Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Police use of Facial Recognition Technology in Canada and the Way Forward

Special Report to Parliament

June 10, 2021

The html version of this special report takes precedence over this document in case of a conflict or discrepancy.

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

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Cat. No. IP54-110/2021E-PDF
ISBN 978-0-660-39086-4

Commissaire à la protection
de la vie privée du Canada

Privacy Commissioner
of Canada

BY EMAIL

June 10, 2021

The Honourable George J. Furey, Senator
The Speaker
Senate of Canada
Ottawa, Ontario K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament the Special Report of the Office of the Privacy Commissioner of Canada entitled *Police Use of Facial Recognition Technology in Canada and the Way Forward.* This tabling is done pursuant to section 39(1) of the *Privacy Act*.

Sincerely,

Original signed by

Daniel Therrien
Commissioner

Commissaire à la protection
de la vie privée du Canada

Privacy Commissioner
of Canada

BY EMAIL

June 10, 2021

The Honourable Anthony Rota, M.P.
The Speaker
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Special Report of the Office of the Privacy Commissioner of Canada entitled *Police Use of Facial Recognition Technology in Canada and the Way Forward*. This tabling is done pursuant to section 39(1) of the *Privacy Act*.

Sincerely,

Original signed by

Daniel Therrien
Commissioner

Table of contents

1. Commissioner's Message

Facial Recognition Technology (FRT) has emerged as a powerful tool of significant interest to both law enforcement and commercial entities. Used responsibly and in the right circumstances, it has the potential to offer great benefits to society. For instance, it can support national security objectives, assist police in solving crime or help authorities find missing persons.

The technology scales easily, costs relatively little to use, and can be deployed as an add-on to existing surveillance infrastructure, which might explain its growing appeal in Canada and abroad, particularly by police agencies.

At the same time, facial recognition can be a highly invasive surveillance technology fraught with many risks.

Studies have shown that it can provide racially biased results and, given the chilling effect it can have on certain activities, it has the potential to erode privacy and undermine freedoms and human rights such as free expression and peaceful assembly. Repositories of FRT data are also high value targets for malicious actors and must be safeguarded accordingly.

FRT involves the collection and processing of very sensitive personal information. Biometric facial data is unique to each individual, unlikely to vary significantly over time and it is difficult to change in its underlying features. Coupled with large data sources such as the Internet, government databanks or closed circuit television, it can be a powerful intelligence and tracking tool.

The data involved in FRT speaks to the very core of individual identity and as both commercial and government use of the technology expands, it raises important questions about the kind of society we want to live in. The deployment of FRT writ large is worthy of closer examination as to whether our laws adequately protect Canadians from potential misuses of the technology. The focus of this report, however, is on the application of privacy laws and best practices to the use of FRT by police.

OPC actions and next steps

This Special Report to Parliament includes the findings of our investigation of the RCMP's use of Clearview AI, a technology company that has offered services of FRT to law enforcement and some private organizations.

Clearview AI itself was the subject of a previous investigation by the OPC, the results of which were published in February 2021.

Also included in this Special Report is draft privacy guidance on facial recognition for police agencies. A joint initiative with our counterparts in each province and territory in Canada, the draft guidance seeks to clarify police agencies' privacy obligations relating to the use of FRT, with a view to ensuring that any use of this technology complies with privacy laws, minimizes privacy risks and respects privacy rights.

We will be consulting with police forces and other stakeholders on the guidance in the weeks and months ahead. It will be important to have a public discussion on how this technology that is potentially useful, but also comes with significant risks, should be used.

Along with an earlier investigation into Cadillac Fairview – a commercial real estate company that embedded cameras inside digital information kiosks at shopping malls to estimate the gender and age of shoppers, without their knowledge or consent – we hope our work contributes to the important conversations taking place regarding the regulation of potentially disruptive technologies such as FRT.

We welcome the fact that Parliamentarians are currently seized with the issue of FRT. Just last month, I was invited before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) to discuss privacy concerns related to the technology. Committee members expressed a keen interest in our investigations into the use of FRT in the context of law enforcement.

We felt it would be a missed opportunity and a disservice to Canadians not to share details of our investigation into the RCMP's use of Clearview AI's facial recognition technology in a timely fashion, especially as the government looks to modernize Canada's privacy regime.

Overview of investigation into RCMP's use of Clearview AI

Our investigation of the RCMP's use of FRT, the full details of which appear later in this special report, is linked to a separate investigation of Clearview AI.

In that investigation, we found the company's technology allowed law enforcement and commercial organizations to match photographs of people against the company's databank of more than three billion images scraped from internet websites without users' consent.

The result was that billions of people essentially found themselves in a "24/7" police line-up. We concluded this represented mass surveillance and was a clear violation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private sector privacy law.

Now, in our investigation of the RCMP, we found that Canada's national police force contravened the *Privacy Act,* which applies to federal government institutions, when it collected personal information from Clearview AI. In essence, a government institution cannot collect personal information from a third party agent if that third party agent collected the information unlawfully.

We were also concerned that the RCMP at first erroneously told our office it was not using Clearview AI. When it later acknowledged its use, it said publicly it had only used the company's technology in a limited way, primarily for identifying, locating and rescuing children who have been, or are, victims of online sexual abuse.

However, our investigation found the RCMP did not satisfactorily account for the vast majority of the searches it made.

This highlights what our investigation revealed in more detail: that the RCMP has serious and systemic gaps in its policies and systems to track, identify, assess and control novel collections of personal information. Such system checks are critical to ensuring that the RCMP complies with the law when it uses new technology such as FRT, and new sources, such as private databases.

After we launched our investigation, the RCMP issued internal guidance to staff to restrict the use of Clearview AI and initiated a pilot "National Technology Onboarding Program" intended to systematically examine the compliance of new investigative techniques with the *Privacy Act* and the *Canadian Charter of Rights and Freedoms*.

The RCMP is no longer using Clearview AI as the company ceased to offer its services in Canada in July 2020 in the wake of our then ongoing investigation. However, we remain concerned that the RCMP did not agree with our conclusion that it contravened the *Privacy Act*. The RCMP argued section 4 of the *Privacy Act* does not expressly impose a duty to confirm the legal basis for the collection of personal information by its private sector partners. Requiring the RCMP to ensure a third party's legal compliance with PIPEDA would create an unreasonable obligation on the RCMP, the RCMP maintained.

Nonetheless, the RCMP agreed to implement our recommendations to improve its policies, systems and training. This includes conducting fulsome privacy assessments of third party data collection practices to ensure any personal information is collected and used in accordance with Canadian privacy legislation.

Activities of federal institutions must be limited to those that fall within their legal authority and respect the general rule of law. We encourage Parliament to amend the *Privacy Act* to clarify that the RCMP has an obligation to ensure that third party agents it collects personal information from have acted lawfully.

Further, the common law clearly sets limits on the RCMP's collection powers as a police body. In our view, the use of FRT by the RCMP to search through massive repositories of Canadians who are innocent of any suspicion of crime presents a significant violation of privacy and clearly warrants careful consideration against these constraints.

To be effective, such an assessment must be based on a nuanced understanding of the privacy issues at play.

Draft guidance for police agencies

We and fellow privacy regulators have drafted guidance for police agencies to clarify the circumstances and conditions under which FRT use might be appropriate.

We have not yet arrived at final positions on the conditions of use of FRT and we look forward to consulting stakeholders on our recommendations before finalizing them. The draft guidance emphasizes that police agencies must have lawful authority for the proposed use of the technology, and the importance of applying privacy protective standards that are proportionate to the potential harms involved.

The privacy principles of necessity and proportionality ensure that privacy-invasive practices are carried out for a sufficiently important objective, and that they are narrowly tailored so as not to intrude on privacy rights more than is necessary.

In other words, police should not use FRT just because it is thought to be "useful" for law enforcement in general. Police should have a specific reason to use the technology and it should be based on evidence. It is not enough to rely on general public safety objectives to justify the use of such an intrusive technology. The pressing and substantial nature of the specific objective should be demonstrable through evidence.

In some cases, potential harms may be so extreme that no amount of protection will adequately reduce privacy risks. In other cases, it may be possible to appropriately manage the risks associated with FRT through careful planning and the diligent application of privacy protections.

Accuracy, data minimization, accountability and transparency are other critical principles police agencies need to consider before using FRT.

Accuracy has been raised as a global concern given the propensity of FRT to mis-identify certain gender and racial groups. As such, decisions made about individuals should not rely solely on FRT. That means police officers should review matches before any decision to detain, investigate or charge an individual is taken.

Data minimization measures can help reduce the risk of over-broad data collection and the severity of a breach should one occur.

Accountability ensures police agencies know what is being collected, how it is being collected, by whom, for what purposes and the way in which it's being safeguarded. It ultimately ensures organizations can demonstrate their compliance with legal requirements when asked to do so.

Meanwhile, transparency measures can help ensure those who may be impacted by FRT initiatives are well informed about its use.

Besides privacy laws, the Charter also protects aspects of the right to privacy, such as the right to be secure against unreasonable search and seizure by the state. Certain intrusions on this right, however, can be justified in specific circumstances.

For instance, the *Criminal Code* provides for warrants that permit intrusion on people's privacy when a judge is satisfied there are reasonable grounds to believe an offence has been or will be committed, and that evidence of the offence will be obtained through the use of a particular technique or device. Seeking warrants and court authorizations can assist with ensuring that a proposed FRT use meets the proportionality standard.

It also bears mention that private sector actors do not enjoy the same collection authority as police. Commercial FRT vendors often compile their own databases, typically of images taken from the Internet. As noted in our guidance, if police use third-party vendors to supply facial recognition services, they should ensure that these suppliers have the lawful authority to collect and use the personal information contained in their databases, and that they don't use any data supplied to them by police for other purposes.

Law reform and other considerations

FRT raises other important considerations as the government looks to modernize Canada's privacy and data protection regime.

Canada's privacy laws were designed to be technology neutral, which is positive, given the pace of technological change compared to that of legislative modernization.

However, the risks of FRT are such that, due to the inalterable nature of the information involved, specific rules may be warranted. This is already the case for other forms of biometrics collected by law enforcement such as fingerprints and DNA profiles.

To date in Canada, Quebec is the only jurisdiction to enact a law that specifically addresses biometrics, which encompasses FRT. Quebec's *Act to establish a legal framework for information technology* requires organizations to notify the Commission d'accès à l'information before implementing a biometrics database. The regulator may then prohibit such a database from coming into service, order changes to the project, or order the destruction of the database. Furthermore, any secondary information revealed by biometric characteristics about an individual cannot be used as a basis for a decision concerning that person.

There are jurisdictions across the U.S. that have gone so far as to ban the use of FRT by police and other public bodies. The European Data Protection Supervisor has also called for an outright ban on the use of FRT in public spaces, calling it a "deep and non-democratic intrusion into individuals' private lives."

While the European Commission has stopped short of a ban, it has moved to rein in the technology. In a new regulation proposed in April to address artificial intelligence, the European Commission is seeking to restrict the use of real-time facial recognition in public spaces by law enforcement to cases involving terrorism, serious criminality and targeted searches for crime victims and missing children.

Under the proposal, such use of FRT would be subject to judicial authorization. Among the key no-go zones is using the technology subliminally to manipulate an individual's behavior in a way that is likely to be harmful. The threshold in the law is "likely to cause physical or psychological harm".

It would also designate all other remote biometric identification, including those used by commercial organizations, as "high-risk" and impose a number of obligations such as risk and quality assessments, logging and record-keeping for traceability, human oversight and demonstrable accountability.

We have seen how public-private partnerships and contracting relationships involving digital technologies, such as FRT, can create additional complexities and risks for privacy. Common privacy principles enshrined in both our public and private sector privacy laws would help address gaps in accountability where the sectors interact. It would also help address issues related to interoperability and the misalignment between our federal privacy laws and those of other jurisdictions in Canada and around the world.

To that end, Canada's federal privacy laws should share a rights-based foundation. They should include provisions on automated-decision making, including a definition, a right to meaningful explanation and human intervention related to its use. They should also clarify that the concept of publicly available personal information does not apply to information where an individual has a reasonable expectation of privacy. This is particularly critical in the case of FRT, which relies on massive databases of images.

Canada's laws should also strengthen accountability provisions by requiring a demonstration of privacy compliance upon request by the regulator. They should ensure privacy protections are built into any new product or service and that risks are considered and mitigation measures are in place before launch.

Conclusion

Privacy is nothing less than a prerequisite for freedom – the freedom to live and develop independently as persons away from the watchful eye of state bodies or commercial enterprises.

The prospect of police agencies integrating FRT into law enforcement initiatives raises the possibility of serious privacy harms unless appropriate privacy protections are in place.

Canadians must be free to participate voluntarily and actively in the regular, and increasingly digital, day-to-day activities of a modern society. They must be able to navigate public, semi-public, and private spaces without the risk of their activities being routinely identified, tracked and monitored.

While certain intrusions on this right can be justified in specific circumstances, individuals do not forego their right to privacy merely by participating in the world in ways that may reveal their face to others, or that may enable their image to be captured on camera. Privacy is vital to dignity, autonomy, personal growth and the free and open participation of individuals in democratic life. When surveillance increases, individuals can be deterred from exercising these rights and freedoms.

