



PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

285 McLeod Street, Suite 200, Ottawa, ON K2P 1A1

October 15, 2021

Office of the Privacy Commissioner of Canada
Consultation
30 Rue Victoria
Gatineau, QC K1A 1H3

BY EMAIL to: OPC-CPVPconsult1@priv.gc.ca

Re: *Notice of consultation and call for comments – Privacy guidance on facial recognition for police agencies*
Submission of the Public Interest Advocacy Centre

Dear Office of the Privacy Commissioner of Canada Staff,

The Public Interest Advocacy Centre (PIAC) is pleased to provide the OPCC with our submission on the Notice of consultation and call for comments – Privacy guidance on facial recognition for police agencies, which is attached.

Sincerely,

John Lawford
Executive Director & General Counsel
613-562-4002 ext. 125
jlawford@piac.ca

Notice of consultation and call for comments – Privacy guidance on facial recognition for police agencies

PIAC SUBMISSION

Contents

INTRODUCTION.....	1
I. The Current Legal and Policy framework is insufficient to regulate police use of FRT	2
i. Case study: <i>R v Bridges</i>	5
II. The appropriate approach to future policy is two-pronged: implementing both a standalone legal framework and broader privacy reforms	6
i. The danger of a prospective Bill C-11 revival	8
CONCLUSION.....	10

INTRODUCTION

1. The Public Interest Advocacy Centre (“PIAC”) is pleased to provide comments to the Office of the Privacy Commissioner of Canada’s (OPCC) consultation and call for comments regarding the OPCC’s draft guidance on facial recognition for police agencies. The draft guidance aims to help police agencies understand and discharge their current legal responsibilities in a manner that minimizes privacy risks and respects the fundamental right to privacy. As PIAC has long advocated for stronger privacy protections in the public and private sector, we welcome the opportunity to comment on a matter that engages both.
2. “Will this guidance have the intended effect of helping to ensure police agencies’ use is lawful and appropriately mitigates privacy risks?” This first feedback question is at the heart of any initiative aiming to ensure that law enforcement’s practices surrounding facial recognition technology (FRT) comply with the law and broader privacy principles. PIAC submits that the answer to this question is the starting point for realistic, practical discourse on the existing legal framework around police use of FRT, and on the growing role of the private sector therein.
3. PIAC’s answer is this: The draft guidance will indeed help guide police agencies that acknowledge their past faults and fully commit to reforming internal policies in good faith, but the guidance is not a solution to a legal framework that is, at present, ill-suited to addressing the potential threat of FRT to individual privacy rights and democratic freedoms. The guidance will

15 October 2021

be effective to the extent that police agencies will adopt and publicly commit to incorporating recommended practices into internal policies. It may also provide a court with a standard of review in attempting to craft a common law or other rule in the absence of a controlling statutory regime should the legality of facial recognition be challenged in legal proceedings.

4. Most likely, only a specifically targeted statute can ensure uniform compliance with a privacy-compliant set of rules regarding facial recognition in various contexts, and the current patchwork of common law, some statute law and policy does not circumscribe police use of FRT with enough specificity and clarity. This position distils PIAC's response to a subsequent feedback question: "Is the police use of FR appropriately regulated in Canada under existing law?"
5. An essential part of the FRT discourse in the context of law enforcement is the role of the private sector in providing FR software and databases. The relationship between police agencies and third party agents demands careful scrutiny of how the broader legal framework regulates public-private partnerships, especially where there is a mismatch in privacy obligations between public and private sector laws. Private sector privacy laws, in current form or as envisioned in Bill C-11 (the *Digital Charter Implementation Act, 2020*), cannot become a release lever for accountability in the use of FRT by law enforcement.

