Now You See Me?

Advancing Data Protection and Privacy for Police Use of Facial Recognition in Canada

Yuan Stevens | October 2021

cybersecure
policy
exchange

Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

Table of Contents

Executive Summary

Law enforcement in Canada is increasingly turning to facial recognition in hopes of augmenting their investigative powers. Facial recognition is the process of identifying a person or verifying their identity on the basis of facial data and patterns.[1]

There are numerous accuracy challenges associated with facial recognition technology that can exacerbate historical prejudices and stereotypes, especially when deployed at large scale. Studies demonstrate that facial recognition algorithms discriminate against elderly people, children, women, racialized people, as well as the LGBTQ2S+ community.[2] Overconfidence in the technology can lead to serious, and at times devastating, consequences for marginalized individuals.

The technology also threatens the right to anonymity, privacy, and substantive equality.[3] The police can use facial recognition to arrest someone after an alleged crime has occurred by comparing images with a watchlist or general image database. They can also conduct the same comparisons in a live setting for example through CCTV cameras, tracking people's locations and movement in real time without the knowledge or consent of those being surveilled. In either case, facial recognition poses significant threats to privacy, fundamental freedoms, and other human rights.

It is in this context that the RCMP decided to use the services of data scraping and facial recognition company Clearview AI on a trial basis, ultimately leading Canada's federal, provincial and territorial privacy protection authorities to jointly develop guidance for police agencies across Canada on facial recognition.[4] The guidance document outlines the current state of the law in Canada regarding police use of facial recognition and encourages best practices around privacy impact assessments, accuracy, data minimization, purpose limitation, data security, retention, openness and transparency, individual access, and accountability.

We welcome the opportunity to provide feedback on this guidance document. The only commentary we provide on the guidance itself is the encouragement to consider recommending that law enforcement use decentralized, rather than centralized, databases in order to reduce the risk of the systems being compromised or repurposed as explained by privacy and human rights expert Tamir Israel — whose work examining the legal aspects of facial recognition is foundational in the Canadian context.[5] The remainder of our feedback takes the form of comparative analysis of the treatment of facial recognition in other jurisdictions and recommendations for advancing Canada's privacy legal framework to address law enforcement's use of facial recognition technology.

Given the substantial risks posed by this technology, facial recognition systems should not be adopted at this time and the proportionality of current systems in use by law enforcement should be reassessed and reexamined.[6] However, adoption of any facial recognition system for identification requires a dedicated legislative framework that prohibits the use of the technology in the absence of explicit lawful authority[7] and that enables the Office of the Privacy Commissioner of Canada (OPC) to provide oversight of these systems through robust requirements, such as ongoing privacy and algorithmic impact assessments that are made available to the public.[8]

Comparing Legal Approaches to Law Enforcement and Facial Recognition

In numerous jurisdictions, detailed legislative regimes are in place for facial recognition, including its use by law enforcement. Legislation addressing facial recognition can involve data protection and privacy rights more broadly as it occurs in the EU, with a focus on the special protection afforded to biometric data as well as rights and obligations in the context of the automated processing of data. Laws can also focus on privacy rights for biometrics and biometric identifiers, as is the case in Illinois. Legislation can also be tailored to specifically address police use of facial recognition, which is the approach taken by lawmakers in Massachusetts. In comparison to these approaches and jurisdictions, Canada is falling behind by failing to regulate law enforcement's use of facial recognition and in an enforceable manner.

European Union: The GDPR, the LED, and DPIAs

There has been significant interest in addressing the risks of facial recognition in the European context. Outside of the current existing legal regime, two independent EU-run bodies responsible for supervising and shaping the protection of data and privacy across the EU issued a call for a ban in June 2021 on the use of AI for automated recognition of human features in publicly accessible spaces, including the recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals.[9] This came on the heels of a risk-based proposal for regulating high-risk uses of artificial intelligence in April 2021, including some restrictions on law enforcement's use of biometric surveillance in public places but with numerous wide-ranging exceptions.[10]

In response to this, members of European Parliament voted in support of a ban on the use of facial recognition by law enforcement and judicial authorities in October 2021, including a ban on predictive policing based on behavioural data.[11] Danish liberal deputy Karen Melchior said during parliamentary debates that “predictive profiling, AI risk assessment and automated decision-making systems are weapons of 'math destruction'”,[12] because they are “as dangerous to our democracy as nuclear bombs are for living creatures and life.”[13] The proposed law would also forbid use of private facial recognition systems, including the database provided by Clearview AI.