The process of establishing appropriate limits on FRT use remains incomplete. Unlike other forms of biometrics collected by law enforcement, facial recognition is not subject to a clear and comprehensive set of rules.

Its use is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed by the technology. This creates room for uncertainty concerning what uses of facial recognition may be acceptable, and under what circumstances.

The nature of the risks posed by FRT calls for collective reflection on the limits of acceptable use of the technology. The question of where acceptable FRT use begins and ends is in part, then, a question of the expectations we set now for the future protection of privacy in the face of ever-increasing technological capabilities to intrude on Canadians' reasonable expectations of privacy.

We look forward to engaging with police, lawmakers and other stakeholders on important questions surrounding the use of this technology.

Only through respect for the law and the values we cherish will we be able to safely enjoy the benefits of new technologies, while preserving the freedoms and rights that we proudly count on as Canadians.

2. Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)

Complaint under the *Privacy Act*

Overview

1. Clearview AI ("Clearview") is a US-based company that created and maintains a large database of images containing faces (along with associated hyperlinks to the location on the Internet where the image was found). Clearview account holders can search this database for matching faces using facial recognition technology ("FRT"). The RCMP confirmed that it purchased two licenses to use Clearview in October 2019, and that RCMP members had also used Clearview via a number of free trial accounts since that time. The Office of the Privacy Commissioner ("OPC") received a complaint under the *Privacy Act* (the "*Act*") expressing concerns about the use of Clearview by the RCMP.

2. In a related matter, on February 21, 2020, the OPC launched a joint investigation with provincial privacy authorities in Quebec, Alberta and British Columbia ("BC"), into Clearview's collection of facial images in its database and subsequent disclosure to its customers. In that investigation, we found that Clearview's personal information collection practices contravened the *Personal Information and Protection of Electronic Documents Act* ("PIPEDA"), as well as provincial privacy legislation in Quebec, Alberta, and BC.[1]

3. Section 4 of the *Privacy Act* specifies that "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution." In our view, the operating programs and activities of an institution must be limited to activities which fall within the institution's legal authority to conduct and which respect the general rule of law.

4. Following our evidentiary review and legal analyses, we find that since Clearview's personal information collection practices were not compliant with its legal obligations, the RCMP's subsequent collection of that information falls outside its legitimate operating programs and activities, thus representing a contravention of Section 4 of the *Privacy Act*.

5. Clearview's records demonstrate that the RCMP conducted hundreds of searches using Clearview FRT via at least 19 accounts across the country. In light of the significant breadth of these collections of personal information in contravention of the *Act*, to inform our recommendations for appropriate corrective action, we examined the

[1] 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.

adequacy of the RCMP's controls to ensure it complies with Section 4 of the *Act* when it collects personal information in novel ways and from new sources.

6. We found that the RCMP failed to properly assess the potential *Privacy Act* compliance risks that the use of Clearview's massive database and facial recognition technology clearly presented. Further, it did not have systems in place to track, identify, assess, and control such novel collection of personal information. We therefore recommended that, within 12 months, the RCMP institute systemic measures and pertinent training to understand, track, identify, assess, and control the novel collection of personal information to ensure collection is limited as required by the *Act*. These recommendations are not limited to the matter at hand, but apply to any new technology involving the collection or use of personal information.

7. While the RCMP disagreed with our findings that it contravened the *Act*, it nonetheless agreed to implement our recommendations and we therefore find the matter **well-founded and conditionally resolved**. Implementing the recommendations will require broad and concerted efforts across the RCMP. The RCMP has taken certain preliminary remedial steps already, such a creating a National Technology Onboarding Program unit. However, much work remains to be done to ensure adoption of changes in decision-making culture across the RCMP – supported by well-embedded processes, tools and training. We strongly encourage the RCMP to dedicate the sustained resources and senior level-championing necessary for successful implementation of its commitment to the recommendations.

Background

8. The RCMP is the Canadian national police service and a partner agency of Public Safety Canada. It provides all federal policing services in Canada and policing services under contract to the three territories, eight of the ten provinces (i.e., all except Ontario and Quebec), more than 150 municipalities, more than 600 Indigenous communities and three international airports. The RCMP have duties to enforce the law, prevent crime, and protect life. In order to meet these duties they conduct investigations, which entails the collection of information and identification of victims, offenders, or crime scenes.[2]

9. The Complainant, Member of Parliament for Timmins-James Bay Charlie Angus, expressed a range of concerns about the use of Clearview by the RCMP, which had not, at the time of his complaint in late January 2020, confirmed that it had used Clearview. Specifically the complainant wrote:[3]

> *In Canada, there have been important Indigenous-led protests against mega-resource projects, and there is a history of distrust between those participating in social protest and the RCMP. Could technology such as Clearview AI be used to identify protesters and create profiles of civic dissent? Given the power of these*

[2] Further information about the RCMP may be found here.

[3] The Complainant's complete letter of complaint has been posted on his professional website. (last verified May 17, 2021).

> *technologies, we have to be vigilant. At this time, Canadian law enforcement agencies and Clearview Al remain quite tight-lipped about the extent of their collaboration. It is imperative that we understand more about how this technology may be used on Canadians, and for what ends.*
>
> *Any use of such technology must be carried out under clear judicial oversight. However, this technology is being tested and implemented in a legislative and judicial vacuum. To this end, I ask you to launch an inquiry as to whether the RCMP or other police forces are using services such as Clearview Al. I am asking you to provide recommendations on the permissibility, limits and scope of use of facial recognition by law enforcement agencies.*

10. Following receipt of the complaint and in light of media reports about law enforcement use of Clearview, we first asked the RCMP, on January 29, 2020, if it was using Clearview FRT. At that time, the RCMP inaccurately informed the OPC that the RCMP had not used Clearview FRT.[4] It also committed to conduct Privacy Impact Assessments ("PIAs") prior to deploying facial recognition technology. However, after Clearview's client list, which included the RCMP, was reported stolen in February 2020, the RCMP then disclosed publicly, and to the OPC, that it had in fact been using personal information collected from Clearview in investigations. In response to the OPC's recommendation that the RCMP discontinue the use of Clearview FRT during the course of the investigation, the RCMP further stated its intention to continue to use Clearview FRT within its National Child Exploitation Crime Centre ("NCECC") and in other exigent circumstances.[5]

11. Moreover, despite its commitment above to the OPC to conduct PIAs prior to deploying facial recognition technology, in June 2020, eight months after commencing the collection of personal information from Clearview, the RCMP had only completed a PIA checklist – a Treasury Board Secretariat ("TBS") tool used determine if a PIA is required under TBS directives.[6]

12. The RCMP had begun using Clearview FRT in October 2019. In response to our related joint investigation of Clearview's practices, Clearview announced, on July 3, 2020 that it had ceased commercial activities related to its facial recognition tool and discontinued contracts in Canada, including those with the RCMP.

13. In the course of using paid and trial accounts, the RCMP uploaded images of individuals to Clearview, which then displayed a number of matching images using Clearview FRT. Along with each matched image, Clearview provided an associated hyperlink to the webpage from which the image had been collected.

14. According to the RCMP, Clearview accounts were created in five RCMP Divisions: National Headquarters ("NHQ"), BC, Alberta, Manitoba, and New Brunswick, including two paid NCECC licenses and 17 unpaid trial licenses.

[4] See paragraph 51 for details.

[5] See paragraph 68 for details.

[6] Under the TBS Directive on Privacy Impact Assessment.

15. The RCMP initially indicated that it was using Clearview FRT primarily for identifying, locating and rescuing children who had been, or are, victims on online sexual abuse, and that it was "aware of limited use of Clearview AI on a trial basis by a few units in the RCMP to determine its utility to enhance criminal investigations."[7]

16. In response to our question about how many search queries it made to Clearview, the RCMP told us, in May 2020, that the total number of uses by the RCMP was 78. It said 19 were for victim identification (by NCECC), 14 were to attempt to locate an identified suspect evading law enforcement, and 45 were for testing using RCMP members' own images, images of other consenting individuals, or inanimate objects. It qualified these numbers by saying that queries were not tracked unless the application was used to support an investigation - any of its responses requiring estimates relied on the individuals who used the application to estimate "to the best of their knowledge".

17. We later learned from Clearview records that it had recorded 521 searches from RCMP accounts, including 33 searches from accounts labeled "Royal Canadian Mounted Police (Victim ID)" and 488 searches from accounts labeled "Royal Canadian Mounted Police." When we asked the RCMP about the significant gap between their provided figures and those from Clearview, it told us that some of the 'uses' it originally reported to the OPC included multiple searches of the same individual. It explained that, for instance, Victim Identification specialists used images of children at different ages or different lighting, angles or focus. It also stated that prior to July 6, when it lost access to Clearview services, it *was* able to track the individual searches of Clearview, but that it could no longer do so.[8] We note, however, that the RCMP's initial response (see paragraph 16) was provided to the OPC prior to July 6th, 2020 when the RCMP still had full access from Clearview, and that these additional searches had not been factored into their response at that time.

18. In our view, while it is conceivable that the 521 searches recorded by Clearview could be linked to the 78 "uses" the RCMP reported, this does not constitute an accounting for those searches. Relying, therefore, on the search figures available to us (from Clearview records), we note that only approximately 6% appear to be linked to NCECC victim identification, and approximately 85% are not accounted for at all by the RCMP. In this context, the purposes for which the involved RCMP staff conducted these searches remains unknown.

Analysis

19. The images in question constitute "personal information" as defined in Section 3 of the *Act*, in that images of faces constitute information about an "identifiable individual." In fact, facial images are considered highly sensitive biometric information given that they are a unique and permanent characteristic of our body, largely stable over time, and a

[7] RCMP News release February 27, 2020 re use of Facial Recognition Technology

[8] It also suggested that the number of searches conducted by NCECC might be underreported – citing that the number of searches made by the NCECC "significantly exceeded" 33.

key to our identity. Additional personal information is collected via association with the hyperlinks included with images.

20. The methodological process for using Clearview FRT commences with an image being uploaded from the RCMP to Clearview. The image is analyzed by Clearview's software to mathematically map facial features. The result is then used to search Clearview's database for similar faces, with the analytical breakdown of facial features being how faces are "recognized". Clearview displays likely matches, in the form of images, to the RCMP. This constitutes a collection of information by the RCMP from Clearview. Each picture includes a hyperlink to the internet address from whence it was scraped. This allows the RCMP to collect additional contextual information from the internet if such information is still accessible. The hyperlink itself can contain personal information in some cases, depending on the web address.

Issue: The collection from Clearview was not directly related to an operating program or activity

21. Section 4 of the *Act* requires federal institutions to restrict their collection of personal information to information directly related to an operating program or activity. In order to determine if a collection meets this test, as a first step, the scope or nature of the "operating program or activity" must be clearly defined.

22. In our view, the scope or nature of an operating program or activity under Section 4 of the *Act* must be limited to lawful activities of the institution and exclude those that do not respect the general rule of law. At the conclusion of the analysis below, our investigation found that the collection of personal information from Clearview was not within the legitimate scope of the RCMP's operating programs and activities as set out in Section 4 of the *Act*.

23. As a law enforcement agency carrying out police duties, the RCMP has broad authority to collect personal information, often without the knowledge or consent of the individual involved. These police duties range from investigating serious criminality to keeping the peace. The RCMP indicated that it "has the authority under the common law, as well as under statutory law (Section 18 of the *RCMP Act*[9] and 14(1)(a) of the *RCMP Regulations*[10]) to collect, use and disclose relevant information for criminal investigative purposes, as well as to preserve the peace and protect life." It takes the view that this would include the collection of personal information from Clearview in the course of a criminal investigation.

[9] *Royal Canadian Mounted Police Act* (R.S.C., 1985, c. R-10).

[10] *Royal Canadian Mounted Police Regulations*, 2014 (SOR/2014-281).

24. With respect to the RCMP's position that the collection of personal information from Clearview is consistent with its common law powers, the RCMP explained:

> *Under Common Law, police powers are recognized as deriving from the nature and scope of police duties, including, "the preservation of the peace, the prevention of crime, and the protection of life and property."*[11]

25. Section 18 of the *RCMP Act* and paragraph 14(1)(a) of the *Regulations* read as follows:

> ***RCMP Act* – Duties**
> 18. It is the duty of members who are peace officers, subject to the orders of the Commissioner,
>
> (a) to perform all duties that are assigned to peace officers in relation to the preservation of the peace, the prevention of crime and of offences against the laws of Canada and the laws in force in any province in which they may be employed, and the apprehension of criminals and offenders and others who may be lawfully taken into custody […].
>
> ***RCMP Regulations* - Duties**
> 14. (1) In addition to the duties set out in the *Act*, it is the duty of members who are peace officers to:
>
> (a) enforce all Acts of Parliament and regulations and render assistance to departments of the Government of Canada as the Minister directs […].

26. There is no debate that in a broad sense, the investigation of crimes falls under the RCMP's common law powers and the authorities found in Section 18 of the *RCMP Act* and paragraph 14(1)(a) of the *Regulations* and generally constitutes a "program or activity" of the RCMP. However, even in the context of investigations, there are legal limits on the authority of the RCMP. It cannot carry out activities that are illegal or contrary to the general rule of law. To be compliant with Section 4 of the *Act,* a "program or activity" must be carried out in a way that falls within the institution's legal authority and which respects the general rule of law.