I. The Current Legal and Policy framework is insufficient to regulate police use of FRT

6. In the draft guidance, the OPCC itself hints at the inadequacy of the current legal framework, stating that "unlike other forms of biometrics collected by law enforcement, facial recognition is not subject to a clear and comprehensive set of rules," further elaborating that "[i]ts 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."¹ PIAC proposes that a standalone legislation and regulatory framework specifically regulating the use of FRT by police agencies would help to resolve the "uncertainty concerning what uses of facial recognition may be acceptable, and under what circumstances."²
7. As informative as the draft guidance is, PIAC respectfully submits that describing a patchwork of legal authorities that overlap and cover to varying degrees any given use of FRT by police only serves to emphasize a major problem, which is that the current legal framework is confusing. For a new technology as privacy-invasive as FRT and which can be deployed in many different investigative contexts, there should be a single, clear federal framework that does away with guesswork, and is also consistent with privacy and human rights principles and laws, including the *Charter*.

¹ Draft guidance at para 14.

² *Ibid*.

8. The OPCC stated that “[w]hen a police action is found to be authorized by common law, it will generally be considered Charter compliant as the tests for common law and Charter compliance are similar.”³ This is an overstatement that reveals an unconscious bias towards deferring to historical police power that may well not be justified on a modern, sophisticated constitutional analysis. This statement also betrays the difficulty of considering common law policing powers and their interaction with constitutional law. That is precisely the complication and lack of legal clarity we are highlighting.⁴
9. Furthermore, the OPCC points out that “necessity and proportionality exist in varying degrees in privacy laws, the common law, and the Charter.”⁵ So the temptation arises to boil down the current patchwork of legal authorities, each with its own tests and considerations, and to try to distill “general principles” or “guidance” that police agencies must meet to justify its use of FRT. However, PIAC submits that such generality, and possible privacy guidelines, while useful for broad application of laws to police activities, should not be relied upon to justify or excuse police discretion which is not a substitute for law. At best privacy guidance can therefore be used to appropriately dissuade police use of FRT not to justify its use after the fact.
10. Though the common law branch of the legal framework requires that a justifiable exercise of police powers requires consideration of the necessity and extent of the interference with individual liberty, there are few cases that provide guidance on such necessity and the extent of interference on liberty in the context of FRT in Canada, so far.⁶ Police agencies therefore may be tempted to justify the use of FRT for the purpose of mass surveillance, on the theory that though intrusive, it is a necessary interference in the interest of public safety. Even when surveillance activities are excessively intrusive, the issue may not be properly adjudicated until

³ https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/ at para 54.

⁴ See, for example, *R. v. Spencer*, [2014] 2 SCR 212, 2014 SCC 43. As the headnote states, common law investigative policing powers are only confirmed in the *Criminal Code* and are not widened by considering search and seizure and privacy statutes. Whether FRT is a police investigation, or a search and seizure is an open question, further complicating legal analysis:

Whether the search in this case was lawful will be dependent on whether the search was authorized by law. Neither s. 487.014(1) of the *Criminal Code*, nor PIPEDA creates any police search and seizure powers. Section 487.014(1) is a declaratory provision that confirms the existing common law powers of police officers to make enquiries. PIPEDA is a statute whose purpose is to increase the protection of personal information. Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, the police do not gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information. The conduct of the search in this case therefore violated the Charter. Without the subscriber information obtained by the police, the warrant could not have been obtained. It follows that if that information is excluded from consideration as it must be because it was unconstitutionally obtained, there were not adequate grounds to sustain the issuance of the warrant and the search of the residence was therefore unlawful and violated the Charter.

⁵ https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/ at para 55.

⁶ *Fleming v Ontario*, 2019 SCC 45.

