signage prominently displayed in the observation area and on the travel.gc.ca website.

Recommendation 3

That the Government of Canada refer the use of facial recognition technology in military or intelligence operations, or when other uses of facial recognition technology by the state have national security implications, to the National Security and Intelligence Committee of Parliamentarians for study, review and recommendation; and that the Committee report its findings.

Recommendation 4

That the government, in the creation of its regulatory framework around the use of facial recognition technology, set out clear penalties for violations by police.

CHAPTER 3: ACCOUNTABILITY, PROCUREMENT AND PUBLIC INVESTMENT

> "Very little money, time and resources go into dealing with the mess these technologies create and the harm they create."
>
> Ana Brandusescu, artificial intelligence governance expert, who appeared as an individual on 21 March 2022.

Accountability

Transparency

With respect to transparency about how FRT works, Ms. Wang said that models that have been trained using machine learning to perform FR tasks are currently difficult to interpret since it is not clear what patterns the models are relying on.

On the other hand, explaining the model is not necessarily the solution. Ms. Brandusescu said that, while explainable AI is a computational solution to make sure FRT can go forward, the explanation depends on the audience, and that audience is usually comprised of computer scientists, not politicians. She said trying to understand the black box is important but that having an explanation does not mean the technology should be used.

Ms. Piovesan also raised the importance of being able to explain the technology, i.e., understanding how algorithms operate and the output they provide and having independent verification to ensure that the output is accurate and reliable. She also noted the importance of having meaningful discussion with a variety of stakeholders about how these technologies are used and their implications before they are rolled out. She said one way to achieve this goal is to apply and adopt the concept of radical transparency.

Ms. Piovesan explained that radical transparency speaks to the entire disclosure process. She encourages organizations that use advanced technology to let people know who

their vendors are, what their uses are, where they are collecting the data they use and why they are doing so. Radical transparency seeks to engage the public rather than foster a secretive environment that undermines people's trust.

Prof. Jenkins also emphasized that transparency is important because the public needs to understand how these technologies are being used, how they can be effective, and how they may affect them. Auditing the use of FRT and making it public, for example, would help with transparency. He said that transparency is also an important component of an ethical system.

Mr. McSorley said that there needs to be pressure to have greater transparency and accountability from government. He said that federal agencies are required to conduct privacy impact assessments before new technology or private-impactful projects are undertaken but those assessments are often not done at all, or are kept secret.[48] For example, he said that the National Security and Intelligence Review Agency is undertaking a review of the use of biometric surveillance, but that it could take a couple of years before it is made public.[49] He argued that "a lack of transparency and accountability means that such technology is being adopted without public knowledge, let alone public debate or independent oversight."

Mr. Farooq made complementary comments. He said that it is hard to engage with government agencies when basic facts are not being acknowledged. For example, when CSIS refuses to confirm whether it uses FRT, it is hard to get any sense of accountability from it.

Ms. Khoo said that, in the case of police, policies governing the use of FR "can be even more of a black box than the algorithms themselves are said to be." She said this lack of transparency gives rise to severe due process deficits in criminal cases. She recommended that robust transparency and accountability measures be established.

Ms. Brandusescu suggested the Treasury Board should be involved in creating a registry for AI, especially AI used for law enforcement and national security purposes. She said such a registry would be useful for researchers, academics and investigative journalists who inform the public.

---

48   The Government of Canada's *Directive on Privacy Impact Assessment* has been in effect since 2010. It applies to government institutions subject to section 3 of the *Privacy Act*.

49   National Security and Intelligence Review Agency, *National Security and Intelligence Review Agency - 2022–23 Departmental Plan*. The departmental plan states that the Agency is conducting an ongoing review of the use of biometrics.

Dr. Watkins said better insight is needed into how technology tools like FRT are being used, where the data is being stored, how decisions are being made with them, and whether or not humans are involved. In short, more transparency is needed.

Governance and Accountability

Dr. LaPlante said that, since biometric data is sensitive, the security of that data must be ensured when it is collected, used and stored. According to her, FRT, like any high-risk AI system, should undergo extensive validation so that its limitations are properly understood and taken into consideration when applied in the real world. With respect to AI governance, Dr. LaPlante said:

> [G]overnance requirements should be proportional to risk materiality. Impact assessments should be common practice, and there should be context-dependent oversight on issues of technical robustness and safety, privacy and data governance, non-discrimination, and fairness and accountability. This oversight should not end once a system is in production but should instead continue for the lifetime of the system, requiring regular performance monitoring, testing and validation.

To root out bias from technology, Dr. LaPlante recommended that the Committee look into the concept of ethics by design, which involves taking ethical considerations into account throughout the development cycle, from initial data collection, to algorithm development, to production, and to the monitoring of those systems.

Mr. Labonté explained that, when a system is biased, it means that the initial data samples are not equal or are not representative in an equal way. He said that it is essential to regulate data harvesting, after noting that the most competitive players at the moment are the ones that collected enormous amounts of data for use in training AI models.

Mr. Maslej said that, in some cases, the more data provided to an AI model, the more likely it is to contain biased data. If data is not proactively filtered, AI models are likely to behave in problematic ways. He explained that filtering the data used to train an AI model could fix the problem, but would likely affect the model's ability to perform optimally.

Ms. Wang said that to correct bias problems in FRT results, providers should collect more diverse and inclusive data sets, and perform disaggregated analyses to look at the accuracy rates across different demographic groups rather than looking at one overall accuracy metric. She noted, however, that the collection of such data sets may itself be exploitative of marginalized groups by violating their privacy.

Ms. Brandusescu also suggested prioritizing accountability. For example, in the public sector, she said that the RCMP should be required to publish a report explaining its use of FRT. That practice could be applied to all federal departments and agencies in the future.[50]

Federal institutions are already required to comply with the Treasury Board's Directive on Automated Decision-Making. The federal directive requires, among other things, that an algorithmic impact assessment (AIA) be completed prior to the production of any automated decision system. Depending on the impact level, different accountability mechanisms are required (e.g., peer review or human involvement). The directive also imposes transparency and quality assurance obligations, such as making the AIA public.

However, Ms. Brandusescu said that the federal directive needs to be improved. She believes the public should have information about the government's use of technology like FRT and get updates. For example, she suggested that the Treasury Board publish recent government involvement in AI on its website (e.g., the procurement of new technologies such as FRT). She also recommended more specific, ongoing monitoring requirements for AI systems after the initial AIA, such as if the use or impact of the system changes.

Ms. Brandusescu also noted that the only non-governmental stakeholders consulted in AIAs published by the government since the federal directive came into effect were companies.[51] She suggested that AIAs could be improved by engaging civil society. She argued that engaging only companies limits the input of Canadians, affected groups, digital rights organizations and civil society bodies.

---

50   Ms. Brandusescu recommended that the Privacy Commissioner demand this report. The Commissioner does not currently have order-making powers. Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, introduced in the House of Commons in June 2022, if passed in its current form, would give the Commissioner the power to issue orders for the enforcement of federal privacy legislation that applies to the private sector. The *Privacy Act* applies to the public sector, including to the RCMP.

51   The Directive on Automated Decision-Making requires that, depending on the level of impact of the automated decision system, peer review be conducted by one of the following groups or means: a qualified expert from a federal, provincial, territorial or municipal government institution; qualified members of faculty of a post-secondary institution; qualified researchers from a relevant non-governmental organization; a contracted third-party vendor with a related specialization; publishing specifications of the automated decision system in a peer-reviewed journal; a data and automation advisory board specified by Treasury Board Secretariat.