[11] Some examples of specific jurisprudence cited by the RCMP includes:

- *R v. Waterfield*, [1963] 3 All ER 659
- *R v. Stenning*, 1970 CanLII 12 (SCC), [1970] SCR 631, per Martland J, pp. 636-637 - first application of *R v. Waterfield* in Canada
- *Brown v. Regional Municipality of Durham Police Service Board*, 1998 CanLII 7198 (ON CA), per Doherty JA
- *Dedman v. The Queen*, 1985 CanLII 41 (SCC), [1985] 2 SCR 2, per Le Dain J
- *Waterfield*, *supra* ("...was the officer acting within the course of his duties and was the conduct in question a justifiable use of police powers associated with that duty?")

It should be noted that the RCMP did not provide any further detail to support how these cases support its position that the collection and use of information from Clearview was consistent with its common law powers.

27. In relation to this case, we are of the view that Section 4 of the *Act* cannot be read to permit the collection of personal information from a third party agent that collected, used, or disclosed the information in contravention of a law that third party is subject to.[12] It necessarily follows that the RCMP's collection of personal information through contracts with a private company that itself collected the personal information unlawfully would be a breach of Section 4 of the *Act*. To find otherwise would be to permit government institutions to advance their mandates while rewarding organizations whose personal information collection practices are unlawful, including non-compliance with Canadian privacy laws.

28. The RCMP failed to take any active steps to verify the legality of the collection of the information. Concerning any relevant legal constraints on its programs or activities regarding the collections from Clearview, and its compliance with privacy laws, the RCMP's written representations were that it "relied upon the assertions from Clearview AI that their images were all from publicly available information."

29. However, under PIPEDA and provincial privacy laws, private sector organizations must obtain consent from individuals for the collection of their personal information unless certain specific conditions are met (as described in the laws and specific regulations defining "publicly available" information). We could find no evidence that Clearview obtained such consent, despite collecting information from sources that do not qualify as 'publicly available' under PIPEDA regulations and requirements in applicable laws in Quebec, Alberta, and BC.[13] In our related joint-investigation of Clearview, Clearview confirmed that it did not seek the consent of individuals for the collection of their images, as is reflected in our conclusion that Clearview contravened PIPEDA and provincial privacy laws in Quebec, Alberta and BC.

30. We are concerned by the willingness of the RCMP to abrogate its responsibility in respecting the privacy rights of Canadians in favour of accepting general assertions of a private company without any attempt at validation. In response to a preliminary version of this report of findings, the RCMP argued that Section 4 of the *Act* does not expressly impose a duty to conclusively confirm the collection authority of a non-governmental third party. It therefore asserted that it was within its authority to collect information from Clearview under Section 4 of the *Act*. It further argued that requiring the RCMP to ensure the third party's legal compliance would create an unreasonable obligation on the RCMP, as it has neither the legal expertise in PIPEDA, nor on the scope of a third party's legal obligations. It acknowledged that where there is "apparent unlawfulness" that may impact upon the RCMP's ability to collect personal information but contends that was not the case in this instance.

31. We are disappointed that the RCMP, as a state actor with coercive powers, would choose to rely on commercial players to fulfill its mandate to Canadians without accepting the responsibility of selecting partners that comply with the law. To be clear,

[12] For clarity, this does not apply to whistleblowers.

[13] See paragraphs 44-46 of the joint investigation into Clearview AI for more details on the common understanding of publicly available information.

the RCMP is obligated to inform itself of the lawfulness of the collection practices of partners from whom it collects personal information.

32. Based on the foregoing, it is our view that the RCMP's collection of personal information from Clearview, that Clearview had collected unlawfully, fell outside the scope of any "operating program or activity" of the RCMP and was therefore in contravention of Section 4 of the *Act*.

Issue: Appropriate corrective action is required by RCMP to develop controls to prevent future similar contraventions

33. As noted above (paragraph 10), the RCMP did not conduct an assessment for compliance with Section 4 of the *Act* before beginning to collect the information of Canadians from Clearview. In addition, it permitted the creation and use by RCMP members of 16 accounts for which it did not provide a reasonable accounting of purpose or use (paragraph 18).

34. To our knowledge, the RCMP no longer collects personal information from Clearview since Clearview withdrew its services from Canada in July 2020. However, given the widespread nature of RCMP's collection of personal information from Clearview before that time, which included uses it could not account for, we examined the adequacy of the controls that the RCMP had/has in place to ensure compliance with Section 4 of the *Act*. This analysis informs our remedial recommendations in this matter.

35. For the reasons described in detail below, we are concerned that without systemic changes and improved training, similar potential contraventions of the *Act* will continue to occur in the future with facial recognition and other technologies or strategies involving the collection of personal information.

36. We would expect[14] that an institutional program collecting personal information that could present a high risk to individuals' privacy would have in place robust structures, informed by appropriate expertise, to ensure compliance with Section 4 of the *Act* with respect to the personal information it collects; particularly when it considers any novel collection of personal information.[15] Novel collection includes: (i) collecting new types of personal information; (ii) collecting personal information for new purposes; (iii) collecting personal information in new ways (e.g. through biometric or other new technology); and (iv) collecting personal information from new sources.[16]

[14] See Expectations: OPCs Guide to the Privacy Impact Assessment Process, and in particular the section titled "Accountability".

[15] As the complaint against the RCMP is with respect to the collection of personal information, this report focuses specifically on collection. The same principles would apply for any new use or disclosure of personal information.

[16] All four of these cases could affect whether a collection that may appear on its face to be compliant is actually in accord with Section 4 of the *Act*.

37. Our expectations are supported by the TBS's *Policy on Privacy Protection* and *Directive on Privacy Impact Assessment*, to which the RCMP is also subject. The Directive specifies that:

- "The PIA is the component of risk management that focuses on ensuring compliance with the *Privacy Act* requirements and assessing the privacy implications of new or substantially modified programs and activities involving personal information." The definition of substantial modification expressly includes "any change or amendment to the privacy practices related to activities that use automated or technological means to identify, create, analyze, compare, extract, cull, match or define personal information."

- Institutions must establish a PIA development and approval process that, among other things, "is commensurate with the level of risk related to the privacy invasiveness of the institution's programs or activities, and ensures the PIA is completed by the senior official or executive holding responsibility within the institution for new or substantially modified programs or activities."

- For all personal information collected for use in administrative decisions about an individual, [such as law enforcement decisions], PIAs are also to be completed, among other situations, when contracting out activities to the private sector results in substantial modifications to the program or activities.

- Core PIAs must be provided to the Office of the Privacy Commissioner, and, "under the TBS Policy on Privacy Protection, heads of government institutions are required to notify the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the *Privacy Act* or to any of its provisions or that could have an impact on the privacy of Canadians. This notification is to take place at a **sufficiently early stage** to permit the Commissioner to review and discuss the issues involved" [emphasis added].

38. All institutions are required by TBS Policy to conduct PIAs for new or substantially modified programs and activities involving personal information.[17] All institutions should also ensure that their decision makers understand and act on their obligations to prevent contraventions of the *Act*. However, we recognize that not all institutional programs present the same level of risk. Where the potential for privacy invasive collections is higher, we expect the related measures to ensure these risks are properly assessed to be more rigorous.[18] At a minimum, therefore, we would expect an institution with programs collecting personal information that could present a high risk to individuals' privacy to have in place all of the following:

[17] For more information about the OPC's expectations for institutions in the course of conducting PIAs see: Expectations: OPC's Guide to the Privacy Impact Assessment Process

[18] This is in alignment with TBS's expectations, described in paragraph 37 above, that institutions must establish a PIA development and approval process that, among other things, "is commensurate with the level of risk related to the privacy invasiveness of the institution's programs or activities…"

A) **Knowledge of obligations:** Training programs to ensure all individuals empowered to make decisions about the collection of personal information understand the limitations on collection under Section 4 of the *Act*.

B) **Awareness of novel collections:** Systems and procedures to track potential and actual novel collection of personal information.

C) **Processes to identify potential compliance issues:** Procedures, including checkpoints within processes where novel collection may become known, to alert decision-makers that an assessment to ensure compliance with Section 4 of the *Act* may be warranted.

D) **Processes to complete timely assessments where warranted:** Systems, procedures, and training on roles and responsibilities to ensure that if a fulsome assessment for compliance is warranted, that such assessments are completed in a timely way, before collection begins.

E) **Effective controls on collection:** Effective controls, including dynamic monitoring, to limit the collection of personal information by staff at an institution to what it has validated as permissible under the *Act*.

A) Knowledge of obligations

39. Knowledge by decision-makers of the relevant limits on collection of personal information, specific to a particular operating program or activity, is critical to compliance with the *Act*. This should be supported by training programs and access to expertise, including legal services and privacy subject matter experts, to ensure all individuals empowered to make decisions about the collection of personal information have a meaningful understanding of the limitations on collection under Section 4 of the *Act*.

40. The RCMP defended the actions of its decision-makers (those who collected personal information from Clearview). Specifically, it stated, in response to our questions about why it considered the collections lawful, that “The RCMP relied upon the assertions from Clearview AI that their images were all from publicly available information. It was reasonable to rely upon their assertions. There was no requirement for the RCMP to investigate further into the constitution of their database.”[19]

41. As noted above (paragraph 32), our office found that Clearview collected personal information unlawfully, and therefore the collection by the RCMP of this information

[19] We note in addition, that the institutions must comply with Section 4 of the *Act* even when collecting publicly available information. While the *Act* specifies that Sections 7 and 8 of the *Act* do not apply to publicly available information, no such exemption applies to the other provisions in the *Act*, including Section 4.

from Clearview is a contravention of the *Act*.[20] However, this is not the only potential issue with respect to compliance with the *Act* that the RCMP had an obligation to consider.

42. Under the *Charter*,[21] a collection of personal information by law enforcement constitutes a search or seizure where an individual has a reasonable expectation of privacy with respect to the information at issue. The Supreme Court of Canada has also found that individuals may still possess a reasonable expectation of privacy even in public places.[22] The Courts may consider the invasiveness of a technology when determining whether an individual had a reasonable expectation of privacy,[23] and they have recognized informational privacy in relation to anonymity in Internet activity.[24] While we are not making any conclusions as to the RCMP's compliance with the *Charter* in using Clearview technology, in our view, it should have been clear to the RCMP that both the collection from a privately-collected database, and the collection of information via facial recognition technology, warranted assessment from the RCMP for compliance with the *Charter* and common law principles.

43. Government institutions require lawful authority to collect personal information. The RCMP represented that its collection of personal information from Clearview was authorized under the *RCMP Act* and under common law. Further, the common law clearly sets limits on the RCMP's collection powers as a police body. Among other constraints, there are limitations set out by the courts in *Waterfield*[25] and affirmed by the Supreme Court of Canada in *Stenning*[26] and more recently in *Fleming.*[27] Specifically, to determine whether a police action (such as a search) is authorized under common law, the following two factors must be considered:

    i. Whether such conduct falls within the general scope of any law enforcement duty imposed by statute or recognized at common law; and
    ii. whether such conduct constitutes a justifiable exercise of police powers associated with that duty.

44. The second stage of the test assesses whether the police action is reasonably necessary for the fulfillment of the duty, which involves consideration of three factors:

[20] 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.

[21] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*(UK), 1982, c 11 [*Charter*], s 8.

[22] For example*, R v Spencer 2014 SCC 4,* R v Jarvis 2019 SCC 10 (re. reasonable expectation of privacy for the purposes of s. 162(1) of the Criminal Code).

[23] For example, R v Jarvis 2019 SCC 10 (re. reasonable expectation of privacy for the purposes of s. 162(1) of the Criminal Code), *R v Wise 1992.*

[24] For example, in *R v Spencer* 2014 SCC 43: "Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."

[25] *R v. Waterfield*, *supra*.

[26] *R. v. Stenning*, *supra*.

[27] *Fleming v. Ontario*, 2019 SCC 45.

(1) the importance of the performance of the duty to the public good, (2) the necessity of the interference with individual liberty for the performance of the duty, and (3) the extent of the interference with an individual's liberty and privacy.[28]

45. With respect to the first element of the test, as noted above (paragraph 18), the RCMP did not provide an accounting for 85% of the searches it conducted through its Clearview accounts. As a consequence, it seems the RCMP is not able to demonstrate that an evaluation with the first element of the Waterfield test was carried out. The RCMP noted that prior to its directive on the use of Clearview made after the OPC commenced its investigation, usage of Clearview outside an investigation would not have been tracked as there was no established requirement to do so. This represents a significant failure in accountability by the RCMP.

46. With respect to the second element of the test, we note that the use of facial recognition technology, with its power to disrupt anonymity in public spaces, can constitute a meaningful interference with liberty and privacy. Further, the RCMP's use of a service such as Clearview, that is based on the systematic extraction and processing of billions of images of individuals innocent of any crime, is a major and substantial intrusion by the state into the private lives of Canadians.

47. Before using such a service, a police body must, at a minimum, examine whether such a service is reasonably necessary to the investigation and consider the proportionality of the intrusion against the specific public interest being pursued.[29]

48. In this context, the fact that multiple decision makers within the RCMP did not feel it necessary to consider what limits on the use of such technology might be required under common law suggests a lack of meaningful understanding of the RCMP's relevant privacy obligations.