15 October 2021

the police conduct is brought squarely before the courts. In addition, as demonstrated in the Clearview AI case, police agencies' own oversight bodies may not even be aware that its forces are using such technologies.⁷

11. There is no guidance in case law, to our knowledge, so far, nor are there specific statutes or regulations regarding acceptable thresholds of accuracy in the context of FRT. Though the draft guidance admirably outlines best practices to minimize inaccuracy and bias, considerable discretion is still left to police agencies regarding acceptable accuracy thresholds, whether FR algorithms are independently tested, the extent to which decisions are automated based on FR results, etc. In our view, the police are not the agency that should be deciding such matters.
12. There are also no clear legal boundaries regarding who is included in a database of pre-enrolled faces that may be used to purportedly identify a specific individual, or to search for “persons of interest” at an event or in a public space. PIAC submits that more detailed rules on inclusion criteria are necessary to dictate what images should be included in such databases. For example, a mugshot of an individual charged with but not convicted of a minor offence is unlikely to merit inclusion in a FR database intended to search for known terror suspects. Furthermore, who counts as a potential terror suspect, and what the threshold is for the necessity of deploying FRT in a crowd is not specified anywhere but is left to security forces by default. Does a large political gathering on its own merit the use of FRT, or should the police have reasonable expectation that specific individuals will be at an event intending to cause significant harm, based on a tip-off or related investigations? Are any types of events those that should be surveilled with or without FRT assistance? These are questions that must be considered to ensure police agencies do not overreach in their discretion to use FRT, especially for mass surveillance purposes.
13. PIAC acknowledges that in time-sensitive circumstances, it may be difficult for police agencies to conduct and publish a fulsome privacy impact assessment (PIA) based on an unwieldy legal framework. Police agencies, and individual officers, may perceive that they have no choice but to take action based on a cursory assessment and then justify and/or apologize for any misuses of FRT after the fact. Inevitably, in this *ad hoc* arrangement, individual rights and democratic freedoms will erode. While the proposed guideline is helpful for the police in understanding appropriate safeguards, it is only an unenforceable set of recommendations which police agencies may or may not put into practice. Police agencies may choose to incorporate all of the OPCC's recommendations or only some of them that buttress their view of appropriate investigation or policing into their internal policies. The OPCC should therefore be clear that any guidelines should be adopted in whole and are not intended to authorize actions which are not otherwise permitted by law.

⁷ <https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785>

15 October 2021

14. The additional danger of trying to force the existing legal framework to apply to the use of FRT by police is that there are many instances in the framework where a consideration of reasonable expectations is required, but as the OPCC stated, “citizens’ reasonable expectations regarding the use of FR are not yet clearly established.”⁸ This is dangerous language that concedes individuals’ privacy rights without evidence. The statement should be rewritten to indicate that there is no evidence that individuals’ reasonable expectations of privacy are abandoned simply because FRT is being deployed without their consent or knowledge. There is a risk that these expectations will be molded by the mere fact that citizens are increasingly exposed to FRT both by the private and public sector, to the point that the citizenry simply concludes that such intrusive practices must already have been made legal. Rather than adopting a “wait and see” approach to where expectations will fall, PIAC submits that it would be more productive and helpful for both the police and citizens to define and set reasonable expectations through a single, prescriptive regulatory framework governing law enforcement’s use of FRT. While the OPCC’s guidance can help prior to that law being promulgated, it is not a substitute for it.

i. Case study: *R v Bridges*

15. The recent 2020 case of *R (on the application of Bridges) v Chief Constable of South Wales Police* (“Bridges”) in the United Kingdom serves as a cautionary tale on the inadequacies of laws of general application in the context of police use of FRT. The Court of Appeal (CoA) found that the use of automated FRT by South Wales Police to screen crowds against watchlists was unlawful and therefore failed to comply with Article 8 of the *European Convention on Human Rights*, that is, the right of respect for private and family life. General laws that apply to police use of FRT do exist in the UK, much like Canada’s own patchwork of laws and policies, but the CoA determined that the existing framework was not specific enough on the appropriate parameters for FRT.