Dr. Watkins said there is a need to ensure accountability and build the kinds of relationships between government, private actors and the public interest to address the needs of the most vulnerable.

Ms. Brandusescu also noted the need to increase in-house AI expertise so that agencies understand the technology they are buying.

In the same vein, Prof. Jenkins recommended "attention to human operators in the design and implementation of facial recognition systems, transparency and the development of an expert workforce in facial recognition." Though he added: "Human oversight provides important safeguards and a mechanism for accountability; however, it also imposes an upper limit on the accuracy that face recognition systems could achieve in principle." In other words, whenever there is human oversight, there is a risk of human error. To mitigate this risk, it is important to ensure that the people involved in FR decisions are highly qualified.[52]

Procurement and Public-Private Partnerships

Ms. Brandusescu said that the issue relating to technologies like FRT is more than data protection or privacy; it is a conversation about private sector involvement in public governance. She said people should be very concerned about the private sector taking over government policy development to regulate AI and FRT. Public-private partnerships are a key element of procuring, deploying, developing and using these technologies. She said that, in a recent report, she and her colleague argued that taxpayers are essentially paying to be surveilled, while companies like Clearview AI can exploit public sector technology procurement processes and the lack of regulatory mechanisms.[53]

As an example of perceived flaws in the procurement process, Ms. Brandusescu raised the fact that Palantir Technologies Inc. is on the federal government's list of pre-qualified AI suppliers, despite reports that the company has committed human rights violations in the U.S. and elsewhere (e.g., in immigration, mass arrests and the separation of children from their parents).[54] She said companies linked to human rights abuses should be removed from the government's list.

---

52   ETHI, *Evidence*, Rob Jenkins.

53   Centre for Media, Technology and Democracy, Yuan Stevens and Ana Brandusescu, *Weak privacy, weak procurement: The state of facial recognition in Canada*, 6 April 2021.

54   Government of Canada, Treasury Board Secretariat, *List of interested Artificial Intelligence (AI) suppliers*; Amnesty International, *Failing to do Right: The Urgent Need for Palantir to Respect Human Rights*, 2020; ETHI, *Evidence*, Ana Brandusescu.

Moreover, Ms. Brandusescu said that AI can sometimes evade procurement policies by offering free software trials, as was the case with Clearview AI.[55] She said that, to improve public procurement, a policy for the proactive disclosure of free software trials used by law enforcement and all of government should be created, as well as a public registry for them. This would "make the black box a glass box."

Dr. Molnar urged the Committee to consider why the private sector often gets to determine what Canada innovates on and why through public-private partnerships, which states are increasingly keen to make in today's global AI arms race. She reiterated the need to "pay careful attention to the particular actors involved in the ecosystem in which these technologies develop and are deployed." According to her: "None of this is neutral. It is all a political exercise."

Ms. Khoo and Prof. Thomasen raised the emergence of Amazon Ring-police partnerships in the U.S. as an example of surveillance infrastructure using a public-private partnership.

Mr. McSorley noted that, without proper regulation and with so many companies proposing their technology to law enforcement agencies, it is hard to know whether they "will even be using the most accurate [technology]—or will they be using the most accessible, the ones that are targeted more and marketed more towards law enforcement"? He too believes that the lack of regulation is what allowed the RCMP to use Clearview AI's FRT for months without the public's knowledge.

Neither Mr. Israel nor Ms. Bhandari were aware of a centralized registry of companies offering FRT, but said that some U.S. states require data brokers to register. Ms. Bhandari said requiring that kind of transparency from companies selling FR or other algorithmic tools would allow for a private right of action or for regulators to know who they should be monitoring.

Ms. Thomasen suggested that in-house FR systems be developed using data that is legally sourced, with informed consent and through processes that ensure the dignity of the individuals whose data is being processed. These systems could be designed and used only for very specific use cases, as opposed to commercial systems that do not take into account the specific social context in which FRT is used.

---

55   *Special Report on the RCMP*, para. 1. The OPC reported that the RCMP confirmed that it purchased two licenses to use Clearview AI's services in 2019 and that RCMP members had also used Clearview AI technology via free trial accounts.

Procurement by Police Forces

With regard to police procurement of technology, Ms. Khoo explained that that strict legal safeguards must be in place to ensure that police reliance on private sector companies does not create a way to go around people's rights to liberty and protection from unreasonable search and seizure.

For example, software from companies like Clearview AI, Amazon Rekognition and NEC Corporation is typically protected by trade secret laws and procured on the basis of behind-the-scenes lobbying. Ms. Khoo says this circumstance results in secretive public-private surveillance partnerships that strip defendants of their due process rights and subject the public to inscrutable layers of mass surveillance. To address this situation, she recommended that any commercial technology vendor that collects personal data for law enforcement should be contractually bound or otherwise held to standards of privacy and disclosure.

Ms. Khoo made three specific recommendations about the law enforcement procurement process to protect privacy and ensure accountability:

- law enforcement's acquisition of FRT or algorithmic policing technology can be done without engaging with a commercial vendor so as not to be beholden to proprietary interests (e.g., developing FRT in-house);[56]

- if procurement must be from a commercial vendor, strict procurement conditions can be put in place (e.g., waiving trade secrets for independent auditing); and

- ensure less secrecy around contracts so that people know about them prior to being signed rather than through leaks, freedom of information requests, or investigations by journalists.

Ms. Piovesan agreed with Ms. Khoo's recommendations.

Public Investment

Ms. Khoo said that private companies that collect vast quantities of data to capitalize on it are often funded through government grants, whether through the guise of innovation

---

56   Ms. Khoo gave the example of a lab in Saskatchewan (the Saskatchewan Police Predictive Analytics Lab), a publicly funded collaboration between the municipal police force and the University of Saskatchewan, which built their FRT in-house.

or because of lobbying. She said this is "essentially government and private companies working hand in hand to build out this network of surveillance."

Ms. Brandusescu said there is a bigger question about Canada's military-industrial complex and where surveillance technologies like FRT come from. She believes Canada needs to reflect on what tech solutionism means and why so much money is put into tech innovation but not into funding groups who work hard on social issues to understand the technology and create public awareness and education about it.

Ms. Brandusescu believes that the government should not fund FRT. Instead, it should fund civil society, digital rights groups and community groups that are studying FRT and involve them in the conversation about what the government decides to fund. She said:

> I think we can push back on tech inevitability, and we can say no to some of this technology, but that also requires funding and resources for education around these technologies. A lot of these contracts are made behind closed doors. In industry-government relationships, the public-private partnerships sometimes involve universities and labs, but it's always for a private interest focus. You want to fund these technologies, to build them, and then to use them. You don't think about the consequences. Very little money, time and resources go into dealing with the mess these technologies create and the harm they create.

Ms. Polsky said that Canadians are not fully aware of their privacy rights. She raised the idea of developing education programs for schools, but acknowledged that education is a provincial jurisdiction. She said that some media organizations and privacy commissioners across the country have developed courses or programs, but that these are not mandatory. She suggested that the OPC should be given an education mandate and funding for awareness campaigns.[57]

Example of Accountability in Action: Microsoft

Microsoft shared some of its internal AI and FRT practices, portraying itself as an example of a responsible AI provider in the private sector.

