**Submission to the House of Commons Standing Committee
on Access to Information, Privacy and Ethics**

Study on the Use and Impact of Facial Recognition Technology
June 1, 2022

Summary

Technological advances and access to new and larger personal datasets have lowered the costs and increased the public and private adoption of facial recognition technology (FRT). Our research and work by other human rights advocates point to privacy and ethical concerns raised by FRT that, if unchecked, would violate the rights and freedoms Canadians enjoy. The Government of Canada must lead the country forward in determining acceptable uses — if any — of FRT by public and private institutions to ensure that Canadians' fundamental basic human rights are protected.

This briefing summarizes our research and recommendations for the federal government:

- We echo the call from Canada's federal, provincial, and territorial Privacy Commissioners for a regulatory framework concerning uses, prohibitions, oversight, and privacy of FRT for police forces — but add that such a framework is necessary for the federal and provincial public sectors as well as across the private sector.[1]
- Domestic and international experts have raised significant concerns regarding the discriminatory impacts of FRT on women, elderly people, and people of colour,[2] as well as the intrusive and chilling effects of FRT when it comes to the rights to privacy, freedom of expression, and freedom of assembly.[3]
- We recommend that federal privacy laws, including the *Privacy Act* and PIPEDA, be amended to provide special protection for biometric information such as facial images.
- In particular, we advocate for a permanent limitation in federal privacy laws on the collection, use, and disclosure of biometric information such as facial images for the purpose of uniquely identifying individuals through algorithmic systems. At the very least, notice and either consent or explicit legislative permission should be required.
- We also urge the government to adopt a temporary moratorium on FRT use by the public sector until such legal protections are in place and until more research is conducted on the disproportionate impacts of FRT on communities who stand to be most affected by its use such as elderly people, children, racialized communities, people with disabilities, and transgender and non-binary people. Please see the section below entitled '**An Interim Solution: A Public Moratorium on FRT**' for the research that needs to be undertaken.

Types of Facial Recognition Technology Systems and Associated Risks with Other Biometric Technologies

Faces are a type of personal information related to one's body that is completely unique to each person. Faces can reveal intimate information such as health, perceived gender, race or ethnicity, emotional states, and a person's habits such as travel patterns, relationships, and political or personal preferences.

Facial recognition is the process of identifying a face from a digital image or video. FRT generally uses computer pattern recognition to find commonalities in images depicting human faces.[4] FRT can be deployed in real time or on static images. As explained below, it can be used to confirm the identity of a known person, or it can be used to uniquely identify an unknown person. FRT can also allow for the categorization and profiling of a person over time based on their facial information.

Facial recognition systems fall under two categories: one-to-one and one-to-many systems. A one-to-one system compares a user's image to multiple images of a single person to authenticate or verify a person's known identity. A one-to-many system compares an image to a database of different faces (such as a terrorist watchlist or mugshot database) to uniquely identify an individual among a group of people, often in live or real-time settings. The use of these latter systems in law enforcement and public safety is especially contentious due to the greater scale of comparison and the legal ambiguity surrounding the construction of databases and watchlists.

FRT is part of a larger suite of biometric "recognition" technologies. These systems categorize individuals based on more traditional ("strong") biometric identifiers like fingerprints and retina scans, less unique ("weak") indicators like body shape or voice, and non-unique ("soft") indicators like gender or age.[5] Regulating FRT alone is not enough because facial information is a type of biometric information. Biometric information is highly sensitive in nature given that it reveals "intimate details of the lifestyle and personal choices of the individual" and would form a part of the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" as well as from private actors, particularly when they provide services to the state.[6]

Harms and Obligations: The Significant Risks of FRT to Uniquely Identify Individuals

FRT use can come with significant costs. Experts have identified the following harms associated with the use of facial recognition software:[7]

- Lack of human autonomy over decisions;
- Lack of transparency for reasons behind certain results;
- Inaccuracy (e.g., false negatives);
- Discrimination; and
- Risk of unauthorized sensitive data access and manipulation (including children's data).

FRT can enable surveillance, privacy intrusions, discrimination, and limitations on free speech on a mass scale. Experts have identified that FRT can be used for on-the-spot unique

identification of people in real-time, resulting in the mass surveillance of groups of people. Such surveillance can deprive people of their right to privacy at significant speed and scale, including the freedom to remain anonymous, including in public settings. FRT has been used to facilitate real-time apprehension of individuals, with chilling impacts on individuals' lawful speech and expression.[8] Such use of FRT has particularly harmful impacts on equality-seeking communities, including women, racialized communities, people in the LGBTQ+ community, and other communities protected by discrimination law.