16. First, it bears highlighting that the appellant originally brought a claim for judicial review on the basis that the SWP’s use of automated FRT violated his human right to respect for private life under the ECHR. There is no directly comparable right to privacy in Canadian laws. Rather, for years policymakers have come close to, but have largely avoided formalizing an explicit right to privacy, instead affirming the quasi-constitutional status of privacy legislation, and indirectly tying privacy to the realization of other rights protected under the Charter. Without a human rights foundation, federal privacy laws are only data protection statutes, unlike European privacy laws such as the GDPR, which are rooted in human rights and therefore reach beyond data protection to explicitly require consideration of fundamental rights and freedoms.

17. In *Bridges*, the CoA determined that the relevant laws and policies in the UK gave individual police officers so much discretion that there were virtually no limits on where to use automated FRT, and who could be placed on a watchlist.⁹ Specifically, the CoA examined whether the UK’s legal framework applying to SWP’s uses of automated FRT constituted an interference with

⁸ https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/ at para 53.

⁹ [2020] EWCA Civ 1058, at para 91.

15 October 2021

Article 8(1) of the ECHR “in accordance with the law,” as set out in Article 8(2). The expression, as explained by the European Court of Human Rights, and affirmed by the Divisional Court and CoA, implicates that the law must have a certain “quality.” That is, the law under which the interference occurred must be accessible to the affected person, foreseeable enough that a person is able to act in accordance with that law, and most importantly, clearly indicate the scope of discretion it confers on the competent authorities.¹⁰ Specifically in the surveillance context, the Court of Human Rights has expressed that “the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data.”¹¹

18. On the question of whether the SWP’s exercise of surveillance powers was sufficiently restrained “in accordance with the law,” the CoA determined that it was not. The fundamental deficiencies identified by the CoA relate to excessive police discretion arising from a lack of clear criteria on the “who” and “where” of automated FRT deployment. If the exact challenge in Bridges was brought to courts in Canada, it could be argued that police discretion is circumscribed under the necessity and proportionality tests within privacy laws, the common law, and the Charter. However, this framework for justifying intrusions on privacy is not rooted in an explicit, broad acknowledgement of privacy as a fundamental human right that carries with it the weight of intrinsically linked rights and freedoms like freedom of thought and expression.
19. Additionally, the scope of the Canadian framework is comparable to the one the CoA deemed insufficient for the purposes of regulating police use of FRT. General conditions of necessity and proportionality are set out in the UK’s *Data Protection Act 2018* and the Surveillance Camera Code of Practice, yet the CoA did not find these instruments sufficient on their own to circumscribe police discretion on where and on whom to use FRT. . PIAC submits that, in view of the Bridges case, laws of general application in Canada are not well-equipped, at this time, to regulate police use of FRT in a manner that places sufficient limits on their discretion and gives due consideration to broader impacts on human rights.

II. The appropriate approach to future policy is two-pronged: implementing both a standalone legal framework and broader privacy reforms

20. Given the numerous gaps in the current framework, a dedicated FRT framework must set out procedural and substantive safeguards against both intentional and inadvertent misuses of FRT by police agencies. The framework must also ensure there are no uncertainties as to police agencies’ transparency and accountability obligations when contracting with the private sector for FRT services. The increasing prevalence of public-private partnerships necessarily demands

¹⁰ Ibid, at para 55.

¹¹ https://www.echr.coe.int/documents/guide_art_8_eng.pdf at para 15,

15 October 2021

that public and private sector laws are interoperable and, more importantly, do not provide each other escape routes for privacy obligations.