Recommendations:

i. We recommended, and the RCMP has agreed, to engage in dialogue with the OPC and other privacy regulators on the privacy issues surrounding the use of facial recognition technology.

ii. We also recommended, and the RCMP has agreed, to institute a training program commencing no later than 12 months from the receipt of this report to ensure that all decision-makers are trained on the limitations on collection of personal information under the *Act*, including:

   a) When contracting for personal information collection services, not using service providers that are collecting personal information in violation of Canadian privacy laws.

[28] *Knowlton v. R.*, 1973 CanLII 148 (SCC), [1974] SCR 443. Page 446. *See also, Fleming, supra*, at para 75.

[29] *R. v. Waterfield*, *supra*; see also *Fleming*, *supra*.

b) Nuanced and meaningful understanding of the limitations associated with the collection of personal information, particularly when using new privacy-invasive technology, including mass surveillance tools.

49. As noted above (paragraph 30), the RCMP disagreed with our finding that it is obligated to inform itself of the lawfulness of the collection practices of partners from whom it collects personal information. We appreciate that despite the RCMP's disagreement with the finding, it acknowledges that deficiencies exist in its current practices. To that end, the RCMP has agreed to implement the recommendations above, including specifically that it will conduct fulsome assessments of third parties' compliance with Canadian privacy laws those third parties are subject to.

B) Awareness of novel collections

50. Awareness as to what novel personal information collection techniques are taking place (or being considered/tested) is a critical foundation to turning a theoretical understanding of the obligations under Section 4 of the *Act* into action. This is necessary to ensure collection is appropriately limited, and to be able to provide accurate assurances to external stakeholders in support of the public trust.

51. The facts of this case clearly demonstrate significant gaps in the RCMP's systems for ensuring its own awareness of novel personal information collection practices that it is undertaking. As noted above (paragraph 10), the RCMP inaccurately informed the OPC on January 29, 2020 that the RCMP had not used Clearview in an investigative context, despite the fact that it had purchased licenses for Clearview in October 2019, and had since made extensive use of Clearview's services. According to the RCMP, this erroneous declaration occurred because none of the internal experts in the RCMP's Technical Investigative Services who were consulted by members of the RCMP's Access to Information and Privacy Unit were aware of its use, despite the fact that Clearview was used broadly across 5 different RCMP Divisions.

52. Only after Clearview's client list, which included the RCMP, was reported stolen in February 2020, did the RCMP correct the erroneous statement to the OPC.

53. Further, as already noted, the RCMP only provided a reasonable accounting for approximately 15% of the more than 500 searches that, according to Clearview's records, the RCMP made. The purposes for the remaining searches are unknown.[30]

54. The RCMP did not have any system in place, either locally or nationally, to track the consideration of, or actual use of, new investigative technologies or other novel personal information collection.

[30] We note that the RCMP could no longer audit access logs stored in its Clearview accounts following the July 6, 2020 suspension of RCMP accounts by Clearview.

Recommendation:

i. We recommended, and the RCMP has agreed, that no later than 12 months from the receipt of this report, it will institute systems and procedures to ensure that all novel collections of personal information across the RCMP are reliably tracked internally in such a way that they can meaningfully inform, and be meaningfully informed by, the RCMP's decision-making on such collections.

55. With respect to the above commitment, as a preliminary step, the RCMP launched a National Technology Onboarding Program unit in March 2021. The program is intended to create a framework to implement a centralized system to enable the RCMP to identify, assess and track new and emerging investigative techniques that involve the collection of novel types of information for investigational purposes.

C) Processes to identify potential compliance issues

56. The identification of actual or potential collections that warrant an assessment for compliance with the *Act before* they are undertaken is crucial. We would expect these checks to be commensurate to the potential risks to individuals' privacy, based on the volume, sensitivity and complexity of the relevant personal information collection activities. We would expect the checks to be embedded in appropriate processes depending on the activities of the institution. In this way, decision-makers empowered to make potentially high-risk novel personal information collection decisions can demonstrate how they have accounted for compliance with the *Act*.

57. In addition to being embedded into processes for the development and approval of new programs, we would expect such checks to be embedded in other processes where new types of personal information, new purposes for collection, new ways of collecting information, or new sources of personal information could arise. For instance, as a few illustrative examples:

- processes for entering into information sharing arrangements;
- procurement processes;
- processes governing pilots and the use of trial services; and
- processes for vetting new technology.

58. As a key example of gaps, the RCMP indicated it has references to considering the need for PIAs only in IM/IT manuals. PIAs (or alternative measures to assess compliance with the *Act*) are necessary outside of IM/IT processes. Any branch and level of the RCMP that can commence the novel collection of personal information must have procedures in place to initiate an assessment of compliance with the *Act* where warranted.

59. The RCMP indicated that RCMP members are empowered to use their discretion to try new personal information collection techniques with appropriate approvals at the local level. The decision of whether or not to conduct a PIA is left to supervisory staff to determine. In this case, the RCMP opened a total of 19 paid and trial accounts to collect information from a materially new private sector source, including two paid contracts,

all without triggering an assessment for compliance with Section 4 of the *Act*. In addition, the RCMP's collection via a new privacy-invasive technology (facial recognition), which is clearly a substantial modification to the collection of personal information that could affect compliance, did not trigger an internal assessment for compliance with the *Act* before use.

60. The RCMP's representations indicated that it was only on February 6, 2020, more than four months after contracting with Clearview, that it started to consider conducting an assessment for compliance with the *Act* for the collection of information from Clearview. Its records further indicate that it only began filling in a PIA checklist (a TBS tool used determine if a PIA is warranted[31]) in March 2020. This preliminary issue identification step was not completed until June 2020. As demonstrated in this case, adopting an ad-hoc, minimally supervised and ex-post approach will raise the likelihood of privacy contraventions and result in otherwise preventable damages.

61. The OPC is of the view that with a proper vetting process, the contravention at issue could have been prevented. This could have been done if the RCMP had identified the potential compliance issues related to the use of Clearview AI in a timely way in order to begin an appropriate assessment for compliance with the *Act*, informed by appropriate consultation with subject matter experts. Had the RCMP notified the OPC, as required by the TBS *Policy on Privacy Protection* (see paragraph 37), then early discussion of the privacy implications could have taken place. It is a serious concern that the RCMP failed to identify the need for a compliance assessment (in the form of a PIA or otherwise) prior to collecting information via any of its 19 accounts.

Recommendation:

i. We recommended, and the RCMP has agreed, that no later than 12 months from the receipt of this report, it will institute a system of checks where potentially high risk novel collection may become known, to alert decision-makers that a compliance assessment may be needed. Decision-makers can then demonstrate that they have considered compliance with the requirements of Section 4 of the *Act* before they begin collecting personal information, and can initiate full assessments where needed.

D) Processes to complete timely assessments

62. Where a potential compliance issue is identified through the checks described above (i.e., where compliance with the *Act* may be at issue), assessments for compliance with the *Act* should be commenced and completed *before* collection starts. This reduces the risk of unlawful collection, and prevents associated damage to individuals who could otherwise be affected by such collection of their personal information. These assessments should be informed by appropriate privacy and legal subject matter expertise, and where warranted, the OPC.

[31] Under the TBS Directive on Privacy Impact Assessment.

63. While, as described above, the RCMP's internal processes failed to proactively identify the potential privacy concerns in this instance, it should nonetheless have been apparent to the RCMP that a fulsome assessment of the collections from Clearview was warranted after the issue was raised prominently in the media in January 2020. Indeed, the RCMP expressly committed to the OPC in January (when it indicated it was not using Clearview) that it would conduct a PIA before actively deploying such technology.

64. Despite both the clear need and this statement to the OPC, the RCMP provided no evidence that it had commenced an actual *Privacy Act* compliance assessment (beyond the issue identification checklist referenced above), before Clearview AI withdrew its facial recognition services from Canada in July 2020.

65. The RCMP indicated that it does not have training material for staff on conducting PIAs, despite the significant amount of sensitive personal information it collects as a law enforcement agency.

66. Of further concern is that none of the RCMP's decision-makers conducted such an assessment before beginning collection. This is despite the RCMP's previous assertions to our office that it recognized the potential privacy impact of Clearview's services and was committed to doing a PIA before its use. It is our view that this represents a critical failure by the RCMP to ensure it meet its obligations under the *Act*.

Recommendations:

i. We recommended, and the RCMP has agreed, to institute a training program for all decision-makers (i.e., anyone empowered to make decisions to collect novel personal information) on their roles and responsibilities in identifying, assessing, and avoiding collection in contravention of the *Act*, commencing no later than 12 months from the receipt of this report.

ii. We also recommended, and the RCMP has agreed, that no later than 12 months from the receipt of this report, it shall demonstrate that it has dedicated the resources and put in place the processes to ensure that assessments for compliance with the *Act* are carried out every time they are warranted and applied consistently by all parts of RCMP. These resources and processes should ensure assessments are completed in a timely way, informed by appropriate subject matter expertise commensurate to the issues identified, *before* personal information is collected for any law enforcement purposes.

67. As a preliminary step towards satisfying these commitments, as noted above, the RCMP has launched a National Technology Onboarding Program unit in March 2021.

E) Effective controls on collection

68. When the RCMP first created paid Clearview accounts in October 2019, it did not have any specific policies in place limiting the purposes for which this information could be

collected, despite the clear privacy implications described above. After the expression of public concern and the announcement of our investigation the RCMP did issue internal direction to members, on March 5, 2020, imposing limitations on collection using Clearview. Specifically, the directive provided information and instruction to RCMP members including:

> *Given the speed at which technology is evolving, the RCMP continues to explore the broader use of emerging technologies to determine how they could potentially benefit police operations. While leveraging new technology can enhance our ability to conduct investigations more efficiently and effectively, we need to balance this against an individual's right to privacy.*
>
> *[…]*
>
> *[…] The RCMP and other law enforcement agencies are continuously trying to identify, test and potentially acquire new and innovative technologies to further criminal investigations within the scope of their authorities. Discovery, successful testing/piloting and adoption of a new technology requires the development of operational policies to ensure governance and accountability on their use, as well as their associated data acquisition, use and storage. These policies are developed in consideration of the Charter, the Privacy Act and other relevant legislation, regulations and policies.*
>
> *Our review of the continued use of this technology and particularly Clearview AI is ongoing. In the interim, given the sensitivities surrounding facial recognition technology, we will only be using it in very limited and specific circumstances.*
>
> *Going forward, Divisions are asked to carefully scrutinize the use of facial recognition technologies, including Clearview AI, and only use it in exigent circumstances for victim identification in child sexual exploitation investigations or in circumstances where threat to life or grievous bodily harm may be imminent. Divisions should ensure that the Criminal Operations Officers (CROPS) approve any requests to use facial recognition technology. In the case of NHQ, any use is to be approved by the Director General of the requesting Program. You are further asked to advise [the Assistant Commissioner of Technical Operations, SPS] of any use of facial recognition technology. This will provide national oversight and ensure that the organization is informed on an ongoing basis of the limited use of this technology.*

69. During the course of our investigation, the RCMP also centralized the management of the Clearview accounts and created an audit function to monitor RCMP members' use of Clearview.

70. We appreciate these positive indicators that the RCMP recognized, after concerns were identified externally, that the situations in which it could lawfully collect information from the internet via facial recognition technology can be constrained under the common law (and consequently, Section 4 of the *Act*).

71. However (as noted in paragraph 18 above), only 6% of the RCMP's searches using Clearview appeared to be related to victim identification, and the RCMP accounted for only an additional approximately 9% of searches. It did not account for the vast majority (85%) of the searches it conducted according to Clearview records. We cannot say with any confidence that the searches were limited to the purposes identified above, or even that they were for professional purposes. A consequence of the absence of records relating to professional purposes is that it points to the opposite.

72. Further, the RCMP did not indicate that any of the RCMP members who created and collected information through any of the Clearview trial accounts contravened any internal policies or procedures when they did so. This lack of control over a significant novel collection of personal information is a significant concern. We acknowledge that in order to operate efficiently and effectively the RCMP requires that its staff take initiative and innovate. However, it is important that there be measures in place to ensure that such innovation does not cross legal lines.

Recommendations:

i. We recommended, and the RCMP has agreed, to institute clear controls in effect no later than 12 months from the receipt of this report and including: (i) policies to clarify who can make decisions to undertake novel collections of personal information, and what steps staff need to take to determine if a collection they are considering is permissible, and (ii) systems to monitor for unauthorized collections, including collections for inappropriate purposes.

ii. We also recommended, and the RCMP has agreed, to establish a clear methodology and chain of responsibility for members to suggest novel collection techniques to trained decision makers, commencing no later than 12 months from the receipt of this report.

Other

73. Given that the collection of personal information from Clearview by the RCMP was not consistent with Section 4 of the *Act*, and that the RCMP is no longer collecting information from Clearview, we did not examine in detail the RCMP's ancillary procedures relating to its use.

74. However, with a view to informing future practices by the RCMP, we provide certain observations relating to other sections of the *Act* that would be applicable to any future similar activities by the RCMP.

Protection against unintended use or disclosure

75. Section 8 of the *Act* requires that an institution not disclose personal information except for the purpose for which it was collected or a consistent use. This would apply, for

instance, to images collected by the RCMP and uploaded to Clearview for facial recognition matching purposes.