The GDPR and the Law Enforcement Directive

In terms of the current legislative framework, EU member states must enforce the requirements set out by the General Data Protection Regulation (GDPR) as well as the Law Enforcement Directive (LED). While the GDPR does not apply to law enforcement that engages in the prevention, investigation, or detection of criminal offences,[14] the GDPR nonetheless generally applies to the public and private sectors more broadly and is applicable to entities that provide facial recognition technology. This matters because law enforcement agencies may procure the services of private actors which provide automated facial recognition software, which are otherwise subject to the GDPR.

The GDPR sets out enforceable principles and provides rights of data subjects (individuals whose data is collected and processed). In the context of automated facial recognition, Article 9 is particularly important. Among other types of data, it prohibits the processing of biometric data — including facial images — subject to certain exceptions.[15] The European Court of Human Rights (ECtHR) has solidified that facial images are a form of sensitive, biometric data.[16] While few if any ECtHR decisions have thus far involved analysis of automated facial recognition in particular, the data scraping and automated facial recognition activities of companies like Clearview AI could be captured by the prohibition found in Article 9 of the GDPR.[17] This invariably sets limits on the ability for a law enforcement agency to use the services of Clearview AI, given the potential violation of these data protection and privacy rights under the GDPR by a private actor.

A private company providing facial recognition services could also be found subject to obligations related to automated decision-making (ADM). For example, rights holders under the GPDR have the right not to be subject to a decision that is based solely on automated processing, including profiling, which produce legal effects concerning them as an individual or that similarly affects them as an individual.[18] ‘Profiling’ refers to predictive analysis concerning a person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.[19]

Some exceptions exist to the right not to be subject slowly to ADM or profiling, related to contractual agreements, legal authorization, and explicit consent — but safeguards are still required.[20] If a company falls under one of these exceptions, they could subject a person to a decision based solely on automated processing — or profile them — even if it affects their legal rights, but only when authorized by law or when measures are in place that provide suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[21] If the use of automated processing is necessary either for entering into or the performance of a contract or based on the individual's consent, then the entity processing the data (e.g., the facial recognition company) must provide the individual the right to obtain human intervention and to contest the decision.[22]

Recital 71 of the GDPR also requires that companies prevent "discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation" in the context of ADM and profiling.[23] Companies are encouraged to examine datasets for bias, review the accuracy and relevance of decisions on a regular basis, deploy systems that audit ADM software, and introduce appropriate procedures and measures to prevent errors, inaccuracies, or discrimination on the basis of special category data on a cyclical basis.[24]

The GDPR provides numerous other rights to individuals in the context of ADM, which are applicable in the context of automated facial recognition. For example, individuals have the right to be notified when automated decision-making is in use by any entity that processes their data, including when the entity engages in profiling.[25] Individuals also have the right to receive meaningful information about the logic involved in the automated processing, as well as the significance and envisaged consequences of such processing for the data subject.[26] An institution would therefore be required under the GDPR to provide such access and recourse to individuals whenever a person's facial image is processed in an automated fashion for recognition, classification or identification.

Member states are also required to enact legislation that meets the minimum requirements for law enforcement set out in the Law Enforcement Directive. The LED provides similar rights to individuals as provided by the GDPR when it comes to the processing of special categories of personal data and automated decision-making.