For clarity, we have compiled a non-exhaustive list of concrete examples to show how FRT has been used with harmful impacts on privacy and on equality-seeking populations:

- Three people have been wrongfully arrested after flawed matches from a facial recognition algorithm.[9]
- Gender classifiers sold in API bundles made available by Microsoft, IBM, and Face++ for facial recognition models were proven to have error rates up to 34.7% for darker-skinned women.[10]
- Biometrics incorporated into decision-making systems have disproportionately harmed multiply-marginalized disabled people.[11]
- Twitter's image-cropping algorithm was found to have a racial bias by favouring white faces over Black ones.[12]
- Clearview AI's technology allowed law enforcement and commercial organizations to match photographs of unknown people against the company's databank of more than 3 billion images, including of Canadians and children, for investigation purposes, creating a risk of significant harm to individuals, the vast majority of whom have never been and will never be implicated in a crime.[13]
- Government of Canada officials 'quietly' tested facial recognition at Toronto's Pearson International Airport in 2016 to detect travelers using fake identities without informing the public and without consent.[14]
- Facebook was fined $650 million for violating Illinois' *Biometric Information Privacy Act*. Amazon and Microsoft are currently under investigation after being accused of using a database comprised of Flickr images to improve the accuracy of their facial recognition software without the consent of those featured in the images.[15]

Canada's Current Approach to Regulating FRT and Biometric Recognition Systems is Inadequate

In Canada, the lack of clear regulatory frameworks around FRT shines a light on the inadequacy of Canada's approach regarding the privacy and human rights risks of algorithmic systems such as biometric recognition systems.[16] Privacy laws are one of the main regulatory tools to help protect Canadians' human dignity, personal integrity, and control and autonomy over one's information and body.[17] Canada's privacy obligations under international and domestic law include adherence to:[18]

- Article 12 of the [Universal Declaration of Human Rights](#) and Article 17 of the [International Covenant on Civil and Political Rights](#), which prohibit arbitrary interferences into people's private lives;
- [Section 8 of the *Canadian Charter of Rights and Freedoms*](#), which protects individuals from unreasonable search or seizure;
- The [*Privacy Act*](#), which details laws that protect the privacy of individuals with respect to personal information collected, used and disclosed by federal government institutions; and
- [PIPEDA](#), which covers privacy regulations that apply to the private sector in the federal context and when provincial laws do not apply.

Some of the most serious legal concerns and recommendations for Canada's *Privacy Act* related to FRT are outlined in our report [Facing the Realities of Facial Recognition Technology](#). In particular, the Supreme Court has held that the state's collection of bodily information without a person's consent is a serious violation of one's body, thereby threatening protected values under sections 7 and 8 of the Charter, such as dignity, integrity, and autonomy.[19] As outlined in section 7, the very act of collecting biometric information by federal institutions may therefore constitute interference with a person's right to life, liberty, and security of the person. As highlighted earlier, the collection of biometric information may also constitute an unreasonable search and seizure by the state where there exist no reasonable limits on these rights prescribed by law that can be demonstrably justified in a free and democratic society.[20]

Legal Changes Needed in Canada: Start with Privacy Laws Regarding Biometric Recognition Systems Including FRT

Canada lacks specific regulations around the use of biometric recognition technology such as FRT, as well as specific provisions around the collection, use, and retention of data through such biometric systems. Most notably, the *Privacy Act* and PIPEDA do not explicitly include facial and biometric information as subsets of personal information worthy of special protection. Given the already established significant legal and human rights risks associated with the collection, use, and disclosure of biometric information, this legal gap must be closed to protect people's human rights and freedoms, particularly the rights to privacy, free expression, and freedom from discrimination, among others.

Changes are needed to Canada's federal privacy laws to properly account for the harms related to biometric recognition systems. As Sonja Solomun and Yuan Stevens outline in their [February 2021 report](#), the Government of Canada can mitigate serious privacy and security risks by implementing the following recommendations to amend the *Privacy Act*, with lessons that can be applied for any changes or overhaul made to PIPEDA:

1. **Acknowledge and explicitly account for the existence of personal information relating to a person's physical or biological characteristics** or biometric information, including facial information.