Mr. Larter said that Microsoft has a broad responsible AI program with three main components: a company-wide AI governance team that includes multiple stakeholders, including world-leading researchers; an AI standard, which ensures that any teams that

---

57   The federal Privacy Commissioner already has an educational mandate under section 24 of the *Personal Information Protection and Electronic Documents Act*, which requires the Commissioner to "develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part." This obligation remains in the proposed Consumer Privacy Protection Act in Bill C-27. A similar provision is not found in the *Privacy Act*.

are developing or deploying AI systems are doing so in a way that meets AI principles; and a sensitive use review process.[58]

Mr. Larter explained that a sensitive use review is done when any potential development or deployment of an AI system hits one of three triggers: the system is used in a way that affects a person's legal opportunities or legal standing; there is a potential for psychological or physical harm; or there is an implication for human rights. In such cases, Microsoft's governance team meets and reviews whether the company can move forward with a particular AI system.[59]

With respect to FRT, Mr. Larter said Microsoft published a transparency note for its Face application programming interface (API). The note explains in plain language how FRT works, what its capabilities and limitations are, and factors that affect performance. He said that, as Microsoft was developing its FRT, it was very mindful of having representative datasets so that the technology can perform accurately, including across different demographic groups.

Mr. Larter said testing is really important given the wide gap between the best performing facial recognition systems and the least well-performing systems. He said vendors should allow their systems to be tested by independent third parties in a reasonable fashion and be required to address any material performance gaps.[60] Microsoft allows its systems to be tested. He also said there is a need for robust cybersecurity around technology.

Committee Observations and Recommendations

The Committee believes that the government should be more transparent about its use of FRT and other AI, as well as about its procurement process. It should also invest more in studying the impact of AI and raising awareness about privacy rights.

Therefore, the Committee recommends:

---

58   Ibid. Microsoft, *Putting principles into practice at Microsoft*. Microsoft's AI standard consists of a series of requirements related to its six AI principles: fairness, reliability and safety, privacy and security, inclusiveness, transparency and accountability.

59   Ibid.

60   ETHI, *Evidence*, Owen Larter. According to Mr. Larter, there should be a testing requirement for organizations deploying FRT to make sure that the system is working accurately in the environment in which it's going to be used.

Recommendation 5

That the Government of Canada amend its procurement policies to require government institutions that acquire facial recognition technology or other algorithmic tools, including free trials, to make that acquisition public, subject to national security concerns.

Recommendation 6

That the Government of Canada create a public AI registry in which all algorithmic tools used by any entity operating in Canada are listed, subject to national security concerns.

Recommendation 7

That the Government of Canada enhance the Treasury Board Directive on Automated Decision-Making to ensure the participation of civil society groups in algorithmic impact assessments and to impose more specific requirements for the ongoing monitoring of artificial intelligence systems.

Recommendation 8

That the Government of Canada increase its investment in initiatives to study the impact of artificial intelligence on various demographic groups, increase digital literacy, and educate Canadians about their privacy rights.

Recommendation 9

That the Government of Canada ensure the full and transparent disclosure of racial, age or other unconscious biases that may exist in facial recognition technology used by the government, as soon as the bias is found in the context of testing scenarios or live applications of the technology, subject to national security concerns.

Recommendation 10

That the Government of Canada establish robust policy measures within the public sector for the use of facial recognition technology which could include immediate and advance public notice and public comment, consultation with marginalized groups and independent oversight mechanisms.

CHAPTER 4: REGULATING FACIAL RECOGNITION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

> ## "FRTs need to be regulated with a scalpel, not an axe."
>
> Carole Piovesan, managing partner with INQ Law,
> who appeared before the Committee on 21 March 2022

As Ms. Polsky pointed out, the Supreme Court of Canada recognized long ago that "privacy is essential for the well-being of the individual" and that "[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual."[61] However, given the place of AI and FRT already in our society, the Committee wondered: Is it too late to intervene?

Most witnesses said it was not too late.[62] Others said that the proliferation of FRT does not spell the end of individual freedom.[63] Mr. Therrien also felt that it was not too late to intervene. He explained:

> I heard you ask certain witnesses at this committee if it's too late. It's never too late. Actually, the fact that certain practices are currently occurring should be no reason for you to prevent yourself from doing the right thing and regulating the technology in a way that respects the rights of Canadians.
>
> We are living, not completely but in part, in a world of self-regulation that has led to certain unacceptable practices. It's not because they are routine or banal … that they should continue to be authorized.

Witnesses suggested a number of ways to address shortcomings in the current legislative regime.

Moratoriums, Bans and Other Measures

Given the risks of FRT, most stakeholders recommended a moratorium, particularly in law enforcement, until an appropriate regulatory framework is in place and more

---

61   *R v. Dyment*, [1988] 2 SCR 417, para. 17 (Justice La Forest).

62   ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Carole Piovesan; ETHI, *Evidence*, Rob Jenkins; ETHI, *Evidence*, Daniel Therrien; ETHI, *Evidence*, Esha Bhandari; ETHI, *Evidence*, Tamir Israel.

63   ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Ana Brandusescu; ETHI, *Evidence*, Sanjay Khanna; ETHI, *Evidence*, Rob Jenkins.

research and consultation on the use of the technology and its impacts have been done.[64]

For example, Ms. Khoo said there should be a moratorium, or a national pause, on the use of FRT by law enforcement until it is shown to be not only reliable but also necessary and proportionate to legitimate aims and the far-reaching repercussions its use may have. She did not rule out a potential ban on the use of FRT in some cities, as is the case in the U.S.[65]

Ms. Khoo said a moratorium on the use of FRT by law enforcement will give time for further research to determine whether it is appropriate to use it and with what safeguards, such as transparency, adequate oversight mechanisms and disclosure requirements. She called for a moratorium not only on FRT but on all algorithmic policing technologies. She also proposed that, during the moratorium, a national commission or judicial inquiry do an in-depth constitutional and human rights analysis to determine what is appropriate and what is not.[66]

Mr. McSorley and Prof. Thomasen recommended that, during a moratorium, the federal government hold consultations on the use and regulation of FRT, for example to decide what uses should be prohibited.

Ms. McPhail said that one purpose of a moratorium would be to give the government a chance to rectify a major gap in the federal privacy regime: the fact that the Commissioner does not have enforcement powers. She said that a moratorium for law enforcement is particularly important because those are situations where the consequences of an error can be life-altering, but that a general moratorium would also

---

64   ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Kristen Thomasen; ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Sanjay Khanna; ETHI, *Evidence*, Elizabeth Anne Watkins; ETHI, *Evidence*, Angelina Wang; ETHI, *Evidence*, Tim McSorley; ETHI, *Evidence*, Rizwan Mohammad; ETHI, *Evidence*, Mustafa Farooq; ETHI, *Evidence*, Sharon Polsky; ETHI, *Evidence*, Tamir Israel; CMTD and CPE Brief; ICLMG Brief; Tessono Brief; Ligue des droits et libertés Brief; Canadian Human Rights Commission, *Brief to the ETHI Committee – Study on the Use and Impact of Facial Recognition Technology*, April 2022 [*CHRC Brief*].

65   ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Esha Bhandari. According to Ms. Bhandari, at least 23 cities in the U.S. have halted law enforcement or government use of facial recognition technology. See also: CMTD and CPE Brief, p. 8; Tessono Brief, p. 5.