More specifically, law enforcement subject to the LED can process biometric data for identification purposes only when doing so is "strictly necessary" and appropriately safeguards rights and freedoms of the data subject, and only when:

- Doing so is authorized by EU or member state law;
- In order to protect the vital interests of the data subject or another natural person; or
- Where such processing relates to data which are manifestly made public by the data subject.[27]

Parallel to Article 22 of the GDPR, the LED requires member states to prohibit decisions by law enforcement based solely on ADM, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects them.[28] Similarly to Article 22, decisions based solely on ADM and profiling may be allowed when doing so is allowed under EU or member state law and the law provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.[29] Nonetheless, no law enforcement decisions based solely on ADM, including profiling, can be based on special categories of data (including biometric data), unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.[30]

Unlike Canada's *Privacy Act* or *PIPEDA*, the LED explicitly redresses the possibility of profiling through the use of automated decision-making that results in discrimination.[31] Article 11 of the LED prohibits profiling that results in discrimination on the basis of the special categories of data referred to in Article 10, including on the basis of biometric data and therefore facial images.

Data Protection Impact Assessments under the GDPR

Data Protection Impact Assessments (DPIAs) are an important concept to the GPDR that can be used to provide another layer of regulatory protection or limitation in the context of facial recognition. In-depth analyses of DPIAs have been conducted by various experts, including privacy and data protection experts Margot Kaminski and Gianclaudio Malgieri[32] as well as researchers at Data & Society Research Institute.[33] For Kaminski and Malgieri, DPIAs generally serve the dual roles as a tool within the GDPR's systemic (and collaborative) governance regime, as well as an element in the protection of individual rights.[34] In the context of collaborative governance of automated decision-making, DPIAs are a form of monitored self-regulation.[35] They task companies with identifying problems and implementing solutions to those problems, with largely internal oversight and some external input, "under a threat of regulatory oversight but ordinarily minimal regulatory supervision."[36]

The Article 29 Working Party Guidelines interpret the GDPR as mandating DPIAs for all ADM with significant effects.[37] DPIAs must occur before a company implements a system; that is, a company must assess a system and propose risk-mitigation measures, before data processing takes place.[38] Companies also ought to assess whether they are complying with their own DPIA when the risk posed by a system changes.[39]

DPIAs must include:

- A description of the '**processing operations**' (in this case, the ADM's algorithms in question) and the purpose of the processing;
- An assessment of the **necessity** of processing in relation to the purpose;
- An assessment of the **risks** to individual rights and freedoms; and
- Importantly, the **measures** a company will use to address these risks and demonstrate GDPR compliance, including security measures.[40]

The GDPR requires consultation "where appropriate" with impacted individuals, but does not require formal stakeholder consultation with the public or experts.[41] Unlike many impact assessment proposals in existence (including for the environment, human rights, privacy, and surveillance), the GDPR does not require DPIAs to be released to the public even when finalized.[42] This is despite the fact research indicates that public access to impact assessments is a critical element facilitating trust in such a consultative process, and that the "broader the access to its impact statement, the stronger is an impact assessment's potential to enact changes in system design, deployment, and operation."[43]

Illinois: The *Biometric Information Privacy Act*

The *Biometric Information Privacy Act* (BIPA) in Illinois was enacted in 2008 and is possibly one of the strongest laws recently passed in the North American context that protects biometric information used by the private sector.[44] Similar to the GDPR, Illinois' BIPA is relevant in the context of police use of automated facial recognition when private companies are relied on to provide such services to law enforcement.

At the outset, the law's states that unlike other unique identifiers (e.g., social security numbers), biometrics are "biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[45] It also states that "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."

BIPA prohibits companies from collecting biometric information unless they a) inform the person in writing what data is being collected and stored along with the specific purpose and length of time for the collection, storage or use and b) obtain the person's written consent.

The law also provides a very detailed and narrow definition of "biometric identifier," defined as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.[46] Notably, BIPA's definition of biometric identifier excludes photographs and physical descriptions such as height, weight, hair colour and eye colour. "Biometric information" under BIPA means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[47]

The law requires companies that possess biometric identifiers or information to do following things:

- Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied, or within three years of the individual's last interaction with the private entity, whichever occurs first;

- Not sell, lease, trade or otherwise profit from such identifiers or information;

- Not disclose or otherwise disseminate such information unless the subject of the identifier or information consents, the disclosure or redisclosure completes a financial transaction requested or authorized by the subject or the disclosure or redisclosure is required by law, valid warrant or subpoena;

- Store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry and in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.[48]