21. The OPCC hints to the importance of bolstering both sides of the framework. In its Clearview AI report, the OPCC stated that “[w]e 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.”¹² Therefore, on the question of: “Would these changes be better addressed through a standalone regulatory framework specific to FR use, or through reform of privacy laws of general application?” PIAC asserts that **both** are necessary to create a truly privacy-protective framework around police use of FRT.
22. PIAC is encouraged that the RCMP has accepted and has begun to implement the recommendations from the OPCC report on the RCMP’s use of Clearview AI.¹³ PIAC also lauds the RCMP’s National Technologies Onboarding Program (NTOB), which was introduced in March 2021 and will help standardize and track the adoption and use of new and emerging investigative tools involving the collection and use of personal information. However, PIAC also reserves optimism regarding these initiatives, considering that the RCMP agreed to implement the OPCC’s recommendations despite its position that section 4 of the federal *Privacy Act* “does not expressly impose a duty to conclusively confirm the collection authority of a non-governmental third party.”¹⁴ To avoid similar avoidance of accountability in the future, the *Privacy Act* must be amended to clarify that federal institutions, including the RCMP, have an obligation to ensure that the third party agents they collect personal information are compliant with privacy laws.
23. Alternatively, or better yet simultaneously, a standalone legal authority for police use of FRT must explicitly require the police to take accountability for the privacy practices of third party agents who provide FRT services. Appropriate provisions would address contractual transparency, record-keeping requirements, accountability and transparency measures ensuring private sector partners comply with private sector laws, and include restrictions against data-sharing with the private sector partners and other law enforcement agencies (i.e., the CBSA, and the intelligence agencies). Explicit restrictions should also be placed on the admissibility of facial matches obtained through FRT using illegally obtained data.
24. One essential part of PIAs, as the draft guidance explains and as should be codified in legislation, is that police must not proceed with a FRT initiative if they cannot clearly explain:

¹² https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

¹³ <https://www.rcmp-grc.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai>

¹⁴ https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para 30.

15 October 2021

- i. Why the proposed use of FR is necessary to meet a specific need that is rationally connected to a pressing or substantial public goal;
- ii. What the expected benefits of the initiative consist of, and how they are proportionate to the risks involved;
- iii. Why other less intrusive measures are not sufficient;
- iv. How risks will be minimized during implementation of the initiative.

25. PIAC also submits that if documentation on the above is insufficient, FRT legislation should provide that any subsequent charges arising from non-compliant FRT initiatives be dropped, and all facial data collected in the initiative be destroyed. Further, the same consequences should apply where the police failed to adequately assess bias and consider human rights in the planning and implementation of the FRT initiative.

26. PIAC suggests that policy-makers can look to the GDPR, under Articles 35 and 36, as a possible framework for establishing a PIA pre-filing requirement for police use of FRT. That is, Article 35 requires that an impact assessment be conducted prior to the processing of data that is likely to result in a high risk to the rights and freedoms of natural persons, which PIAC submits that FRT more than satisfies. Article 36 then requires that when an impact assessment is conducted under Article 35, the data controller must also consult the supervisory authority prior to the processing. The supervisory authority then has the power to issue advice, correct or even ban the processing operation. In a similar manner, police accountability could be rooted in a requirement for police agencies to conduct impact assessments and consult with the OPCC prior to implementing FRT initiatives. The OPCC would then have knowledge and documentation of the exact intent, scope, and justification for a given FRT initiative, against which the OPCC can assess compliance of future FR activities that rely on this pre-approval process. Although the OPCC cannot require such PIAs be pre-filed with the OPCC for uses of FRT by police agencies, the guidance could promote it as a best practice (which may be of assistance to reviewing courts) while Canada awaits the updating of its law to reflect an appropriate privacy framework for use of FRT.

i. The danger of a prospective Bill C-11 revival

27. Currently, the *Privacy Act*, which applies to the federal government institutions like the RCMP, prohibits government institutions from collecting personal information from a third party agent if that third party agent collected the information unlawfully – this was confirmed by the OPCC in its review of the Clearview AI case.¹⁵ However, Bill C-11, which died on the Order Paper prior to the 2021 federal election but will likely be revived in the near future, will make it much easier for those third party agents to collect more personal information under much broader consent exemptions.