66   ETHI, *Evidence*, Cynthia Khoo. The Citizen Lab report, co-authored by Ms. Khoo, defines algorithmic policing as all new technologies that use an automated mathematical formula to support or supplement police decision-making.

be beneficial given that private sector vendors are selling technologies to public sector actors.[67] Ms. Khoo also said that a moratorium in other sectors would be appropriate.

Some witnesses were against the idea of a moratorium. For example, Mr. Larter said that Microsoft believes that, instead of investing time and effort in imposing a moratorium, police use of FRT should be regulated. He said that Microsoft supports FRT regulation that protects human rights, prohibits mass surveillance and advances transparency and accountability. In his view, a regulatory framework would build public trust in the use of FRT.

Mr. Larter noted, however, that Microsoft has imposed a moratorium on the sale of its FRT to police forces in the U.S. He said that this ban does not apply to Canada, because unlike Canada, the U.S. does not have a federal privacy framework or broad privacy laws.[68]

Mr. Stairs with the TPS does not believe a moratorium on the use of FRT by police forces should be imposed until the technology is further regulated. In his view, there is a balance between the public security and safety benefits of FRT and the human rights challenges with the technology. The important thing is to know when to deploy the technology. For the TPS, it is only in major crimes and major cases.

Mr. Therrien also said he was not in favour of a complete moratorium. He said that a moratorium can be imposed by legislation only. The Commissioner does not have the power to impose a moratorium. The position of the federal, provincial and territorial privacy commissioners is that legislation should prescribe when FR can be used for legitimate, helpful purposes and social good (e.g., investigating serious crimes or finding missing children). The legitimate uses should be defined narrowly, and the law should also prescribe prohibited uses. That ban would be a partial moratorium on the use of FRT.

Mr. Therrien said he believes in the use of FRT in compelling circumstances. He said that, if the RCMP were to use FRT only according to its new policy (targeted, time-limited use, subject to verification by trained experts, and as an investigational aid, not to confirm an

---

67   ETHI, *Evidence*, Brenda McPhail. Ms. McPhail gave the example of a U.S. bill to place a moratorium on government use of facial recognition technology until rules governing its use are in place; Congress.gov., "Text - S.3284 - 116th Congress (2019-2020): Ethical Use of Facial Recognition Act," 12 February 2020. The bill was referred to a U.S. Senate committee, but has not made further progress.

68   ETHI, *Evidence*, Owen Larter, 1550 and 1610.

identity) that would also be a form of voluntary partial moratorium until the legislation is improved.[69]

With respect to bans, Ms. McPhail said that CCLA supports a complete ban on mass surveillance uses of FRT.[70] Dr. Molnar said that there are ongoing discussions in Europe about an outright ban on biometric mass surveillance, high-risk FRT and AI lie detectors in migration and border management. She said Canada should ban the high-risk use of FRT at the border. Mr. Farooq said that the use of real-time FRT at airports and borders should be banned. Ms. Bhandari recommended banning government and law enforcement use of FRT. Mr. Israel recommended a permanent ban on the use of automated, live biometric recognition by police in public spaces.

In addition to a moratorium or ban, Mr. Khanna suggested adopting a digital charter of rights for Canadians that would recognize the sanctity of personal data, like facial data. Such a charter could align with the *Canadian Charter of Rights and Freedoms*. He said it would allow Canadians to own and have a portable and secure form of biometric data that is considered sacrosanct. He also encouraged legislators to use scenario planning to inform resilient strategy and public policy in the face of digital advances.

Privacy Guidance on Facial Recognition for Police Agencies

On 2 May 2022, the federal privacy commissioner and his provincial and territorial counterparts issued guidance on facial recognition for police agencies.[71]

Mr. Therrien explained that the guidance is meant to assist police in ensuring that any use of FRT complies with the law, minimizes privacy risks and respects privacy rights. He said that the guidance was developed following a national public consultation with a broad range of people. Stakeholders agreed that current laws were inadequate. However, there was no consensus on the content of a new law.[72]

---

69   ETHI, *Evidence*, Daniel Therrien, 1135 and 1210.

70   See also: Ligue des droits et libertés Brief, p. 8. The organization believes that three uses of FRT should be immediately prohibited through legislation: mass surveillance of public places; mass online surveillance; and use of image banks created by public agencies or departments.

71   OPC, *Privacy guidance on facial recognition for police agencies*, May 2022.

72   Stakeholders representing civil society, minority groups and the police itself participated in the consultation. Mr. Therrien met a number of times with the Royal Canadian Mounted Police and the Canadian Association of Chiefs of Police. His colleagues also met with provincial equivalents.

Mr. Therrien noted that, until the laws are amended, the guidance offers advice to police on how to use FRT under current laws. He hopes that the guidance will mitigate risks.

Mr. Therrien also acknowledged that some stakeholders wanted the guidance provided by the commissioners to include advice on use cases. While he agreed on the need for advice on particular uses in different contexts, he said the commissioners thought it important and relevant to have general guidance that can be augmented as use cases are developed.

Ms. Kosseim said it may take several years before there is any jurisprudence on FRT under the Charter. It is why the commissioners recommend the adoption of a legislative framework. In the interim, they developed the guidance to help mitigate risks.

Ms. Kosseim presented the five key elements of the guidance:

> First, before using facial recognition for any purpose, police agencies must establish that they are lawfully authorized to do so. This is not a given, and cannot be assumed …
>
> Second, police agencies must establish strong accountability measures. This includes designing for privacy at every stage of a facial recognition initiative and conducting a privacy impact assessment, or PIA, to assess and mitigate risks in advance of implementation …
>
> Third, police agencies must ensure the quality and accuracy of personal information used as part of a facial recognition system to avoid false positives, reduce potential bias and prevent harms to individuals and groups …
>
> Fourth, police agencies should not retain personal information for longer than necessary …
>
> Fifth, policy agencies must address transparency and public engagement. Direct notice about the use of facial recognition may not always be possible in the context of a specific police investigation. However, transparency at the program level is certainly possible.

Ms. Kosseim also made clear that any communication with the public should be two-way. She said that key stakeholders, particularly representatives of over-policed groups, should be consulted in the very design of a police service's FR program. She added that, given the importance of reconciliation in Canada, this must include input from Indigenous groups and communities.

Ms. Kosseim said that the basic principles advanced in the guidance should apply regardless of the sector, but with the necessary adjustments for other contexts and the range of risks at play, since it was specifically designed for police services.

Mr. Therrien made similar comments, noting that the common factor that applies horizontally to all stakeholders who would like to use FRT, whether police services, businesses or government, is the principle of necessity and proportionality. For example, in police services, the use of FRT can have extremely serious consequences, resulting even in the loss of freedom. A total prohibition on its use by police services in certain circumstances might not necessarily apply to all stakeholders. He confirmed that the recommendations made by the commissioners can apply to the use of FRT in public spaces as well.

Legislation

With respect to regulating FRT and AI, most witnesses agreed that, while the current legislative framework provides some protections, it is insufficient.

For example, Mr. Therrien said that there is a patchwork of laws that govern FR: the *Canadian Charter of Rights and Freedoms*, the common law and certain other laws, including privacy legislation.[73] The problem, he says, is that this patchwork of laws can be used in many ways. He believes that current rules are too vague to give the necessary level of trust that citizens should have in the collection of information by the public and private sector.