Individuals can seek damages for BIPA violations, including up to $1,000 for negligent actions and up to $5,000 for intentional or reckless violation of the law.[49]

Claims and class actions have been initiated under BIPA in the context of facial recognition technology. In early 2020, Facebook agreed to pay $550 million USD to settle a class action over collecting facial recognition data on images of people in Illinois without disclosure,[50] which was ultimately raised to $650 million in 2021.[51] Both Amazon and Microsoft are also facing class actions regarding their use of a database comprised of Flickr images in order to improve the accuracy of their facial recognition software without the consent of those featured in the images.[52]

Massachusetts: An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth

The state of Massachusetts has enacted law in the wake of the tragic murder of George Floyd that seeks to strengthen accountability for law enforcement agencies wishing to use facial recognition. The *Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth* (the Act) has been in force as of December 31, 2020.[53]

The Act requires law enforcement to obtain a warrant before conducting a facial recognition search, except in emergency situations.[54] Police in Massachusetts are also prohibited from acquiring, accessing, or using facial recognition software themselves as well as making a request or entering into a contract to do so.[55] After seeking a warrant to run a facial recognition search, the police must submit a written request to have someone from the state police, the FBI, or the Registry of Motor Vehicles perform the search.[56] Law enforcement may only submit such a written request without a warrant if the agency "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any individual or group of people requires the performance of a facial recognition search without delay."[57]

Law enforcement agencies must document each facial recognition search performed. They must provide this documentation on a quarterly basis to the Executive Office of Public Safety and Security. Documentation must include a copy of the written request, the date and time of the request, number of matches returned, databases searched, name of the requesting individual and agency, reason for the request (including any underlying suspected crime), the entity to which the request was submitted, and data detailing the individual characteristics included in the facial recognition request.[58]

The Executive Office of Public Safety and Security will then, on annual basis, publish information such as the total number of searches performed by each law enforcement agency and the total number of searches performed by the state police and by the FBI broken down by each law enforcement agency's requests.[59] The Registry of Motor Vehicles also has detailed documentation requirements, which must be made available to the public.[60]

The Act also establishes a special legislative commission to study the use of facial recognition by the Massachusetts Department of Transportation.[61] The commission will undertake numerous tasks, including (but not limited to): evaluating the facial recognition system operated by the registry of motor vehicles; proposing standards to ensure the system's accuracy and equity in light of age, race, gender and religion; identifying which federal agencies have access to databases comprised of faces and the terms of authorization of such access; providing recommendations to ensure procedural fairness when facial recognition technology is used in any part of an investigation; providing recommendations for adequate training and oversight on the use of facial recognition technology.[62] The commission is required to submit its findings and recommendations to the Massachusetts house of representatives and senate by December 31, 2021.

Changes to Canada's Legal Framework

The Need for a Dedicated Legislative Framework

In response to the Office of the Privacy Commissioner of Canada's question of whether police use of facial recognition is appropriately regulated in Canada under existing law, **the answer is no**. In its guidance, Canada's privacy protection authorities clearly state that no laws in Canada specifically address the risks posed by facial recognition, resulting in a legal vacuum and uncertainty "concerning what uses of [the technology] may be acceptable, and under what circumstances."[63] Work by privacy law expert Teresa Scassa also demonstrates that public sector privacy laws "were not written for our emerging context in which government institutions increasingly rely on data analytics and data-fueled AI services provided by the private sector."[64]

Facial recognition systems are increasingly recognized as posing unacceptable risks to marginalized communities and as an intrusive form of surveillance involving highly sensitive information.[65] There is also risk that facial recognition information and capabilities will be repurposed and expanded outside of current uses, which challenges the legitimacy and desirability of building enormous government databases given the tangible risk of increased surveillance associated with this information.[66] Finally, the biologically unique nature of facial information makes the potential for ongoing harm in the event of a breach of misuse extremely high. A legal framework is needed that addresses these risks in Canada in the law enforcement context.