2. **Adequately safeguard the privacy and security of Canadians** by implementing requirements concerning biometric information such as facial images. These requirements should provide:
   a. Limitations on the collection, use and disclosure of such biometric information, requiring at the very least notice and either consent or explicit legislative permission;
   b. Requirements to minimize information collection; and
   c. More expansive safeguards for the security of sensitive information, once collected.

3. **In particular, align privacy laws such as the *Privacy Act* with the requirements of the Directive on Automated Decision-Making.** This alignment would dictate more specific terms for use by law enforcement — ensuring public notice, bias testing, employee training, security risk assessments, and the need for a human to make a final decision in the case of high-impact decisions. These requirements should be expanded to provide for adequate and meaningful consultation before the deployment of FRT for unique identification of individuals.

4. **As outlined below, implement a federal moratorium on automated facial recognition and the disclosure of facial information, until:**
   a. The framework described in this submission has been developed in consultation with Canadians, as well as with government institutions and public servants in relevant government departments; and
   b. More research is done on the disproportionate impacts, or potential for disproportionate impact, on members of certain demographic groups, particular to the realities and populations in Canada.

An Interim Solution: A Public Moratorium on FRT

As the federal government identifies the best legal solutions regarding more robust privacy regulations for biometric information, we strongly recommend a temporary moratorium on the use of FRT, at the very least by federal government institutions.[21] Canada's privacy commissioners, the Ligue des droits et libertés, the Canadian Human Rights Commission, and over 70 Canadian and international organizations and advocates in the fields of privacy, human rights, and civil liberties have called for such a moratorium in policing and surveillance.[22]

Although law enforcement contains the clearest risks and most publicized abuses of FRT, other government agencies currently use or are likely to adopt this technology. To better understand the risks and safeguard people's rights, this prohibition should thus extend across the public sector at the federal level.

The Centre for Media, Technology and Democracy has advocated for this approach since August 2020, when we released two policy briefings on the subject. The first briefing describes the rationale for and implications of a moratorium on the Canadian public sector's use of FRT. The second briefing explores conditions under which a moratorium could be lifted.

Swift government action is needed to identify, manage, and mitigate the possible harms that arise with this quickly evolving landscape.[23] Moratoriums have become the default policy option worldwide for regulating the use of FRT by government agencies and police forces.[24] A national moratorium is not in itself a solution; instead, it affords the government time to evaluate and develop the necessary conditions FRT companies and public sector actors should follow. These conditions should include updated legal frameworks for privacy and the automated processing of data, accountability measures for institutions that use FRT, and social impact assessments, among others.[25]

In the interim, we advise that the Government of Canada:

- Create an expert panel to study the current use of biometric recognition systems such as FRT in Canada, to review data and privacy legislation to identify gaps, and to ultimately develop the optimal regulatory requirements for lifting a moratorium;
- Conduct large-scale consultations to assess the perspectives of Canadians — particularly those in marginalized communities — on FRT in public use, building on initial consultations regarding police use of FRT;
- Coordinate a national research effort on the use of biometric systems such as FRT in the public and private sectors, with a series of reports jointly commissioned by the Office of the Privacy Commissioner, the provincial and territorial Privacy Commissioners, and the National Research Council; and
- Commission Privacy Impact Assessments and Data Protection Impact Assessments for FRT use by each relevant government institution.[26]

This was a main topic of discussion at the policy roundtable we convened in November 2020 with the Cybersecure Policy Exchange at Toronto Metropolitan University. 30 expert stakeholders and government officials weighed the push for a limited public-sector prohibition on FRT against alternative approaches to mitigate FRT risks. Their prescriptions for government varied, but stakeholders all stressed the importance of swift government action to identify, manage, and mitigate the possible harms that arise with this quickly evolving landscape.[27]

APPENDIX 1: Organizations and Individuals

About the Centre for Media, Technology and Democracy
The Centre for Media, Technology and Democracy at McGill University's Max Bell School of Public Policy is an interdisciplinary research centre dedicated to understanding and responding to the social, political, and policy challenges posed by our evolving information ecosystem and digital technologies. Facial recognition technology has been a critical issue for the Centre since its launch in 2020. Over the last two years, the Centre has conducted and commissioned research, hosted convenings, and presented several policy recommendations in the area of FRT in Canada. Learn more at www.mediatechdemocracy.com/projects/facial-recognition-governance.