76. In order for institutions to ensure they respect these limitations, including when contracting for services (as was the case here), the TBS *Directive on Privacy Practices* requires that when personal information is disclosed to a private sector institution, contracts established with private sector entities must outline measures and provisions to address privacy issues. This includes provisions to limit inappropriate handling, use, or disclosure by the contracted entity and to ensure adequate protections of personal information from unintended disclosures to third parties. In addition, the protection provisions are to ensure government security standards are respected.

77. Such measures are demonstrably important. We note in this regard that Clearview suffered a data breach in February 2020, though we have no indications that this breach affected images uploaded to Clearview by the RCMP.

78. According to its representations, the RCMP took certain measures to protect personal information disclosed to Clearview from subsequent inappropriate use or disclosure:

    - For the small subset of searches of Clearview that the RCMP could account for, it had procedures in place that required that photos be cropped to just the face being searched before uploading to Clearview to avoid uploading irrelevant information to limit disclosure risk.
    - It indicated that Clearview confirmed to the RCMP that data transmissions are encrypted, and that uploaded images are not added to Clearview's database.
    - It requested that Clearview reduce the retention period for uploaded images to 45 days, and subsequently retain only a low resolution thumbnail for 6 months.

79. However, the RCMP did not demonstrate that it had included any or all of the elements above in its contracts (licensing agreement) with Clearview. The RCMP submitted that its licences – whether paid or trial – were subject only to Clearview's Terms of Services and Privacy Policy.

Accuracy

80. Subsection 6(2) of the *Act* specifies that "A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."

81. The RCMP submitted that with respect to the accuracy of the results obtained by Clearview and used by the RCMP, it directed its members via the NCECC Standard Operating Procedure to treat all information as leads, not confirmed identity matches. Whether or not to pursue further steps was based on the assessment of the members.

82. With respect to the use of facial recognition technology in general, we believe that it is important to recognize that concerns exist with respect to the accuracy and algorithmic bias in facial recognition technologies. This includes the potential for 'false positive'

identifications that could affect law enforcement decisions taken about individuals, such as whether to make further enquiries about them. Such actions can in turn have a significant impact on individuals' privacy.

83. For example, there is extensive scientific literature detailing the inaccuracy of anthropometric data[32] for the purposes of racial or ancestral determination in the field of forensic anthropology at the level of skeletal analysis, particularly the skull and face, and the use of external soft tissue markers used for forensic facial approximation (reconstruction) appears to be even less accurate. According to Ubelaker *et al*., "Techniques of facial approximation are improving with enhanced information regarding the relationship of facial hard and soft tissues and more sophisticated computer technology. Despite these advancements, facial approximation does not represent a method of positive scientific identification."[33] We believe that this is important to recognize because facial recognition technology is based on anthropometric data that makes certain assumptions about common facial features of various ethnic/racial groups.

84. A recent study by the US National Institute of Standards and Technology ("NIST") as part of its "Face Recognition Vendor Test"[34] series focused on demographic differentials for contemporary face recognition algorithms (NISTIR 8280).[35] In summary, the NIST study made the following findings:

    i. For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians.

    ii. Among U.S.-developed algorithms, there were similar high rates of false positives in one-to-one matching for Asians, African Americans and native groups.

    iii. However, a notable exception was for some algorithms developed in Asian countries.

    iv. For one-to-many matching, the team saw higher rates of false positives for African American females.

    v. However, not all algorithms give this high rate of false positives across demographics in one-to-many matching.[36]

85. To be compliant with Section 6 of the *Act*, to the extent that the RCMP considers future use of specific facial recognition technologies, it will be important for it to carefully

[32] "Anthropometric data" refers to measurements of the size and shape of various parts of the human body.
[33] DH Ubelaker, A Shamlou, A Kunkle (2019) "Contributions of forensic anthropology to positive scientific identification: a critical review." *Forensic Sciences Research* 4(1): 45-50. (last verified October 23, 2020).
[34] Face Recognition Vendor Test (last verified October 23, 2020).
[35] Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. (last verified May 20, 2021).
[36] NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software; see also Facial-Recognition Software Might Have a Racial Bias Problem and Facial Recognition Is Accurate, if You're a White Guy (last verified May 20, 2021)

assess measures that may be needed to address such accuracy-related concerns, particularly the potential for false positives. We look forward to further engaging with the RCMP on this matter in planned dialogue with the OPC and other privacy regulators in the context of our development of guidance on the use of facial recognition technology by law enforcement.

Conclusion

86. We find that the RCMP's collection of personal information from Clearview was in contravention of Section 4 of the *Act*. The basis for this finding is that Clearview's collection of personal information of Canadians was in contravention of the law. It therefore follows that that the RCMP contravened the *Act* when it subsequently collected personal information that was unlawfully gathered by Clearview.

87. 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. This includes widespread failures to know what it was collecting, control how collection occurs, identify potential compliance issues, and assess and prevent contraventions of the *Act*.

88. Prior to the OPC providing the recommendations above, in response to questions we raised, the RCMP had already begun to explore ways to improve its review of collection practices for compliance with its legal obligations, and in March 2021 it launched a National Technology Onboarding Program unit. Further, the RCMP committed to implementing the recommendations made by our office in the report above.

89. We remain concerned that the RCMP disagreed with our findings that it contravened the *Act*, and takes the position that it is not obliged to ensure that third party agents it collects personal information from have acted lawfully with respect to the collection and use of that personal information. However, we are encouraged by the preliminary steps the RCMP has already taken above, and its commitment to implement all of our recommendations. We therefore find the matter **well-founded and conditionally resolved**.

90. Implementing the recommendations will require broad and concerted efforts across the RCMP. Much work remains to be done to ensure adoption of changes in decision-making culture across the RCMP – supported by well-embedded processes, tools and training. We strongly encourage the RCMP to dedicate the sustained resources and senior-level championing necessary for successful implementation of its commitment to the recommendations. By fully implementing our recommendations, the RCMP will be able to more effectively explore and responsibly use new technologies to advance its critical mandate.

3. Draft privacy guidance on facial recognition for police agencies

Table of contents

Overview

1. Facial recognition (FR) has emerged as a powerful technology that can pose serious risks to privacy. The purpose of this guidance is to clarify police agencies' privacy obligations relating to the use of this technology, with a view to ensuring any use of FR complies with the law, minimizes privacy risks, and respects privacy rights.

2. This guidance is issued jointly by the privacy protection authorities for each province and territory of Canada, and the Office of the Privacy Commissioner of Canada.

Scope

3. This guidance is for federal, provincial, regional and municipal police agencies. It was not written for other public organizations outside of the police that are involved in law enforcement activities (for example, border control), nor for private-sector organizations that carry out similar activities (for example, private security). However, these organizations must still ensure their compliance with all applicable laws, including privacy and human rights laws. Sections of this guidance may be helpful for that purpose.

Introduction

4. FR technology has emerged as a tool of significant interest to law enforcement. Used responsibly and in the right circumstances, FR may assist police agencies in carrying out a variety of public safety initiatives, including investigations into criminal wrongdoing and the search for missing persons.

5. At the same time, FR has the potential to be a highly invasive surveillance technology.

6. The use of FR involves the collection and processing of sensitive personal information: biometric facial data is unique to each individual, unlikely to vary significantly over periods of time, and difficult to change in its underlying features. This information speaks to the very core of individual identity, and its collection and use by police supports the ability to identify and potentially surveil individuals.

7. FR technology also scales easily, costs relatively little to use, and can be deployed as an add-on to existing surveillance infrastructure. This includes the capacity to automate extraction of identifying information from a wide range of sources, including virtually any source of digital imagery, both online and off.

8. The prospect of police agencies integrating FR technology into law enforcement initiatives thus raises the possibility of serious privacy harms unless appropriate privacy protections are put in place.

9. The freedom to live and develop free from surveillance is a fundamental human right. In Canada, public sector statutory rights to privacy are recognized as quasi-constitutional in nature, and aspects of the right to privacy are protected by the *Canadian Charter of Rights and Freedoms* (the Charter). These rights dictate that individuals must be able to navigate public, semi-public, and private spaces without the risk of their activities being routinely identified, tracked and monitored. While certain intrusions on this right can be justified in specific circumstances, individuals do not forego their right to privacy merely by participating in the world in ways that may reveal their face to others, or that may enable their image to be captured on camera.

10. Privacy is also necessary for the realization of other fundamental rights that are protected by the Charter. Privacy is vital to dignity, autonomy, and personal growth, and it is a basic prerequisite to the free and open participation of individuals in democratic life. When surveillance increases, individuals can be deterred from exercising these rights and freedoms.

11. Surveillance is also linked with systemic discrimination, including discrimination experienced by racialized communities. Longstanding concerns about the disproportionate policing of racialized communities raise serious questions about the privacy and human rights impact of applying FR technology to, for example, historical datasets such as mugshot databases. When considering the impact of FR technology on individual privacy then, law enforcement agencies must also account for and respect the right to the equal protection and equal benefit of the law without discrimination.

12. If used inappropriately, FR technology may therefore have lasting and severe effects on privacy and other fundamental rights. This includes not only harms to specific individuals whose personal information may be collected, processed, or disclosed, but also more general societal harms that flow from increases in the capacity of authorities to monitor the physical and virtual spaces in which we interact. Such increases can be difficult to contain once they are set in motion.

13. The nature of these risks calls for collective reflection on the limits of acceptable FR use. These limits are defined not only by the risks associated with specific FR initiatives, but also by the aggregate effects of all such initiatives, taken together over time, on the general surveillance of public and private space. The question of where acceptable FR use begins and ends is in part, then, a question of the expectations we set now for the future protection of privacy in the face of ever-increasing technological capabilities to intrude on Canadians' reasonable expectations of privacy.

14. The process of establishing appropriate limits on FR use remains incomplete. Unlike other forms of biometrics collected by law enforcement such as photographs,

fingerprints or DNA profiles, FR use is not subject to a clear and comprehensive set of rules. Instead, its use is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed by FR. This creates room for uncertainty concerning what uses of FR may be acceptable, and under what circumstances.

15. It is in this context that our offices issue the present guidance document. The guidance is meant to clarify legal responsibilities, as they currently stand, with a view to ensuring any use of FR by police agencies complies with the law, minimizes privacy risks and respects the fundamental human right to privacy. This guidance should not be read as justifying, endorsing or approving the use of FR by police agencies. Nor does it replace the broader need for a more robust regulatory framework for FR.

16. While this document addresses many legal requirements that pertain to FR use, it does not necessarily address all such requirements. Police agencies remain responsible for ensuring that any use of FR complies with all applicable legal requirements.

FR technology

17. FR technology is a type of software that uses complex image processing techniques to detect and analyze the biometric features of an individual's face for the purposes of identification or verification (also known as "authentication") of an individual's identity. While early versions relied on humans to manually select and measure the landmarks of an individual's face, today the process of creating a facial template or "faceprint" is fully automated. Using advanced, "deep learning" algorithms trained on millions of examples, FR technology is able to create three-dimensional faceprints consisting of close to a hundred biometric features from two-dimensional images.

How is FR used?

18. Identification and verification have specific meanings within the context of FR. Identification is used in the investigative sense of determining the identity of an otherwise unknown individual. Here, FR compares the image inputted into the system (also known as the "probe" image) against all other images in a database of pre-enrolled faces in an attempt to learn the individual's identity. This is sometimes referred to as "1:N" matching.

19. Verification is a special case of identification. It is used primarily for security in cases where an identity is already attached to the probe image. Rather than multiple images, FR compares the probe image to the one image in the database corresponding to the identity claim. If they match, the individual's identity is proven to a higher level of assurance. In contrast to identification, verification is sometimes referred to as "1:1" matching.

20. This guidance is focussed primarily on FR use for the purposes of identification. While verification is a common use of FR in general (e.g., to unlock one's phone), identification is more closely aligned to the mandate of law enforcement.

How does FR work?

21. FR has a number of components that each play a role in determining how it functions in a particular set of circumstances. Depending on the FR product in use, some components may be configurable by the end user. However, in cases where FR is purchased from a vendor rather than built in-house, the functionality of some components will be hard-coded into the product itself and can only be changed through switching products or by receiving an updated version.

22. The following list provides a brief description of the key components police agencies should be aware of when deploying FR in a law enforcement context.

23. **Training data.** The image processing algorithms that power FR are generated using machine learning methods that take labelled examples of individuals' faces as their input. This input is known as the training data of the algorithm. By tuning the parameters of a model to best fit this data, FR is able to "learn" to detect the distinguishable features of human faces, without the need for explicit programming by its developers.

24. **Algorithms.** FR works by performing a series of discrete tasks. There are four key ones to be aware of. Each is automated using an algorithm. However, taken together, they form one overarching algorithm for the system. Their work may be described as follows:

    - A *face detector* scans an image and picks out the faces in it
    - A *faceprint generator* takes an image of a face and creates a faceprint of it
    - A *faceprint comparator* compares two faceprints and returns a similarity score and
    - A *faceprint matcher* searches a database of faces and (using the faceprint comparator) returns a list of candidates whose similarity score is at or above a given threshold

25. **Face database.** To identify or verify the identity of an individual, FR must have access to a database of identified faces against which to match an image of the individual in question. Usually, the face database in a FR initiative is provided by the end user. In the law enforcement context, examples may include a mugshot database or missing persons database. However, some FR vendors have attempted to compile their own databases, typically of images taken from the Internet, and include use of them as part of their product, the legal basis for which is far less clear. [1]

[1] See, for example: 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, February 2 2021.