The EU, Illinois and Massachusetts involve dedicated legal frameworks (whether currently in place or proposed) to establish safeguards and limitations on the use of facial recognition, which is needed in Canada. Even in the EU context, where the data protection and privacy legislation has been heralded as some of the strongest in the world,[67] a law that specifically addresses police use of artificial intelligence including facial recognition will be implemented.[68] **A dedicated legal framework that sets out permissible uses of facial recognition and provides safeguards and limitations regarding its use would similarly be warranted in Canada**. This is in line with our recommendation that the use of facial recognition for identification should be prohibited in the absence of explicit lawful authority.

Options for Lawful Authority

Without being exhaustive or providing recommendations on which of the following should be implemented, options for such lawful authority include:

- Canada could follow the 30 recommendations on government, police, and private use of facial recognition put together by the Georgetown Law Center on Privacy & Technology, including implementing a version of the Model Face Recognition Act that is tailored to the Canadian context.[69] The recommendations include the threshold that should be met for law enforcement to conduct searches on facial recognition databases, which databases can be searched and how, who must be omitted from mugshot database searches, when real-time or live facial surveillance can occur, public reporting and auditing requirements, accuracy and bias testing, procurement requirements, and numerous other best practices.

- Law enforcement could be required to obtain a warrant to conduct a facial recognition search for serious crimes only. This would require legislative amendments to the *Criminal Code* in line with s. 487.04 that concern forensic DNA analysis, which limits the production of such warrants only for certain serious crimes (and upon provision of certain information by police that justifies receiving the warrant) that assess the necessity, effectiveness and proportionality of the proposed use of information in light of *Charter* rights.[70] However, experts at the Georgetown Law Center on Privacy & Technology observe that a simple warrant is not enough for pervasive, real-time facial surveillance through CCTV, and that, at minimum, a warrant with more onerous procedural and substantive requirements related to life-threatening public emergencies would be needed in that context.[71]

- Law enforcement could be prohibited from using the facial recognition services of third parties and could be allowed only to use such facial recognition through ministries of transportation by obtaining a warrant or in life-threatening public emergency situations, and with publicly available documentation requirements like those required in Massachusetts. This would help to mitigate the risks associate with police use of third-party services (as was the case with the RCMP and Clearview AI) and would help to address the legal grey zone that currently permits police to access driver's licence databases and passport photos with little to no oversight or accountability in Canada.[72] In line with recommendations again by experts at the Georgetown Center on Privacy and Technology, searches conducted on driver's licence and other ID databases should, at minimum, require probable cause and should also be limited for the most serious crimes.[73]

The legislative framework for facial recognition in Canada could draw on our recommendations for the *Privacy Act*, where we advocated for limitations on the collection, use and disclosure of facial information, minimization of the information that is collected, adequate employee training, human involvement in high impact decisions, meaningful explanations to affected individuals of the reason for certain automated recommendations, and security safeguard and notification requirements.[74]

The framework could also be informed by the recommendations provided by Tamir Israel, who advocated for decentralized facial recognition reference datasets to reduce the risks that facial recognition systems will be compromised or repurposed at a systemic level, as well as for:

- Deletion as soon as possible of images or live recordings;
- The introduction of image quality assurance mechanisms;
- The limited benefits of keeping humans in the loop for final decisions;
- Rigorous pre-emptive and ongoing proportionality and impact assessments that are also rigorously transparent;
- Limitations on when facial identification is permitted and the repurposing of facial recognition systems;
- Minimum accuracy and bias thresholds; and
- Ongoing obligations for disparate impacts and errors.[75]

On top of these recommendations, the legislative framework should also provide recourse to individuals regarding use of facial recognition as an example of an automated decision-making system. Drawing on the GDPR for inspiration, individuals should explicitly be afforded:

- The **right to meaningful explanation** of how and why the automated decision was made;
- The **right to human intervention** or final decision-making prior to arrest or detainment on the basis of a recommendation provided by a facial recognition system; and
- The **right to freedom from discrimination** based the grounds for discrimination referred to in s. 15 of the *Charter*.