Ms. Piovesan made similar comments. She said there are some protections under current federal privacy laws (the *Privacy Act* and PIPEDA) that apply to the use of FRT. For example, she said that the PIPEDA requires companies to obtain consent to collect highly sensitive data and, for public actors, regulation and the common law govern how certain information can be collected, stored and retained. However, she said that there is no comprehensive or really focused law around FRT.

Prof. Thomasen explained that facial surveillance systems are socio-technical systems. They cannot be understood only by looking at how a system is built: "One must also look at how it will interact with the people who use it, the people affected by it and the social environments in which it is deployed." She added that part of the socio-technical context in which facial surveillance is introduced includes gaps in the application and underlying theories of laws of general application, and these laws do not adequately protect against misuses of this technology.

---

73   CMTD and CPE Brief, p. 4; ICLMG Brief, p. 4. These stakeholders also referred to Canada's obligations under article 12 of the *Universal Declaration of Human Rights* and articles 17 and 21 of the *International Covenant on Civil and Political Rights*.

The Committee notes that Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, introduced in the House of Commons in June 2022, if passed in its current form, could address certain gaps in the current privacy legislative framework that may apply to FRT and AI.[74] However, since the bill has not yet been passed, the Committee is making its recommendations based on the legislative framework in place.

Legislative Framework for the Public and Private Sector

To shape a relatively comprehensive regulatory framework for FRT that mitigates the threat this technology poses and takes advantage of its real beneficial possibilities, Ms. Piovesan said that Canada should consider four AI principles that align with the Organisation for Economic Co-operation and Development (OECD) AI Principles[75] and leading international guidance on responsible AI. The OECD AI Principles are technical robustness, accountability, lawfulness and fairness.

For example, she said that, with respect to technical robustness, questions that should inform regulation include what specific technical criteria ought to be associated with FRT use cases and whether independent third parties should be engaged as oversight to assess FRT from a technical perspective. In terms of accountability, questions include what administrative controls should be required (e.g., an impact assessment), how are those controls determined and by whom, and what stakeholders should be consulted. With respect to lawfulness, questions include what oversight is needed to promote alignment of FRT uses with societal values and the law. Finally, with respect to fairness, questions about the adverse effects of FRT on rights and freedoms and ways to minimize these effects must be asked.[76]

The Committee notes that witnesses have proposed various legislative measures that would address many of the issues raised by Ms. Piovesan.

---

74 LegisInfo, Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, 44th Parliament, 1st Session (Bill C-27). The bill was introduced in the House of Commons on 16 June 2022; Sabrina Charland, Alexandra Savoie, Ryan van den Berg, *Legislative Summary of Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, Publication No. 44-1-C27-E, 12 July 2022.

75 Organisation for Economic Co-operation and Development (OECD), *OECD AI Principles overview*.

76 ETHI, *Evidence*, Carole Piovesan.

With respect to enforcement, several witnesses recommended granting the federal privacy commissioner greater powers, including the power to make orders and impose stiff fines such as those found in the General Data Protection Regulation (GDPR) from the European Union.[77] Mr. Therrien himself said that the powers of his office should be strengthened to make its decisions binding.[78]

As for consent, Ms. Piovesan said that, although it depends on the use case, consent should not be thrown out as a requirement for immutable biometric data. She said that "[h]aving appropriate notice, with some ability for that individual to make decisions about how they share that information or how it's collected, is really critical." Ms. Khoo also agreed that Canadians must be able to give prior and informed consent to their data being collected.

Dr. LaPlante said that regulations need to provide FRT developers, deployers and users with clear requirements and obligations regarding the specific uses of this technology, including "the requirement to gain affirmed consent for the collection and use of biometric data, as well as purpose limitation to avoid function creep." She added, however, that regulations should seek to take a balanced approach that reduces the administrative and financial burdens for public and private entities where possible.

Mr. Israel recommended that both the *Privacy Act* and PIPEDA be amended so that the collection, use and disclosure of biometric information requires express consent in all contexts. He also recommended that biometric information be defined as sensitive, as is the case in Quebec law.[79] Ms. Bhandari said that a consent requirement before biometrics are captured is critical. Mr. Labonté said people need to be aware of how their data is going to be used and give informed consent.

However, Ms. Poitras said that obtaining consent from people in the context of FR is not always appropriate because there is a power asymmetry, whether between the citizen and the state or the citizen and a major corporation, like the web giants.[80] She explained

---

77   ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Carole Piovesan; ETHI, *Evidence*, Tim McSorley; ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Tamir Israel; ICLMG Brief, pp. 8–10.

78   Bill C-27, if passed in its current form, would grant the Privacy Commissioner the power to make binding orders. However, it would not grant the Commissioner the power to impose fines or penalties. This power would be granted to the new tribunal established by the bill. See sections 94 and 95 of the proposed Consumer Privacy Protection Act (CPPA).

79   See also: CMTD and CPE Brief, p. 5. These stakeholders also recommended that federal privacy laws be amended to provide special protection for biometric information, including notice and consent prior to its use or legislative permission.

80   See also: ETHI, *Evidence*, Elizabeth Anne Watkins.

that the way to mitigate consent is to legally authorize acceptable uses and prohibit others uses, because even with consent or authorization, they are not appropriate in a democratic society.

Mr. McSorley recommended that private sector privacy laws be based on human rights and on necessity and proportionality. Regulations should have clear rules on consent, and the rules should apply to AI oversight and development in the private sector.[81] Dr. LaPlante also said that FRT legislation should be based on the principles of necessity and proportionality.

With respect to the public sector, Mr. McSorley recommended the clear establishment of no-go zones and clear rules around the issuance of privacy impact assessments. He also recommended having a mandatory review of algorithmic and biometric surveillance tools used by law enforcement to assess their human rights impact, accuracy, and bias.

Ms. Polsky said that laws must be enacted requiring everyone who creates, purchases or uses technology to demonstrate a clear and correct grasp of Canadian laws and privacy rights. In the same way that vehicles and foods must meet stringent government regulations before being allowed for sale or use, creators of technologies should be subject to laws requiring that technologies undergo comprehensive independent examination of their privacy access and algorithmic integrity as well as their bias and impact.[82]

Ms. Polsky suggested that the technology be tested in a neutral sandbox run by the Privacy Commissioner and involving other civil society groups to approve it before it is allowed for sale in Canada. The Centre for Media, Technology and Democracy and the Cybersecure Policy Exchange recommended that the *Privacy Act* and PIPEDA be harmonized with the federal government's *Directive on Automated Decision-Making*.[83]

Mr. Israel suggested a similar approach. He argued that the onus is on the government to justify the use of FRT. He recommended that the *Privacy Act* and PIPEDA be amended to legally require companies and government agencies to file impact assessments with

---

81   Ibid.

82   Ibid. Section 15 of the Artificial Intelligence and Data Act created by Bill C-27 authorizes the Minister designated under the Act to order, if the Minister has reasonable grounds to believe that a person has contravened the requirements under the Act, that an organization conduct an audit of the possible contravention or engage an independent auditor to conduct the audit and provide a report to the Minister. The audit would not be done before the product is commercialized. The obligations in the Artificial Intelligence and Data Act would not apply to government institutions.

83   CMTD and CPE Brief, p. 5.

the Privacy Commissioner prior to adopting intrusive technologies. The Commissioner should be empowered to review these technologies through a public regulatory process and to put in place usage limitations or even moratoria where necessary.[84]

Mr. Israel also said it is important to legislate a human in the decision-making loop on AI technologies, although he noted that human intervention does not solve all bias problems. He said that, when using facial recognition systems, the tendency is to trust in the automated results and assume an accurate match, which can end up embedding cognitive biases. Mr. Farooq also agreed that human checks are important, but said that in law enforcement, for example, given the problem of systemic racism and bias within police agencies, courts are the place to get those checks and balances.