26. **Faceprint.** After detecting the various features of an individual's face, FR measures them and encodes the result in a vector of numerical values called a faceprint. A faceprint is a biometric, similar to a fingerprint—a set of unique physical characteristics inherent to an individual that cannot be easily altered. Examples of biometric features encoded in a faceprint may include:

    - distance between eyes
    - width of nose
    - distance between nose and lips
    - depth of eye sockets
    - shape of cheekbones
    - length of jaw line

27. **Similarity score.** Faces exhibit a wide range of variability, both in terms of their similarities and differences. Some may have virtually no similarities. Others may be similar or even identical in some respects but in others less so or not at all. Even the same face may look different depending on the circumstances, such as the level of light, orientation angle or the amount of time that has passed between images. To express the different ways faces may be similar or different, FR calculates a "similarity score," also sometimes referred to as a "confidence score." This is a numerical value representing the degree of similarity between two faceprints based on the biometric features encoded in them. A lower value indicates less similarity; a higher value more.

28. **Threshold.** Even though two faceprints may have a positive similarity score, only those that meet or exceed a given threshold are considered potential matches. Some FR products allow the end user to set the threshold; others do not. How the threshold is set directly affects the number of results returned in a given search, with implications for the accuracy, including error rates, of the FR algorithm. Depending on the circumstances, some implementations may require higher thresholds than others.

29. Additional FR components not mentioned in the list above include quality assessment and impersonation detection.

Privacy framework

30. As explained in the introduction, the use of FR technology can pose extremely serious privacy risks. Many of these risks may be difficult to mitigate, and can cause significant harm to individuals and groups.

31. When considering the use of FR technology, it is therefore imperative that police agencies not only ensure they have lawful authority for the proposed use, but also that they apply standards of privacy protection that are proportionate to the potential harms involved. In some cases, potential harms may be so extreme that no amount of

protections can be applied to adequately reduce the privacy risk. In other cases, it may be possible to appropriately manage risks through careful planning and diligent application of privacy protections.

32. The framework outlined below is intended to assist police agencies in ensuring FR use is legal and developed with privacy protections that are proportionate to the specific risks involved. It is based on the application of internationally-accepted privacy principles, many of which are reflected in privacy laws. While specific legal obligations may vary by jurisdiction, we expect all police agencies to comply with the law and recommend they follow the best practices included in this framework given the high risk of harm that can result from the inappropriate use of FR technology.

33. Police agencies are ultimately responsible for ensuring any use of FR technology is lawfully authorized and that privacy risks are managed appropriately. This guidance provides a baseline from which to build privacy protections into FR initiatives; police agencies may need to implement additional privacy protections depending on the nature and scope of risks to privacy posed by a specific initiative.

Lawful authority

34. Police agencies must have the legal authority to use FR, and use it in a manner that respects the privacy rights of Canadians. This section discusses both potential sources of legal authority for the use of FR by police agencies, as well as limits on those potential uses.

35. Police agencies should obtain a legal opinion on whether they have the authority to implement or operate a proposed FR program, and on whether such a program adequately respects individuals' rights. Unless these conditions are met, the proposed program cannot proceed.

36. Canadian jurisdictions do not yet have legislation specifically addressing FR technology, with the exception of Quebec, which has enacted legislation governing biometrics.[2]

37. Since FR involves the collection and use of personal information, it is subject to applicable privacy legislation. Law enforcement must also determine whether FR is compliant with the Charter and human rights laws.[3] The extent to which these laws permit police use of FR is unclear.

[2] *An Act to establish a legal framework for information technology*, CQLR c C-1.1. This regime may be updated by Bill 64.

[3] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, *1982,* being Schedule B to the *Canada Act* 1982(UK), 1982, c 11 [Charter], s. 8.

Sources of legal authority

38. There is no specific legal framework for FR use in Canada. Rather, the legal framework comprises a patchwork of statutes and the common law. Federal and Provincial privacy laws provide a starting point for understanding the existing framework by requiring police agencies – or anyone acting on their behalf – to have lawful authority in order to collect and use the personal information of individuals.

39. As described in the previous section, FR requires that personal information be collected and used at multiple stages, such as: training a FR algorithm, creating a face database, collecting image(s) to be compared against that database, and possibly others. Lawful authority must exist for all steps that implicate personal information. Additionally, where police use vendors or third parties to supply FR services, including FR databases, police must ensure that these suppliers have the lawful authority to collect and use the personal information contained in their services.

40. Sources of legal authority can include statutes or common law. Please note that the following discussion is primarily for illustrative purposes, and should not be interpreted as a comment on the validity or scope of potential legal authorities.

Judicial Authorization

41. Police agencies may seek and obtain judicial authorization to collect and use faceprints in circumstances that merit such action. The *Criminal Code* provides for warrants that permit intrusion on individuals' privacy when a judge is satisfied that there are reasonable grounds to believe that an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique or device; that it is in the best interests of the administration of justice to do so; and in instances where there is otherwise no statutory basis for doing so.[4] These authorizations are subject to the usual requirements for obtaining a warrant, in addition to any conditions or limitations imposed by courts when granting them.

Statutory Authority

42. The *Identification of Criminals Act* allows police agencies to fingerprint or photograph individuals charged with, or convicted of, certain crimes.[5] It permits these identifiers to be used for the purposes of identifying criminals, and providing information to officers and others engaged in administrating and executing the law. The *Identification of Criminals Act* does not, however, authorize the indiscriminate collection of photographs of other individuals at the broader population level. Legal advice would be required to determine if - and in what circumstances - this Act provides a legal basis for a specific use of FR applied to existing mugshot databases collected under this authority.

[4] *Criminal Code*, RSC 1985, c. C-46, at s.487.01.

[5] *Identification of Criminals Act*, RSC, 1985, c. I-1.

Common law authority

43. Police agencies have a crucial role in furthering public interests such as the preservation of peace, the prevention of crimes, and the administration of justice.[6] The common law, like statutory authorities, can authorize police actions that infringe on individual liberties in the pursuit of these societal goals. The term “liberty” in discussion of common law police powers encompasses constitutional rights and freedoms such as privacy, discussed further below.[7]

44. Canadian courts have set out limitations on police powers provided by common law.[8] In order for a police action to be authorized by common law it must:

    1. fall within the general scope of a statutory or common law police duty; and
    2. involve a justifiable exercise of police powers associated with that duty.[9]

45. The second requirement entails an assessment of whether the police action “is reasonably necessary for the fulfillment of the duty” and considers three factors:

    1. the importance of the performance of the duty to the public good;
    2. the necessity of the interference with individual liberty for the performance of the duty; and
    3. the extent of the interference with individual liberty.[10]

46. These factors require that the interference with liberty be necessary given the extent of the risk and the liberty at stake, and no more intrusive to liberty than reasonably necessary to address the risk.[11]

47. Judicial consideration of police use of FR has so far been limited, and Canadian courts have not had an opportunity to determine whether FR use is permitted by common law.[12] If FR use interferes with individuals’ reasonable expectations of privacy (“REP”) and is not enabled by a statute or common law, authorization under section 487.01 of the Criminal Code will be generally required for its use.

[6] For example, see *Royal Canadian Mounted Police Act*, RSC, 1985, c. R-10, at s.18.

[7] *R v Clayton*, 2007 SCC 32 at para. 46.

[8] *R v. Waterfield*, [1963] 3 All ER 659, *R v. Stenning*, 1970 CanLII 12 (SCC), [1970] SCR 631, *Fleming v. Ontario*, 2019 SCC 45

[9] *Fleming v. Ontario*, *ibid* at para. 46.

[10] *Ibid.* at para. 47.

[11] See *Clayton, supra* note 8 at para 21.

[12] See e.g. *R. v. Voong*, 2018 ONCJ 352, which does not address common law police powers, but represents the very limited Canadian jurisprudence on police FR use.

Respecting Canadians' rights

48. While police agencies require legal authority to proceed with a FR program, they must also protect the rights of individuals. Protections can be found in the Charter, as well as federal and provincial privacy legislation.

Privacy legislation

49. Privacy legislation sets out the conditions under which public agencies may collect, use, disclose, and retain individuals' personal information. Public institutions, including police agencies, are generally authorized by privacy legislation to collect personal information for valid purposes. For example, some provincial public sector privacy legislation permits the collection of personal information for "law enforcement" purposes.[13] Police agencies would need to determine whether the collection of personal information by FR falls within the scope of "law enforcement" as defined by the legislation, or is otherwise authorized by one of the other permitted purposes for collection of personal information set out in the legislation. Under federal legislation, the collection of personal information must relate directly to an operating program or activity of the federal institution collecting the personal information.[14] This means that federal institutions must ensure that they have parliamentary authority for the program or activity for which the information is being collected.[15]

50. While the requirements for valid collection of personal information vary by jurisdiction, the privacy principles discussed below are found in many privacy laws that will apply. Once collected, police agencies may generally only use personal information for the purpose for which the information was collected or compiled, or for a use consistent with that purpose, unless otherwise authorized. Compliance with privacy statutes does not necessarily cure any legal defect that may exist under the Charter.[16]

The Charter

51. In addition to a general interest in being left alone and free from police interference,**[17]** the Charter gives individuals the right to be secure against unreasonable searches and seizures by police.**[18]**

52. To determine whether police action constitutes an unreasonable search, a court first considers whether a search occurred. This depends on whether an individual had a REP

[13] For example, see Alberta *Freedom of Information and Protection of Privacy Act*, sections 33(b).
[14] *Privacy Act*, R.S.C., 1985, c. P-21, s.4.
[15] Treasury Board of Canada Secretariat, *Directive on Privacy Practices,* s. 6.2.6.
[16] Department of Justice, "Charterpedia: Section 8 – Search and Seizure" (accessed May 13, 2021)
[17] *Hunter v Southam Inc*, [1984] 2 SCR 145
[18] *Charter*, *supra* note 2 at s.8.

within the context of the possible search, with consideration given to the totality of circumstances. The analysis of whether a search occurred is based on a number of interrelated factors such as the subject matter of the search and the nature of the individual's privacy interests therein. This means not only the source photographs and faceprints themselves, but also any additional information about an individual's actions and whereabouts that may be revealed when connecting personal identity, video footage, meta-data, such as date and time stamp, and other identifying information.[19] The existence of a REP is also dependent on the context in which FR use occurs, and that may give rise to an individual's subjective REP. Additionally, courts consider whether that REP is objectively reasonable, informed by what levels of privacy individuals ought to expect in a free and open society, highlighting that expectations of privacy are not just descriptive, but also normative in nature.[20]

53. While citizens' reasonable expectations regarding the use of FR are not yet clearly established, it is clear that FR uses sensitive personal information that generally cannot be changed, and can be used to identify people for various privacy sensitive purposes. We therefore presume that FR will generally raise a REP, whether online or in person, despite faces being publicly visible. Individuals do not expect to be the subject of surveillance when going about their normal and lawful activities, and generally maintain some degree of a REP even when in public spaces.[21] Conversely, even if an individual might expect FR to be used, greater privacy invasions do not become socially acceptable simply due to technological advancements or evolving police practices.[22]

54. If a search occurs in a context where the concerned individual has a REP, a court will then determine whether the search was reasonable. In order for a search to be reasonable, it must be authorized by a reasonable law, and be conducted in a reasonable manner. When a police action is found to be authorized by the common law, it will generally be considered Charter compliant as the tests for common law and Charter compliance are similar.[23]

Necessity and Proportionality

55. The privacy principles of necessity and proportionality ensure that privacy-invasive practices are carried out for a sufficiently important objective, and that they are narrowly tailored so as not to intrude on privacy rights more than is necessary. In the case of law enforcement, there is a clear public interest in ensuring public safety, but also in protecting individuals' fundamental right to privacy. While the right to privacy is not absolute, neither can the pursuit of public safety justify any form of rights violation. Therefore, police may only use means justifiable in a free and democratic society.

[19] *R v Spencer*, [2014] 2 SCR 212

[20] *R v Jarvis,* 2019 SCC 10, at para. 68, *R v Wise*, [1992] 1 SCR 527

[21] *Jarvis*, *ibid*.

[22] *R v Tessling*, 2004 SCC 67, at para. 42.

[23] *Fleming*, *supra* note 9 at para 111.

56. As noted above, necessity and proportionality exist in varying degrees in privacy laws, the common law, and the Charter.[24] In the context of FR use, necessity and proportionality will generally require an assessment of the following:

57. **Necessary to meet a specific need:** Rights are not absolute, and can be limited where necessary to achieve a sufficiently important objective.[25] Necessary of course means more than useful. Significantly, the objective of an FR program must be defined with some specificity. It is not enough to rely on general public safety objectives to justify such an intrusive technology as FR. Police agencies should demonstrate the pressing and substantial nature of the specific objective through evidence. Further, the personal information collected should not be overbroad; it should be tailored and necessary to achieve the specific goal.