Rigorous Impact Assessments and Public Transparency Facilitated by the OPC

This legislative framework should require that law enforcement conduct rigorous proportionality and impact assessments before and during any use of facial recognition systems.[76] The Office of the Privacy Commissioner is in the best position to provide oversight of the assessment process and the oversight of facial recognition systems more generally.[77]

Drawing on the GDPR, these assessments could include at minimum:

- A description of the how the systems and algorithms operate and the purpose for the collection and use;
- The necessity of the collection and use in relation to the purpose;
- An assessment of the risks to individual rights and freedoms; and
- The measures used to demonstrate privacy, data protection, and security compliance.[78]

Impact assessments for privacy and automated decision-making are already separate requirements in Canada,[79] but a cohesive approach to impact assessments for facial recognition would be beneficial given the interconnected nature of the privacy and algorithmic accountability issues raised by the technology.

It would be useful to incorporate the best practices laid out by Algorithm Watch in the organization’s work on impact assessments for automated decision-making systems in the public sector.[80] The authors provide a comprehensive framework and checklist focused on seven values for conducting impact assessments, including four principles based on respect for human autonomy, prevention of harm, impartiality or fairness, and benefits that outweigh harms, as well as three instrumental principles based on control, transparency, and accountability. Where a system assessed poses particular risk, a detailed “transparency report” would be needed because the system would be subject to additional transparency requirements.

One compelling solution proposed by the research and advocacy organization Algorithm Watch is the recommendation that governments provide a public registry showing all automated decision-making systems used in the public sector.[81] The registry would ideally provide information contained within the impact assessment, as well as the name of the developers of the system. Where there are legitimate reasons for restricting access to the transparency report, information should be provided to the appropriate oversight institution (such as the OPC), which should in turn be communicated to the public.[82]

A public registry for algorithms, tools and systems powered by data is already in place in Ontario.[83] Municipalities in Europe such as Amsterdam, Helsinki and various cities in France have also begun providing public registries for deployment of artificial intelligence and as a way for citizens to provide feedback on the algorithms used.[84] Such transparency is not in and of itself an adequate solution to many of the issues posed by technology such as facial recognition systems, but it helps to create conditions in which compliance with legal requirements can be assessed and accountability is more achievable.

References

[1] Stevens, Y., & Solomun, S. (17 February 2021). *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act*. Cybersecure Policy Exchange. https://www.cybersecurepolicy.ca/frt-privacy-act.

[2] Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Conference on Fairness, Accountability and Transparency. https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf; Bushwick, S. (2019, December 27). *How NIST Tested Facial Recognition Algorithms for Racial Bias*. The Scientific American. https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/; European Parliament Committee on Civil Liberties, Justice and Home Affairs (2021). *Report on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters*. European Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf.

[3] Robertson,. K., Khoo, C., & Song, Y. (September 2021). *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*. Citizen Lab. https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf.

[4] Office of the Privacy Commissioner. (2021). *Draft privacy guidance on facial recognition for police agencies*. Office of the Privacy Commissioner. https://priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/.

[5] Israel, T. (15 December 2020). *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond*. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC). https://cippic.ca/en/news/facial_recognition_transforming_our_borders, pp. 6-11.

[6] Ibid, pp. 162-163.

[7] Stevens & Solomun. *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act.*

[8] Israel, T. *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond.*

[9] European Data Protection Board. (21 June 2021). *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*. European Data Protection Board. https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

[10] Lomas, N. (21 April 2021). *Europe lays out plan for risk-based AI rules to boost trust and uptake*. TechCrunch. https://techcrunch.com/2021/04/21/europe-lays-out-plan-for-risk-based-ai-rules-to-boost-trust-and-uptake/.

[11] European Parliament. (6 October 2021). *Use of artificial intelligence by the police: MEPs oppose mass surveillance*. European Parliament News. https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.

[12] O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing. https://crownpublishing.com/archives/news/weapons-math-destruction-cathy-oneil.

[13] Rogal, A. (6 October 2021). *MEPs back ban on AI-driven mass and indiscriminate surveillance*. The Parliament Magazine. https://www.theparliamentmagazine.eu/news/article/meps-back-ban-on-aidriven-mass-and-indiscriminate-surveillance.

[14] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Article 2(2.d).