With this understanding, Mr. Mohammad recommended that the government put forth clear privacy legislation that severely curtails how FRT can be used in the non-consumer context. According to the NCCM, such a law should impose a blanket ban on FRT by the government without judicial authorization, particularly for national security agencies. It should also set out clear penalties for agencies that violate privacy rules. Mr. Farooq said that the process for using FRT should be similar to the process police must follow to obtain a search warrant: appear before a judge and put forward an argument with clear documentation (evidence).[85]

With respect to the PIPEDA, Mr. Therrien explained that principles-based, technology-neutral legislation for the private sector makes sense as a starting point. However, he said that FRT shows the limits of the virtues of a principles-based approach, because such an approach leaves a lot of discretion, for example to the police, to exercise those broad principles in a way that suits their interests. Because of the risks of FRT, Mr. Therrien said there ought to be specific provisions to prohibit uses except in certain

---

84   Bill C-27 proposes to create an Artificial Intelligence and Data Act (AI Act), which imposes certain requirements on high impact artificial intelligence systems. The Privacy Commissioner is not responsible for the administration of this Act. That responsibility will rest with the Minister of Industry, or the minister designated under the Act. The minister may designate a senior official of the department over which the Minister presides to be called the Artificial Intelligence and Data Commissioner. There is no explicit requirement for privacy impact assessments in the proposed AI Act.

85   ETHI, *Evidence*, Mustafa Farooq.

circumstances.[86] He said that the commissioners recommend that legislation define "allowable" and "prohibited" uses.

For her part, Ms. McPhail told the Committee that attention must be paid not only to technical privacy protections, but also to contextually relevant protections for the full set of rights engaged by this technology. She recommended a cross-sector data protection law grounded in a human rights framework. She noted that targeted laws governing biometrics or algorithmically driven technologies could be even better fit for purpose. A comprehensive and effective legislation that applies to FRT should provide a clear legal framework for the use of FRT, rigorous accountability and transparency provisions, independent oversight and effective means of enforcement for failure to comply.

Mr. Therrien also noted that FRT brings rights other than to privacy into play, such as the right to equality and democratic rights. He said it was therefore possible to have a number of regulatory agencies, including the OPC, responsible for oversight. For example, the Canadian Human Rights Commission or its provincial equivalents could be responsible in cases of discrimination.

Mr. Khanna said that legislation on FRT should be based on research and insight on racialized minorities, First Nations, children and anyone who is more vulnerable to this sort of exploitation. For example, he recommended consulting UNICEF's policy guidance on AI for children.[87] He also underscored the need to draw on what people know within industry to equalize and create a proper symmetry between what legislators know and what companies using that technology know.

Ms. Polsky, on the other hand, said that standards should be set without the direct or indirect influence or input of industry.[88] She also suggested replacing fragmented legislation at the federal, provincial and territorial levels with one overarching piece of legislation that covers the public sector, the private sector, the non-profit sector and political parties.

---

86   Bill C-27, if passed in its current form, creates an Artificial Intelligence and Data Act that regulates international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems. The Act would also prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests.

87   UNICEF, *Policy Guidance on AI for Children*. The report highlights toys that interact with children through AI and the risks they pose around children's security and privacy (p. 24).

88   ETHI, *Evidence*, Sharon Polsky.

Finally, some witnesses suggested that changes could also be made to non-privacy legislation.

For example, Mr. Therrien said that, if certain circumstances required a court warrant for the use of FRT, amendments to the *Criminal Code* may be required. Mr. Israel recommended amending the *Criminal Code* to limit law enforcement use of FRT to investigations of serious crimes and in the absence of reasonable grounds to believe. Mr. Farooq mentioned the possibility of amendments to the *Royal Canadian Mounted Police Act* or the *Canadian Security Intelligence Service Act*, but did not specify which provisions should be amended.

Legislative Framework for Police Services

Ms. Kosseim said the commissioners' main recommendation is that police agencies establish a comprehensive statutory regime governing their use of FRT. Clear guardrails with force of law are necessary to ensure that police agencies can make use of FRT, grounded in a transparent framework and capable of earning the public's enduring trust.

Mr. Therrien explained that he and his colleagues believe that the legislative framework that should apply to the use of FRT by police agencies should be based on four elements:

> First, we recommend that the law clearly and explicitly define the purposes for which police would be authorized to use facial recognition technology and that it prohibit other uses. Authorized purposes should be compelling and proportionate to the very high risks of the technology.
>
> Second, since it is not realistic for the law to anticipate all circumstances, it is important, in addition to limitations on authorized purposes, that the law also require police use of facial recognition to be both necessary and proportionate for any given deployment of the technology.
>
> Third, we recommend that police use of facial recognition should be subject to strong, independent oversight. Oversight should include proactive engagement measures such as privacy impact assessments, or PIAs; program level authorization or advance notification before use; and powers to audit and make orders.
>
> Finally, we recommend that appropriate privacy protections be put in place to mitigate risks to individuals, including measures addressing accuracy, retention and transparency in facial recognition initiatives.

Mr. Therrien raised the possibility, for example, that a police force's program to use FRT require a privacy commissioner's authorization. He suggested that, once the technology

is adopted and actually used, oversight should include the authority to investigate complaints and make orders as to the lawfulness of the use of the technology in a given case.

The Canadian Human Rights Commission indicated that the legal framework for police use of FRT should take a human-rights-based approach that integrates protections for children and youth. Such an approach uses international human rights as a foundation.[89]

Best Practices in Other Jurisdictions

Ms. Poitras said that, in Quebec, biometric databases and the use of biometrics for identification purposes are governed by the *Act to establish a legal framework for information technology* and by privacy statutes applicable to public and private organizations.[90] Under this act, the creation of every biometric database must be reported to the CAI. As of September 2022, reporting will also be required for every instance in which biometrics are used for identification purposes. Ms. Poitras said that Quebec's act could be improved by expanding its scope. The act establishes obligations only where biometrics, including FRT, are used to verify identity. However, FRT can be used for other purposes.

Ms. Poitras explained that, in Quebec:

> [B]iometrics may not be used for identification purposes without the express consent of the person concerned. No biometric characteristic may be recorded without that person's knowledge. Only a minimum number of biometric characteristics may be recorded and used. Any other information that may be discovered based on those characteristics may not be used or preserved. Lastly, biometric information and any note concerning that information must be destroyed when the purpose of the verification or confirmation of identity has been achieved. The commission has broad authority and may make any order respecting biometric banks, including authority to suspend or prohibit their bringing into service or order their destruction. General privacy protection rules also apply in addition to these specific provisions. That means, for example, that the use of facial recognition must be necessary and proportionate to the objective pursued.

---

89   CHRC Brief, pp. 5–8. The five elements of a human-rights-based approach are legality, non-discrimination, participation, empowerment and accountability.

90   Quebec, *Act to establish a legal framework for information technology*, chapter C-1.1; Quebec, *Act respecting access to documents held by public bodies and the protection of personal information* [Quebec public sector act] chapter A-2.1; Quebec, *Act respecting the protection of personal information in the private sector*, chapter P-39.1 [Quebec private sector act].