58. **Effectiveness:** Police must be able to demonstrate that collection of personal information actually serves the purpose of the objective. Police should provide evidence that demonstrates why the specific use of FR being proposed will likely be effective in meeting specific program objectives. This demonstration of effectiveness should take into account any known accuracy issues associated with the specific use.

59. **Minimal Impairment:** Police agencies' intrusion on individuals' privacy must not extend beyond what is reasonably necessary to achieve the state's legitimate objective.[26] The scope of a program should be as narrow as possible. If using FR, police agencies should be able to demonstrate that there are no other less privacy invasive means that will reasonably achieve the objective,[27] and be able to show evidence as to why less privacy invasive measures are not used.[28]

60. **Proportionality:** This stage requires an assessment of whether the intrusion on privacy caused by the program is proportional to the benefit gained.[29] Police agencies should therefore seek, first, to identify how their specific use of FR will impact the privacy of individuals, having regard to general factors such as those mentioned in the introduction, but also impacts specific to their intended use of FR, for instance on certain groups. Then, police agencies should consider whether these intrusions on privacy are justified by the benefits of the specific deployment of FR. Inherent in this step is the recognition that not all objectives carry the same weight. For example, preventing a known terrorist plot would justify a greater privacy intrusion than catching someone who committed a minor act of vandalism. In making this assessment, law enforcement agencies must be open to the possibility that, in a free and democratic society, a

[24] For instance, the *Oakes* test is primarily used to test the constitutionality of statutory laws, but has also been used to test police conduct within the context of common law powers: *R v Clayton*, supra note 8.
[25] *Canada (AG) v JTI-Macdonald Corp*, 2007 SCC 30 at para 36.
[26] *Frank v. Canada (Attorney General),* 2019 SCC 1 at para. 66.
[27] *R v KJR*, 2016 SCC 31 at para 70.
[28] *Thompson Newspapers Co v Canada (AG)*, [1998] 1 SCR 877.
[29] *R v KJR,* supra note 26 at para 77.

proposed FR system which has a substantial impact on privacy (such as via mass surveillance) may never be proportional to the benefits gained. Where the impact is substantial, law enforcement agencies should be particularly cautious about proceeding in the absence of clear, comprehensive legal safeguards and controls capable of protecting the privacy and human rights of members of the general public. Seeking warrants and court authorizations can assist with ensuring that a proposed FR use meets the proportionality standard.

61. Recall that these privacy principles repeat and overlap with legal authorities as well as individuals' privacy rights. These recurrent themes reinforce the need for police agencies to respect limits to law enforcement powers, and ensure that the simultaneous goals of public safety and respect for privacy are achieved at the same time.

Designing for privacy

62. It is important to design initiatives with privacy protections built in from the outset. This is commonly referred to as "privacy by design". Following a privacy by design approach will help to ensure that privacy protection is an essential component of any FR initiative or system. To be most effective, such protections must be incorporated during initial conception and planning, following through to execution, deployment, and beyond.

63. Implementing privacy by design means police agencies must formally integrate privacy protections **before** engaging in any use of FR technology. Privacy protections must also be designed to protect **all** personal information involved in an initiative, including training data, faceprints, source images, face databases, and intelligence inferred from FR searches, in addition to any other personal information that may be collected, used, disclosed, or retained.

Privacy impact assessments

64. A key element of putting privacy by design into practice is to conduct a privacy impact assessment (PIA). A PIA is a widely accepted tool for analyzing and addressing the impacts of initiatives on privacy. When used properly, PIAs help to ensure that programs and activities meet legal requirements and mitigate privacy risks.

65. Police agencies should conduct a PIA before implementing or making substantial modifications to initiatives that involve the collection, use, or disclosure of personal information, including pilot projects. In some Canadian jurisdictions, government institutions are required to conduct PIAs by policy or legislation.

66. When conducting a PIA, police agencies are expected to:

- Conduct the PIA in accordance with any applicable legislative and policy requirements

- Follow any guidance issued by the relevant privacy commissioner on the PIA process[30]
    - Where no such guidance exists, police agencies may consult with the oversight body in their jurisdiction
- Document the PIA process in a PIA report
- Mitigate any risks raised in the PIA and designate an individual responsible for managing residual risks
- Publish a summary of the completed PIA report before deploying FR, and update it if planning and implementation of the initiative evolve
- Conduct a new PIA (or, if appropriate, amend the existing PIA) if major changes are made to the initiative that could impact the collection, use, disclosure, or retention of personal information

67. As police agencies assess privacy risks through the PIA process, they should consider all relevant privacy risks. This includes assessing the potential impacts of the initiative on:

    - Individuals
    - Communities in which FR may be deployed
    - Groups that may be disproportionately harmed by privacy incursions
    - Public confidence in the collection and use of personal information by law enforcement agencies
    - Human and democratic rights, including rights to privacy, equality, peaceful assembly and free expression

68. After assessing these potential impacts, police agencies should not proceed with further planning and implementation of the initiative unless they can clearly explain:

    (1) Why the proposed use of FR is necessary to meet a specific need that is rationally connected to a pressing or substantial public goal
    (2) What the expected benefits of the initiative consist of, and how they are proportionate to the risks involved
    (3) Why other less intrusive measures are not sufficient
    (4) How risks will be minimized during implementation of the initiative

69. Police agencies should document explanations for the above along with their risk assessment in the PIA report. To assist in doing so effectively, police agencies should:

    - Engage with relevant stakeholders and privacy experts about the potential privacy impacts of the proposed initiative

[30] Federal. Expectations: OPC's Guide to the Privacy Impact Assessment Process
Ontario. Planning for Success: Privacy Impact Assessment Guide
Alberta. Privacy Impact Assessments
Quebec. Guide d'accompagnement: Réaliser une évaluation des facteurs relatifs à la vie privée

- Consult their privacy commissioner's office early in the planning phase of the initiative, in jurisdictions where these offices offer advisory services
- Consult their human rights commissioner's office when planning the initiative, given the strong connection between privacy rights and broader human rights, including the right to be free from discrimination
- Ensure the PIA is conducted by individuals with appropriate competencies in identifying and analyzing privacy risks. This process should involve key parties in the initiative, which may include:
    - legal counsel
    - privacy staff
    - program staff (those who will administer the initiative)
    - stakeholder groups (those who may be affected by the initiative)
    - technical experts
    - management
    - third party service providers

Monitoring and re-assessment

70. Privacy risk analysis is an ongoing process that does not stop with the conduct of a PIA or the deployment of an initiative. PIAs should be evergreen and can help to ensure the ongoing management of privacy risks as part of a police agency's overall risk management strategy.

71. Police agencies should monitor and re-assess privacy risks, and the effectiveness of privacy protections, on an ongoing basis. This can be done by implementing the following best practices as FR initiatives are deployed:

- Audit the initiative at regular intervals
    - Audits should address both the initiative's compliance with legal requirements, and program operators' adherence to the policies and procedures set out for the initiative (see also recommendations in the Accountability section below)
    - Audits should also address compliance by third parties with the terms and conditions of information sharing and service agreements
- Conduct regular reviews (for example, annually) of program effectiveness
    - Reviews should assess the extent to which program activities are achieving the goals of the initiative, using demonstrable criteria (for example, number of arrests or convictions resulting from the program, etc.)
- Review and update safeguards, policies, and procedures as needed and as appropriate to ensure continued compliance with privacy responsibilities
    - For instance, agencies may need to adjust policies in light of audits, program reviews, breaches, law reform, new guidance or technological developments
- Review and, where necessary, update information sharing and service agreements with third parties
- Review and update training procedures as needed and as appropriate

  - Ensure that changes to policies and procedures are communicated promptly to relevant personnel
- Monitor information holdings regularly (for example, databases of personal information) to ensure records are being retained and destroyed in accordance with established policies and procedures
- Document any changes to the program in the PIA
- Engage with external stakeholders throughout deployment (for example, privacy experts, community groups, civil society organizations)
  - Stakeholders can be a valuable source of feedback about the privacy impacts of initiatives

Accuracy

72. Police agencies must ensure that personal information collected and used as part of a FR initiative is sufficiently accurate and up to date. The accuracy of FR software cannot be taken for granted given the serious risks to individuals' rights posed by the collection and use of inaccurate information.

73. Fulfilling accuracy obligations within the context of a FR initiative requires consideration of the FR system *as a whole*. FR is comprised of a number of components, each of which raises unique considerations. Only when the constituent parts of a FR system process personal information accurately and fairly can the system as a whole be said to do the same.

74. With respect to training data, one of the main considerations is the role it may play in contributing to bias in the FR system. If the training data used to generate a FR algorithm lacks sufficient representation of faces from certain demographics, the algorithm will likely produce disparate accuracy metrics across groups. It is possible for a FR algorithm to produce flawed results, particularly where it has been trained on non-representative or otherwise biased data. Studies have demonstrated considerable variation in FR algorithms with respect to the error rates they produce for faces of individuals from different racial backgrounds and across genders,[31] with other research showing that a lack of diverse and high quality training data is the main culprit.[32]

75. Regarding the FR algorithm, there are three key considerations to be aware of with respect to accuracy. The first is that accuracy is understood *statistically*. The output of a FR algorithm is a probabilistic inference as to the likelihood that two images are of the same person. It is not a verified fact about the individual. As such, accuracy is not a binary "true/false" measure, but rather is computed based on the observed error rates of the algorithm across searches. There are two types of errors to consider:

[31] See Patrick Grother, Mei Ngan, and Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Interagency Report 8280, National Institute of Standards and Technology, December 2019.
[32] See Jan Lunter. Beating the bias in facial recognition technology. *Biometric Technology Today*. 2020;2020(9):5-7. doi:10.1016/S0969-4765(20)30122-3.

1. false positives (also known as “type I” errors) where the algorithm returns a candidate match in the face database that is not of the individual in the probe image; and
2. false negatives (also known as “type II” errors) where the algorithm fails to return a genuine match in the face database even though the database contains one.

76. The second consideration is that there is generally a trade-off between the false positive and false negative rate of a FR algorithm. The reason for this has to do with another component, the threshold for a probable match. Depending on how high (or low) the threshold is set, a FR algorithm will generally return fewer (or more) candidate matches. However, how many results the algorithm returns has implications on its error rates. While a higher threshold will return only higher probability candidates and lead to fewer false positives, this same threshold will in general make the algorithm more likely to miss lower probability matches and potentially lead to greater false negatives.

77. Lastly, it is important to consider that the determination of an appropriate threshold will depend on the nature, scope, context and purpose of the FR initiative, taking into account the risks to the rights and freedoms of individuals. Strictly speaking, there is no single appropriate threshold. It is a matter of prioritizing the reduction of certain types of errors based on the nature and severity of risks they pose to individuals, while at the same time ensuring the overall effectiveness of the FR system.

78. The face database is another component that raises important issues regarding accuracy and fairness. One consideration is the quality and/or age of the images and the effects this may have on the accuracy of the FR system. For example, studies have shown that the time elapsed between two images of the same individual increases false negative rates.[33] However, it is also important to consider the demographics of *who* is in the face database and whether the disproportionate representation of certain groups may lead to adverse effects. A FR system may be susceptible to a “feedback loop” where the makeup of individuals in a face database leads police to repeatedly cast suspicion on them, their associates or their community, thereby increasing the disproportionality of their demographic representation over time.

79. A final component to mention is human review. While human review serves as an important mitigation measure to reduce the risks of inaccuracy and bias, it may also inadvertently reintroduce those very same risks into the FR system. Unlike computers, humans can be overwhelmed with too much information. Effective human review requires content moderation training, and for reviewers to be granted a non-rushed amount of time proportionate to the number of candidate matches they are expected to adjudicate. However, even with sufficient training and time, human review may be unduly influenced by the level of statistical precision in the FR system. It is important to avoid “automation bias” or the tendency to over-rely on automated systems when making

[33] See Patrick Grother, Mei Ngan, and Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 2: Identification. Interagency Report 8271, National Institute of Standards and Technology, September 2019.

human decisions. Just because the FR system uses mathematical calculations does not necessarily mean that its predictions are accurate or fair.

80. Given the above, it is imperative that police agencies take steps to minimize inaccuracy and bias in any deployment of FR technology. These steps should include the following best practices:

81. Police agencies should require FR vendors to:

- Make their FR algorithms available for independent external testing
    - The testing should include an evaluation of the accuracy of the algorithm as well as its performance across distinct socio-demographic populations (for example, racial, gender and age groups)
- Indicate, in the results of each FR search, the similarity score; that is, an estimate of the probability that a given match is accurate (for example, as a percentage).

82. Police agencies should also:

- Determine an appropriate threshold so as to prioritize reducing certain types of error based on the nature and severity of risks, while ensuring the overall effectiveness of the FR system
- Internally test for bias and inaccuracy in the performance of FR system as a whole before deployment, and routinely during deployment
- Ensure testing is carried out by individuals or organizations qualified to independently assess the performance of FR systems
- Include the similarity score, as indicated in FR search results, when recording or disclosing information about a match
- Discontinue FR use if internal or external testing reveals:
    - insufficient statistical accuracy in the FR system, or
    - meaningful variation in error rates across socio-demographic populations

83. Police agencies should not:

- Fully automate administrative decisions based on the results of FR matching procedures
    - In other words, decisions that affect legal rights, privileges, or interests should be made by humans, including, for example, decisions to detain, investigate or charge individuals in relation to a crime
- Act on a FR match unless that match has been reviewed within a suitable timeframe by an officer trained in FR identification procedures and limitations

Data minimization

84. Police agencies must limit the collection of personal information to that which is directly relevant and necessary for the specific objectives of a FR initiative.