[15] GDPR, Article 9. Article 4 of the GDPR defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.' Exceptions to the prohibition on processing special categories of data generally include when the individual involved has given consent; when the processing is necessary for the enforcement of employment, social security, and social protection obligations; when the individual is unable to provide consent but processing is necessary to protect vital interests; for legitimate activities of foundations, associations, or non-profits with a political, philosophical, religious or trade union aim subject to certain requirements; the individual has "manifestly made public" their personal data; in the context of judicial proceedings; when member states allows the processing for substantial public interest so long as certain requirements are met; in the context of providing healthcare and public health so long as certain requirements are met; in the context of archiving data for public interest, scientific, historical research, or statistical purposes with certain requirements.

[16] Dushi, D. (2020). *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*. Global Campus of Human Rights. https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1625/1.GlobalCampus2020_SouthEast_Europe.pdf, citing these two cases: Case C-291/12 *M Schwarz v Stadt Bochum* [2013] 22, 48-49; *Szabó and Vissy v Hungary App* no 37138/14 (ECtHR, 12 January 2016) 56

[17] Another consideration is that while one of the exceptions to the prohibition on processing of biometric data is when the data has been manifestly made public by the subject, the GDPR also requires that the subject be informed at the time the data is collected.

[18] GDPR, Article 22(1).

[19] GDPR, Article 4(4).

[20] GDPR, Article 22.

[21] *Ibid.*

[22] GDPR, Article 22(4).

[23] GDPR, Recital 71.

[24] *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01). https://ec.europa.eu/newsroom/article29/items/612053/en.

[25] GDPR, Articles 13(f), 14(g), 15(h).

[26] *Ibid.*

[27] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), Article 10. https://eur-lex.europa.eu/eli/dir/2016/680/oj.

[28] Law Enforcement Directive, Article 11.

[29] *Ibid.*

[30] *Ibid.*

[31] *Ibid.*

[32] Kaminski, M., & Malgieri, G. (2020). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. *International Data Privacy Law*, 11(6), 125-144. https://academic.oup.com/idpl/article/11/2/125/6024963.

[33] Moss, E., Watkins, E.A., Singh, R., Elish, M.C., & Metcalf., C. (29 June 2021). *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest.* Data & Society Research Institute. https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/

[34] Kaminski, M., & Malgieri, G. Algorithmic impact assessments under the GDPR: producing multi-layered explanations.

[35] *Ibid.*

[36] *Ibid.*

[37] *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation*. Article 35(3)(a) of the GDPR requires a DPIA for 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing… on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.'

[38] GDPR, Article 35(1).

[39] *Ibid.*

[40] GDPR, Article 35(7), Recitals 84 & 90.

[41] Article Article 35(9). The GDPR also require consultation with internal but independent data protection officers if they are in place.

[42] Kaminski, M., & Malgieri, G. Algorithmic impact assessments under the GDPR: producing multi-layered explanations.

[43] Moss, E., Watkins, E.A., Singh, R., Elish, M.C., & Metcalf., C. *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest*, p. 10.

[44] (740 ILCS 14/) *Biometric Information Privacy Act* (BIPA). https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[45] *Ibid*, section 5

[46] *Ibid,* section 10.

[47] *Ibid.*

[48] *Ibid,* section 15.

[49] *Ibid,* section 20.

[50] Coldewey, D. (29 January 2020). *Facebook will pay $550 millino to settle class action lawsuit over privacy violations*. TechCrunch. https://techcrunch.com/2020/01/29/facebook-will-pay-550-million-to-settle-class-action-lawsuit-over-privacy-violations/.

[51] Bryant, J. (5 March 2021). *Facebook's $650M BIPA settlement 'a make-or-break moment'*. IAPP News. https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/.

[52] Long, A. (20 April 2021). *Amazon and Microsoft team up to defend against facial recognition lawsuits*. The Seattle Times. https://www.seattletimes.com/business/technology/facial-recognition-lawsuits-against-amazon-and-microsoft-can-proceed-judge-rules/.

[53] *An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. 2019 MA S2963. https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253.

[54] Office of Governor Charlie Baker and Lt. Governor Karyn Polito. (31 December 2020). *Governor Baker Signs Police Reform Legislation.* Mass.gov. https://www.mass.gov/news/governor-baker-signs-police-reform-legislation.