Ms. Poitras added that a privacy impact assessment will be mandatory in Quebec as of September 2023 and that biometric information will be expressly designated as sensitive personal information.[91]

In the U.S., Mr. Larter said that Washington State passed legislation in 2021 that lays out important transparency and accountability measures for the use of FRT, including a testing requirement and oversight by an appropriately trained human.[92] In Utah, the bill entitled S.B. 34 Governmental Use of Facial Recognition Technology, passed in 2021, requires government entities to notify individuals whenever they are capturing images that could be used in conjunction with FRT and to provide 30 days prior notice to the proposed use.[93]

In 2008, Illinois passed the Biometric Information Privacy Act (BIPA). The act prohibits companies from selling or otherwise profiting from consumers' biometric information.[94] Dr. Watkins said that the BIPA allowed a lawsuit to be filed against Facebook for using facial recognition in their photo identification processes.[95] Ms. Bhandari added that the act also allowed the ACLU to file a lawsuit against Clearview AI, which resulted in a settlement. Under the settlement, the company can no longer provide access to its database containing hundreds of millions of face prints to private entities across the U.S., with a few exceptions, and is banned from selling its technology to Illinois law enforcement for five years.[96]

Ms. Bhandari advocated for the adoption of legislation like the Illinois BIPA, but with some updates. She said biometric privacy law should clearly require companies to obtain notice and written consent before collecting, using, or disclosing any person's identifier. It should prohibit companies from withholding services from people who choose not to

---

91   National Assembly of Quebec, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*. Passed in September 2021, this bill amends the Quebec public sector act and the Quebec private sector act to include this obligation. With some exceptions, the provisions of the bill come into force on 22 September 2023.

92   Washington State Legislature, SB 6289 – 2019-20, Concerning the use of facial recognition services. Under the bill, Washington State and local agencies, including law enforcement, that use or plan to use facial recognition technology must meet certain reporting and deployment requirements.

93   OPC, *Letter to the Committee*, 13 May 2022, p. 3.

94   Ibid.

95   The Committee invited Facebook to appear before it as part of its study, but it declined, stating that Facebook no longer uses facial recognition technology; Meta, *An Update On Our Use of Face Recognition*, 2 November 2021. Google was also invited but declined. Amazon accepted an invitation to testify but could not appear after a change in schedule. None of these companies submitted a brief.

96   ACLU, *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law*, 9 May 2022, News release.

consent. It should also require businesses to delete biometric identifiers after one year of the individual's last interaction with the business.[97]

Ms. Bhandari named two other models to follow. In Maine, the proposed An Act To Regulate the Use of Biometric Identifiers would require private entities to obtain the express consent of individuals to collect, use and disclose biometric identifiers. The law would also prohibit the sale of biometric data and impose limits on data storage. In Maryland, a bill entitled the Biometric Data Privacy Act has been introduced. It seeks to create a framework similar to the one in Illinois.[98]

Mr. Therrien mentioned federal laws proposed in the U.S., including the Fourth Amendment Is Not For Sale Act, which would stop data brokers from selling personal information to law enforcement agencies without court oversight and would ban the use of data that was illegally obtained by public agencies.[99] The Algorithmic Accountability Act would require private organizations to conduct assessments of automated decision systems for algorithmic bias and effectiveness.[100]

With respect to Europe, several witnesses said that the GDPR is a model for data protection.[101] Under the GDPR, biometrics, including facial images, are considered a special category of data that is prohibited, unless the controller can rely upon a legal ground and a ground for processing.[102]

Ms. Piovesan said that the GDPR includes a right to recourse and a right to objection on profiling solely by automatic means.[103] She also said that, under the GDPR, fines can be imposed for the use of data of European residents, even if the actual activity does not

---

97   Bill C-27, if passed in its current form, contains a right to opt out in section 55 of the new CPPA.

98   ACLU, *LD 1945 Biometric Identifiers: Fact Sheet*, Document submitted to the ETHI Committee, 21 June 2022 (Maine bill); ACLU, *HB 259 – The Biometric Data Privacy Act: Amendment Recommendations & Fact Sheet* (Maryland), Document submitted to the ETHI Committee, 21 June 2022 (Maryland bill). The ACLU said that several amendments made to the text of the original bill by the Maryland House of Representatives weakened the bill.

99   OPC, *Letter to the Committee*, 13 May 2022, p. 2. An identical bill was introduced in the Senate: S.1265 - Fourth Amendment Is Not For Sale Act.

100   OPC, *Letter to the Committee*, 13 May 2022, p. 2. An identical bill was introduced in the Senate: S.3572 - Algorithmic Accountability Act of 2022.

101   ETHI, *Evidence*, Ana Brandusescu; ETHI, *Evidence*, Elizabeth Anne Watkins.

102   European Union, EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); OPC, *Letter to the Committee*, 13 May 2022, p. 2.

103   She noted that a similar right exists under Quebec law as well.

take place in the European jurisdiction. The GDPR therefore has extra-jurisdictional applicability. Dr. Watkins said that the GDPR contains a right to an explanation that ensures, for example, that companies have to provide workers with insights into how decisions are made about them by automated systems.[104]

The European Union directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, was also raised by witnesses.[105] It forbids law enforcement from processing biometric data for the purpose of uniquely identifying a person except where authorized by law and from making decisions based solely on automated processing, including profiling, unless European Union or domestic law provides appropriate safeguards for individual rights and freedoms.[106]

Finally, some witnesses brought up the European Union's proposed Artificial Intelligence Act.[107] Mr. Therrien explained that the act, if adopted:

> would outlaw public and private sectors from using harmful AI applications that, among other things, manipulate individuals or exploit vulnerabilities of individuals due to certain personal characteristics. Non-prohibited applications that are high-risk (including use of biometrics for identification and categorization) are subject to specific legal requirements such as risk management measures and systems; logging and record-keeping; general human oversight; accurate and representative data for AI training; ex-ante conformity assessments; and, demonstrable accountability.[108]

Mr. Therrien said that the European proposal protects constitutional and human rights. Ms. Kosseim and Ms. Poitras agreed with him.

---

104   Bill C-27, if passed in its current form, contains a right to an explanation in sections 63 and 64 of the CPPA.

105   "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA," *Official Journal of the European Union*.

106   CMTD and CPE Brief, p. 8.

107   European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts; ETHI, *Evidence*, Petra Molnar; ETHI, *Evidence*, Cynthia Khoo; ETHI, *Evidence*, Alex LaPlante.

108   OPC, *Letter to the Committee*, 13 May 2022, p. 2.

[Ms. Piovesan](#) said that a risk-based approach to the regulation of AI, as the European proposal does, is seen in other jurisdictions. The European proposal would also prohibit the use of real-time FRT in public spaces for law enforcement purposes.[109]

[Dr. Molnar](#) said the EU proposal recognizes that individual risk assessments for the purposes of immigration and refugee processing are high-risk and bans assessments that can be used for profiling and for strengthening systemic discrimination.