85. To assist in doing so, police agencies should implement the following practices for data minimization:

- Minimize the amount of personal information collected and used to perform each task, based on the amount of personal information needed to complete the task
    - Images used to perform a FR search should be cropped to prevent identification of individuals in the image who are not the subject of the search.
- Promptly and irretrievably discard personal information that falls outside the scope of the initiative, including personal information collected inadvertently during the initiative
- Include a policy framework supported by mechanisms to systematically verify that data collected by the initiative falls within the initiative's lawful authority to collect

86. When collecting and storing personal information in FR initiatives, police agencies should:

- Not cross-link the information with personal information contained in other databases, except to the extent that doing so is necessary to fulfill the lawful objectives of the initiative
- To the greatest extent possible, store the information in separate databases from other personal information, and isolate those databases from other networks

Purpose limitation

87. Police agencies must ensure that personal information is only used for the purpose for which it was collected, or a purpose consistent with that purpose. They must also ensure that each use of personal information falls within the scope of the initiative's lawful authority.

88. To assist in meeting these requirements, police agencies should implement a comprehensive set of administrative, technical, and physical controls for managing access to, and use of, data and software used in FR initiatives.

89. These controls should include:

- A mechanism for officers to inform senior management about new investigative tools that may involve the collection or use of biometric information
    - While management approval should be required before using new investigative tools, approval does not replace applicable privacy requirements, including the conduct of a PIA
- A system for authorizing individuals to access and use FR software and related databases only as necessary to fulfill objectives of the initiative

- A protocol that specifies the circumstances under which officers are authorized to perform a FR search
- A system for documenting decisions to initiate a FR search
- Standard operating procedures for performing a FR search, including instructions specifying what data may be used and how the search is to be performed
- A mechanism that holds authorized individuals meaningfully accountable for misuse of FR software or related data, whether intentional or accidental

90. These controls should prevent:

- Access to FR software and data by unauthorized individuals
- Use of FR software or data for unauthorized purposes
- Use of any FR software outside of a lawful initiative that is approved and overseen by senior management
- Experimentation with new biometric technologies on real-world data, outside of lawful initiatives that are approved and overseen by senior management

91. Police agencies must also ensure that third parties engaged on their behalf do not use personal information transferred to them during an initiative for purposes other than those that are consistent with the original purpose of collection. For example, if a police agency transfers an image to a third party FR software vendor for identification purposes, the police agency must take reasonable steps to ensure the vendor does not use the image (or associated faceprint data) as training data, or enter that data into a face database for comparison in future searches.

92. To help meet this requirement, police agencies should use information sharing agreements (ISAs) to codify limitations on the use of personal information disclosed to third parties during an initiative, as well as other privacy protections.[34] This includes disclosures to FR software vendors of images to be matched, as well as disclosures to any other organizations (for example, other law enforcement bodies) of images, databases, or other personal information.

93. Subject to specific legal requirements in each jurisdiction, ISAs should specify, at a minimum:

- The lawful authority under which information is to be disclosed
- The specific elements of personal information being disclosed
- The specific purposes for the disclosure
- Limits on use and onward transfer

[34] Information sharing agreements (ISAs) are written records of understanding between parties that outline the terms and conditions under which personal information is shared between the parties. They may exist in a variety of forms, including letters of understanding, memoranda of understanding, terms of engagement, or other such mechanisms. Parties often enter into ISAs as part of a broader service agreement. See the Treasury Board of Canada Secretariat's Guidance on Preparing Information Sharing Agreements Involving Personal Information for more details.

- Specific safeguarding measures
- Data localization requirements, if any
- Data breach procedures
- Retention periods and data destruction requirements
- Accountability measures, including compliance monitoring

Data security

94. Personal information must be protected by appropriate security measures relative to the sensitivity of the information.

95. Given the high sensitivity of facial data, police agencies are expected to implement highly protective security measures as part of FR initiatives. At a minimum, these should include the following measures, although these may not be sufficient in all cases:

    - Use encryption and other digital safeguarding tools to secure data while in storage and while in transit between databases, servers and end-user devices
    - Ensure records and equipment, including memory disks, servers and end-user devices, are used and stored only in secure physical locations
    - Log all access to, and use of, FR software and databases
    - Review and update security measures regularly to address evolving security threats and vulnerabilities
    - Use ISAs to ensure any third parties involved in the initiative follow relevant best practices for data security

96. Data security requirements may also require that all personal information collected or created by police during a FR initiative be stored in Canada. In some Canadian jurisdictions, police agencies are explicitly required to do so by law or policy instruments.[35] In others, they must first ensure that personal information released outside of its jurisdiction will receive equivalent protection.[36]

[35] For example, British Columbia's *Freedom of Information and Protection of Privacy Act* has data localization provisions that require all public bodies, including police forces, to only access and store personal information in Canada.

[36] For example, see s. 70.1 of Quebec's *Act respecting Access to documents held by public bodies and the Protection of personal information*.

Retention

97. Police agencies should not retain personal information for longer than is necessary to fulfill the purposes of an initiative.

98. Given the high sensitivity of facial data, it is especially important that police agencies promptly and securely destroy any personal information that does not need to be kept.

99. In FR initiatives, some personal information may be needed for longer than other personal information. For instance, retention periods may vary for:

- Original media from which facial data was collected (for example, a digital image or video)
- Faceprints created by FR software when analyzing an image
- Intelligence inferred from the outputs of FR analysis

100. Appropriate retention periods for different components of FR data may also vary depending on the context of FR use. For example, it may sometimes be necessary to retain images or faceprints of individuals who are identified as persons of interest to the police, but images and faceprints collected from the general population should be promptly destroyed unless there is a specific and lawful purpose for retaining them, or another legal requirement to do so. Similarly, it may sometimes be necessary to retain faceprints or video surveillance data for the duration of an active police investigation, but faceprint or video surveillance data that is not relevant to a police investigation should be destroyed.

101. In order to ensure personal information is not retained for longer than it is needed in FR initiatives, police agencies should:

- Identify applicable retention periods for personal information at the outset of its collection
- Apply different retention periods to different forms of personal information, as appropriate
- Conduct reviews of data holdings at regular intervals to identify personal information that may have been retained unnecessarily
- Implement protocols to ensure personal information is destroyed securely and promptly upon expiry of the applicable retention period
- Use ISAs to ensure any third parties involved in the initiative destroy personal information promptly and securely at the end of the applicable retention period
- Implement wind-down protocols for destroying personal information if the initiative is discontinued

Openness, transparency and individual access

102. Wherever possible, individuals and the public must be informed of the purpose of the collection of their personal information, including how the information may be used or disclosed.

103. In general, when FR technology is used, individuals should be informed at the time their image is collected that their image may be collected and stored in a face database. At the same time, individuals should be informed of the purpose(s) for which their image is collected. Such transparency measures are important, in part because they help to facilitate individuals' right to request access to their recorded personal information.

104. Police agencies should implement policies and procedures to accommodate access requests whenever possible, including any time faceprint data is collected from the general public.

105. In the context of police initiatives, however, it may not always be possible to provide individuals with access to complete information about the collection of their personal information, for example when individuals are the subject of an ongoing investigation.

106. Given the sensitivity of facial data, and the privacy risks implicated by FR use, it is therefore especially important for police agencies to implement transparency measures at the program level for FR initiatives. Doing so can help to inform the public about FR initiatives, and can increase public confidence that such initiatives are being implemented responsibly.

107. Police agencies should implement the following transparency measures in FR initiatives:

- Disclose the initiative on the police agency's public website, including an explanation of the initiative and its objectives, as well as a link to the PIA summary
- Update public disclosure of the initiative regularly as the initiative moves from planning and development to implementation
- Publish regular reports on program activity
    - Reports should include:
        - statistics on the number of searches performed in a given period
        - the purpose for which those searches were performed
        - statistics concerning the effectiveness of the initiative, in light of its objectives
        - the results of any accuracy or bias testing performed by the police agency, with justification for any variations across groups
- Make data on FR system use, including search data, available for oversight purposes

Accountability

108. Police agencies are responsible for personal information under their control and should be able to demonstrate their compliance with legal requirements.

109. An accountable police agency should have a privacy management program in place, with clear structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with privacy laws.

110. To help ensure accountability for FR initiatives, police agencies should implement the following accountability measures. These should be considered a baseline from which to approach program accountability, rather than an exhaustive checklist:

- Have policies and procedures in place for handling personal information that is collected, used, created, disclosed and retained over the course of an initiative
    - Where appropriate, policies and procedures specific to FR initiatives should be integrated into the police agency's overall privacy management program
- Establish a clear reporting structure for the initiative that designates an individual responsible for overseeing compliance with privacy obligations
- Establish a specialized training program for individuals authorized to use FR software
    - Completion of the training program should be required in order to gain authorization to access and use FR software and related databases
- Log all uses of FR software, including all searches and the credentials of individuals who performed each search
    - The logging procedure should be automated, and beyond the control of individuals who access and use the system to perform FR searches.
    - Logging FR use is a key means of facilitating oversight functions by public bodies; as such, logs should be made available to oversight bodies on request
- Log all disclosures of personal information, with a record of the authority under which the information was disclosed (including reference to the governing ISA), to whom the information was disclosed, the means of disclosure, any conditions attached to the disclosure, and the identity of the program operator who authorized the disclosure
- Undertake periodic reviews of program activity, including assessment of compliance with privacy requirements and effectiveness of the initiative in meeting program objectives
- Establish a clear protocol for redressing non-compliance with the policies and procedures set out in the initiative
- Update the PIA if major changes are made to the initiative that could impact the collection, use, or retention of personal information

111. As well, police agencies should provide appropriate training to all individuals with access to FR software and related databases, including training on policies and procedures for

handling FR data. Doing so can help to ensure program operators adhere to the initiative's policies and procedures for collecting, storing, using and disclosing personal information.

112. As part of this training, police agencies should require program operators to understand and analyze the privacy risks associated with the initiative, including the limitations associated with FR technology. These include:

- The potential for bias in FR matching procedures on the basis of race, gender and other relevant demographic characteristics.
- The potential for errors due to low quality probe images or outdated errors in the face database
- The importance of human review of FR matches for the prevention of automation bias

113. Police agencies should update training as needed to ensure program operators always have sufficient knowledge, competencies and experience to fulfill their duties in compliance with legal requirements.

Conclusion

114. Given the significant risks posed by FR, we expect police agencies to assess the risks associated with any contemplated use of FR and to mitigate potential harms by building appropriate privacy protections into the design of proposed initiatives. If police agencies proceed with FR use, they must follow through on privacy protection over the lifespan of the initiative.

115. Above all, police agencies must ensure that any use of FR complies with the law. While specific legal requirements vary by jurisdiction, the recommendations in this guidance document can help to ensure proposed uses of FR meet legal requirements, minimize privacy risks, and respect Canadians' fundamental right to privacy.

Summary of Recommendations

Below is an abbreviated summary of key recommendations made in this guidance document. The summary is compiled for reference purposes only; please consult the guidance document for full recommendations.

When proposing, developing, and implementing initiatives involving the use of FR technology, we recommend police agencies:[37]

- Ensure lawful authority exists for each collection, use, retention, and disclosure of personal information.
    - Lawful authority must exist for all steps of FR use, including training a FR algorithm, creating a face database, and collecting probe images.
    - Ensure any third parties involved in the collection or use of personal information operate with lawful authority.

- Design for privacy
    - Integrate privacy protections into proposed initiatives before using FR technology.
    - Conduct a PIA to help ensure FR programs meet legal requirements and to identify and mitigate privacy risks.
    - Monitor and re-assess privacy risks and the effectiveness of privacy protections on an ongoing basis.

- Ensure personal information is accurate and up to date.
    - Test data and systems as appropriate to identify and reduce inaccuracy and bias.
    - Keep a "human in the loop" to review FR matches.

- Minimize collection of personal information to that which is directly relevant and necessary based on the objectives of the initiative.

- Ensure personal information is used only for the purpose for which it was collected, or a purpose consistent with that purpose.
    - Implement administrative, technical, and physical controls for managing access to, and use of, FR data and software.
    - Use ISAs to limit use of personal information disclosed to third parties.

- Protect personal information using security measures that are appropriate given the sensitivity of the information and use ISAs to ensure third parties are required to do the same.

[37] Depending on the jurisdiction, some of these recommendations may be legal requirements, while others may be best practices. Police agencies are responsible for ensuring any initiative involving FR use complies with all applicable legal requirements within their jurisdiction.

- Retain personal information for no longer than is necessary to fulfill the purposes of the initiative (or as otherwise required by law).
    - Appropriate retention periods for different components of FR data may vary depending on their use.

- Implement openness and transparency measures as appropriate to allow individuals and the public to be informed about the initiative.
    - Implement policies and procedures to accommodate access requests whenever possible.

- Implement effective accountability measures.
    - Implement a privacy management program with clear structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with privacy laws.
    - Log all uses of FR, including all disclosures of personal information outside the organization.
    - Ensure all personnel with access to FR systems are appropriately trained.