[55] Massachusetts Police Association. (n.d.). *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. Massachusetts Police Association. https://masspolice.com/wp-content/uploads/2020/07/legislativesummary.pdf.

[56] *An Act relative to justice, equity and accountability in law enforcement in the Commonwealth,* section 26.

[57] *Ibid,* section 26(b).

[58] *Ibid,* section 26(c).

[59] *Ibid,* section 26(d).

[60] Massachusetts Police Association. *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*.

[61] *Ibid,* section 105.

[62] *Ibid.*

[63] Office of the Privacy Commissioner. *Draft privacy guidance on facial recognition for police agencies*, para 14. Canada's privacy laws have also long ignored the human rights impacts of new surveillance technologies. See: Steeves, V., (2015). Now You See Me: Privacy, Technology, and Autonomy in the Digital Age. In G.D. Editor, *Current Issues and Controversies in Human Rights* (pp.1-31) University of Toronto Press.

[64] Scassa, T. (2 March 2020). *Privacy investigations into Clearview AI in Canada: Old laws and new tech*. Teresa Scassa. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=321:privacy-investigations-into-clearview-ai-in-canada-old-laws-and-new-tech&Itemid=80.

[65] Israel, T. *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond.*

[66] Goldenfein, F. (27 January 2020). *Facial Recognition is Only the Beginning*. Public Books. https://www.publicbooks.org/facial-recognition-is-only-the-beginning/.

[67] Satariano, A. (24 May 2018). *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*. The New York Times. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

[68] European Parliament. *Use of artificial intelligence by the police: MEPs oppose mass surveillance.*

[69] Garvie, C., Bedoya, A., & Frankle, J. (18 October 2016). *The Perpetual Line-up: Unregulated Police Face Recognition in America*. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/recommendations.

[70] *Criminal Code,* RSC 1985, c C-46, s. 487.04.

[71] Garvie, C., Bedoya, A., & Frankle, J. *The Perpetual Line-up: Unregulated Police Face Recognition in America*. See also warrants for intercepting communications, *Criminal Code*, s. 184.2(3).

[72] See for example, *R. v. Voong*, 2018 ONCJ 352; *R. v. Voong*, 2018 ONCJ 353; *R. v. Baldovi et al*, 2016 MBQB 221.

[73] Garvie, C., Bedoya, A., & Frankle, J. *The Perpetual Line-up: Unregulated Police Face Recognition in America*, Recommendation 4.

[74] Stevens, Y., & Solomun, S. *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act.*

[75] Israel, T. *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond.*

[76] *Ibid*. Proportionality is an aspect of the determination of whether a limitation on a person's rights under the *Charter of Rights and Freedoms* is reasonable, see: *R v Oakes*, [1986] 1 SCR 103.

[77] *Ibid*, p. 162.

[78] GDPR, Article 35(7), Recitals 84 & 90.

[79] *Directive on Privacy Impact Assessment*. (18 June 2020). Treasury Board Secretariat. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308; *Directive on Automated Decision-Making*. (1 April 2021). Treasurby Board Secretariat. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

[80] Loi, M., Mätzener, A., Müller, A., & Spielkamp, M. (2021). *Automated Decision-Making Systems in the Public Sector: An Impact Assessment Tool for Public Authorities*. Algorithm Watch. https://algorithmwatch.org/en/wp-content/uploads/2021/06/ADMS-in-the-Public-Sector-Impact-Assessment-Tool-AlgorithmWatch-June-2021.pdf.

[81] *Ibid*, pp. 2, 5, 24.

[82] *Ibid*, pp. 2, 23.

[83] Artificial Intelligence and Algorithms. (n.d.) Government of Ontario. https://data.ontario.ca/group/artificial-intelligence-and-algorithms.

[84] Ada Lovelace Institute, AI Now Institute and Open Government Partnership. (2021). *Algorithmic Accountability for the Public Sector*. Ada Lovelace Institute, AI Now Institute and Open Government Partnership. https://www.opengovpartnership.org/documents/algorithmic-accountability-public-sector/, p. 19.