With respect to the United Kingdom, [Prof. Jenkins](#) brought up the Surveillance Camera Code of Practice, which provides guidance on the appropriate use of surveillance camera systems by local authorities or police. The code states that the use of FRT should always involve human intervention before decisions are taken that affect an individual adversely.[110] The Biometrics and Surveillance Camera Commissioner is an independent monitoring body that encourages compliance with the code of practice.[111] Scotland has also had a biometrics commissioner since 2020, who published a draft code of practice in April 2022.[112]

Committee Observations and Recommendations

The Committee found that witnesses clearly demonstrated the inadequacy of the current legislative framework for the regulation of FRT and AI. The Committee therefore makes the following recommendations:

Recommendation 11

That the government define in appropriate legislation acceptable uses of facial recognition technology or other algorithmic technologies and prohibit other uses, including mass surveillance.

---

109   ETHI, *Written response submitted to the Committee by Sharon Polsky*, 17 June 2022; European Parliamentary Research Service, *[STOA study on diverging obligations facing public and private sector applications of artificial intelligence](#)*.

110   United Kingdom, Home Office, *[Surveillance Camera Code of Practice, 2021](#)*.

111   United Kingdom, *[Biometrics and Surveillance Camera Commissioner](#)*; See also: ETHI, *Written response submitted to the Committee by Sharon Polsky*, 17 June 2022.

112   Scotland, *[Scottish Biometrics Commissioner](#)*; United Kingdom, *[Scottish Biometrics Commissioner Act 2020](#)*; See also: ETHI, *Written response submitted to the Committee by Sharon Polsky*, 17 June 2022. In April 2022, the Scottish Commissioner published a draft [code of practice](#) on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland.

Recommendation 12

That the Government of Canada amend the *Privacy Act* to require that prior to the adoption, creation, or use of facial recognition technology, government agencies seek the advice and recommendations of the Privacy Commissioner, and file impact assessments with his or her office.

Recommendation 13

That the Government of Canada update the *Canadian Human Rights Act* to ensure that it applies to discrimination caused by the use of facial recognition technology and other artificial intelligence technologies.

Recommendation 14

That the Government of Canada implement the right to erasure ("right to be forgotten") by requiring service providers, social media platforms and other online entities operating in Canada to delete all users' personal information after a set period following users' termination of use, including but not limited to uploaded photographs, payment information, address and contact information, posts and survey entries.

Recommendation 15

That the Government of Canada implement an opt-in-only requirement for the collection of biometric information by private sector entities and prohibit such entities from making the provision of goods or services contingent on providing biometric information.

Recommendation 16

That the Government of Canada strengthen the ability of the Privacy Commissioner to levy meaningful penalties on government institutions and private entities whose use of facial recognition technology violates the *Privacy Act* or the *Personal Information Protection and Electronic Documents Act* to deter future abuse of the technology.

Recommendation 17

That the Government of Canada amend the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to prohibit the practice of capturing images of Canadians from the internet or public spaces for the purpose of populating facial recognition technology databases or artificial intelligence algorithms.

Recommendation 18

That the Government of Canada impose a federal moratorium on the use of facial recognition technology by (Federal) policing services and Canadian industries unless implemented in confirmed consultation with the Office of the Privacy Commissioner or through judicial authorization; that the Government actively develop a regulatory framework concerning uses, prohibitions, oversight and privacy of facial recognition technology; and that the oversight should include proactive engagement measures, program level authorization or advance notification before use, and powers to audit and make orders.

Recommendation 19

That the federal government ensure that appropriate privacy protections are put in place to mitigate risks to individuals, including measures addressing accuracy, retention and transparency in facial recognition initiatives as well as a comprehensive strategy around informed consent by Canadians for the use of their private information.

CONCLUSION

The Committee's study confirmed that Canada's current legislative framework does not adequately regulate FRT and AI. Without an appropriate framework, FRT and other AI tools could cause irreparable harm to some individuals.

The Committee is therefore of the view that, when FRT or other AI technology is used, they must be used responsibly, within a robust legislative framework that protects Canadians' privacy rights and civil liberties. Since such a legislative framework does not exist at the time, a national pause should be imposed on the use of FRT, particularly with respect to police services.

The Committee strongly encourages the Government of Canada to implement its recommendations as quickly as possible.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
As an individual	2022/03/21	11
Ana Brandusescu, Artificial Intelligence Governance Expert		
Cynthia Khoo, Research Fellow The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto		
Kristen Thomasen, Professor Peter A. Allard, School of Law, University of British Columbia		
INQ Law	2022/03/21	11
Carole Piovesan, Managing Partner		
Refugee Law Lab	2022/03/21	11
Petra Molnar, Lawyer York University		
Borealis AI	2022/03/24	12
Alex LaPlante, Senior Director Product and Business Engagement		
Canadian Civil Liberties Association	2022/03/24	12
Brenda McPhail, Director Privacy, Technology and Surveillance Program		
Computer Research Institute of Montréal	2022/03/24	12
Françoys Labonté, Chief Executive Officer		
International Civil Liberties Monitoring Group	2022/03/24	12
Tim McSorley, National Coordinator		

Organizations and Individuals	Date	Meeting
As an individual	2022/04/04	15
Rob Jenkins, Professor University of York		
Sanjay Khanna, Strategic Advisor and Foresight Expert		
Angelina Wang, Computer Science Graduate Researcher Princeton University		
Elizabeth Anne Watkins, Postdoctoral Research Associate Princeton University		
Royal Canadian Mounted Police	2022/04/28	17
André Boileau, Officer in Charge National Child Exploitation Crime Centre		
Paul Boudreau, Acting Deputy Commissioner Specialized Policing Services		
Toronto Police Service	2022/04/28	17
Colin Stairs, Chief Information Officer		
Toronto Police Services Board	2022/04/28	17
Dubi Kanengisser, Senior Advisor Strategic Analysis and Governance		
Commission d'accès à l'information du Québec	2022/05/02	18
Diane Poitras, President		
Office of the Information and Privacy Commissioner of Ontario	2022/05/02	18
Patricia Kosseim, Commissioner		
Vance Lockton, Senior Technology and Policy Advisor		
Office of the Privacy Commissioner of Canada	2022/05/02	18
Daniel Therrien, Privacy Commissioner of Canada		
David Weinkauf, Senior Information Technology Research Analyst		
Microsoft	2022/05/05	19
Owen Larter, Director Responsible Artificial Intelligence Public Policy		
National Council of Canadian Muslims	2022/05/05	19
Mustafa Farooq, Chief Executive Officer		
Rizwan Mohammad, Advocacy Officer		

Organizations and Individuals	Date	Meeting
Royal Canadian Mounted Police	2022/05/09	20
André Boileau, Officer in Charge National Child Exploitation Crime Centre		
Gordon Sage, Director General Sensitive and Specialized Investigative Services		
Roch Séguin, Director Strategic Services Branch, Technical Operations		
Toronto Police Service	2022/05/09	20
Colin Stairs, Chief Information Officer		
As an individual	2022/06/09	25
Nestor Maslej, Research Associate Institute for Human-Centered Artificial Intelligence, Stanford University		
Privacy and Access Council of Canada	2022/06/09	25
Sharon Polsky, President		
American Civil Liberties Union	2022/06/16	27
Esha Bhandari, Deputy Director		
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic	2022/06/16	27
Tamir Israel, Staff Lawyer		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Canadian Human Rights Commission

Centre for Media, Technology and Democracy

Cybersecure Policy Exchange

Jenkins, Rob

International Civil Liberties Monitoring Group

Ligue des droits et libertés

Maslej, Nestor

Refugee Law Lab

Tessono, Christelle

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 11, 12, 15, 17-20, 25, 27, 28, 34 and 35) is tabled.

Respectfully submitted,

Pat Kelly
Chair