28. Overall, PIAC submits that Bill C-11 sets a preference for commercial interests over human rights and individual privacy interests, that privacy obligations must inevitably evolve based on

¹⁵ https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

15 October 2021

commercial needs. For example, the bill expands consent exemptions for “business operations,” especially in section 18(2)(e), which allows collection and use without individual’s knowledge or consent if it is for “an activity in the course of which obtaining the individual’s consent would be impracticable because the organization does not have a direct relationship with the individual.” Some protection is carried over from PIPEDA in section 12 of the Bill, which limits s 18 collection “only for purposes that a reasonable person would consider appropriate in the circumstances.” However, the fenceposts around what is “appropriate” may be in flux under the influence of the private sector.

29. Overall, the consent exemptions under section 18(2) are very broad, and could potentially be interpreted to increase opportunities for companies to collect facial recognition data without individuals’ knowledge or consent, to “prevent or reduce the organization’s commercial risk” (s 18(2)(b)), for “activity that is necessary for the organization’s information, system or network security” (s 18(2)(c)), for “an activity that is necessary for the safety of a project or service that the organization provides or delivers” (s 18(2)(d)). All of these circumstances could conceivably justify the collection, use, or disclosure of facial identification data, to protect the company from fraud, liability, or security risks, or to ensure that more personalized, specialized services and products are targeted to specific demographics or individuals.

30. In Bill C-11, and also within broader discourse on privacy reforms, de-identification is becoming an increasingly attractive tool for enabling enhanced use of broader swathes of personal data while minimizing the need to obtain individual consent. Perhaps counter-intuitively, facial images could also be subject to de-identification, which under the Bill allows for a cascade of activities without individual consent or knowledge. There are already emerging techniques that can apparently render facial images unidentifiable to FRT while still retaining basic but useful biometric details.¹⁶ However, PIAC submits that rendering facial images to its most basic features while removing further identifying factors holds great potential for perpetuating bias, especially when training AI algorithms. Such bias seeping into the law enforcement context can be extremely harmful.

31. PIAC submits that, given the inadequacies of the current legal framework, and ongoing uncertainty around private sector privacy reforms, it may be wise to impose a moratorium on police use of FRT until a specific, enforceable legal framework is in place and private sector reforms are resolved in manner that adequately protects individual privacy rights.

¹⁶ Elaborate in footnote: <http://latanyasweeney.org/work/face.html> ;

https://www.nist.gov/system/files/documents/2020/08/06/09_tuesday_shenoy_arunashenoy_ibpc2014.pdf ;

<https://hal.archives-ouvertes.fr/hal-01187654/document> ;

<https://medium.com/@kenrobbins/call-for-image-de-identification-standards-6b33e6576a12>

CONCLUSION

32. Facial recognition technology in the hands of law enforcement can greatly enhance public safety and criminal investigations, but without proper limitations under a specialized legal framework, police use of FRT is more likely to be incompatible with individual privacy rights and a free and democratic society. Though PIAC lauds the draft guidance as a detailed overview of the general legal framework, at most the guidance is a set of aspirational, but not enforceable, set of recommendations. For police agencies that are truly and publicly committed to improving their internal FRT policies, the guidance is a useful model, but for others, it is inconsequential.
33. PIAC submits that the potential negative impacts of FRT merit a specific, enforceable statutory authority setting out criteria for how, why, when, where and on whom police agencies may use FRT. Laws of general application, though technologically neutral, do not adequately protect individual privacy rights in the context of FRT. This was the crux of the UK Bridges case, which determined that a legal framework conferring wide areas of discretion to the police is not appropriate for the use of FRT, particularly in mass surveillance contexts.
34. Furthermore, private sector privacy laws face imminent reform, likely towards more permissive consent exemptions based on the now dormant Bill C-11. Until broader policy reforms are finalized and adequately protective of privacy rights, law enforcement is essentially free to operate within a framework that allows wide discretion, lacks real scrutiny of and consequences for FRT misuse, and enables police agencies to neglect public sector privacy obligations through public-private partnerships.

***** END OF DOCUMENT *****