About the Cybersecure Policy Exchange
The Cybersecure Policy Exchange (CPX) at the Toronto Metropolitan University (TMU) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, sponsored by the Royal Bank of Canada and co-led by the Rogers Cybersecure Catalyst and the Leadership Lab at TMU. We undertake research and policy development on the responsible governance of technology and work to broaden and deepen public discussions of these issues through speeches, roundtables, and workshops. We have published a number of reports, including results from national surveys, interviews, and focus groups, and convened a broad network of policymakers, industry experts, academics, and civil society on a number of pressing information security and democracy issues, including regulation of facial recognition technology, social media platforms, COVID-19 contact tracing apps, encryption technology, and trans-border data storage.

Sonja Solomun
Sonja Solomun is the Director of Research at the Centre for Media, Technology and Democracy at McGill University's Max Bell School of Public Policy. She is a Research Affiliate at the Data & Society Research Institute, the Center for Information, Technology, and Public Life (CITAP) at the University of North Carolina at Chapel Hill, and at the Climate Social Science Network at Brown University's Institute for Environment and Society. She is a Co-Founder of the Coalition for Critical Technology, and a founding member of the Platform Governance Research Network.

Yuan Stevens
Yuan (you-anne) Stevens is Policy Lead on Technology, Cybersecurity and Democracy at the Leadership Lab and Cybersecure Policy Exchange at Toronto Metropolitan University. She received her JD/BCL from the Faculty of Law at McGill University. She previously worked at the Berkman Klein Center for Internet and Society at Harvard University and is a research fellow and LL.M Candidate at the Centre for Law, Technology and Society at the University of Ottawa.

Julia Bugiel

Julia Bugiel is a research assistant at the Centre for Media, Technology and Democracy. She is an MA student in Communication Studies at McGill University and a Canada Graduate Scholarship recipient. She previously worked at the Institute for Research on Public Policy.

APPENDIX 2: Lessons from the US and the EU

Given the high-risk and highly sensitive nature of FRT for equality-seeking groups, there is an urgent need for Canada to implement shared lessons from regulatory frameworks in the EU and several US states.[28] The Government of Canada may wish to look to the following international precedents to glean shared lessons:

- The EU's **Artificial Intelligence Act** aims to comprehensively harmonize the legal framework on artificial intelligence among EU Member States with respect to trade, commerce, research, and the protection of fundamental rights. Article 29 imposes on users of high-risk AI systems (i.e. systems that pose significant risks to the health and safety or fundamental rights of person) the obligation to carry out a data protection impact assessment according to Article 35 of the EU General Data Protection Regulation (GDPR).
  - 120 civil society organizations have signed a collective statement calling on the EU to adopt an Artificial Intelligence Act that centres fundamental rights.[29]
- The **EU Law Enforcement Directive** forbids law enforcement from processing biometric data for the purpose of uniquely identifying a person except where authorized by law, to protect a person's vital interests, or where the data is "manifestly made public" by a person. It also prohibits law enforcement from making decisions based solely on automated processing (including profiling), unless EU or domestic law is enacted that provides appropriate safeguards for individual rights and freedoms. Moreover, it prohibits profiling that results in discrimination on the basis of special categories of data, including biometric information such as facial images.[30]
  - **The European Data Protection Supervisor** has also called for a general ban on any use of AI for the automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes, and other biometric or behavioural signals, in any context.[31]
- In the **US**, several cities (e.g. San Francisco, CA; Bellingham, WA; Oakland, CA; Somerville, MA) have banned police use of facial recognition technology. Vermont and Virginia have banned the practice at the state level.[32]
- The **Illinois** *Biometric Information Privacy Act* (BIPA) imposes stricter requirements on companies that provide automated facial recognition services to law enforcement. It prohibits 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.
- **Massachusetts** recently enacted its *Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth*, which requires law enforcement to obtain a warrant before conducting a facial recognition search, except in emergency situations. It also prohibits the police from acquiring, accessing, or using facial recognition software themselves as well as making a request or entering into a contract to do so.[33]

Endnotes

1. Joint Statement by Federal, Provincial and Territorial Privacy Commissioners, "Recommended legal framework for police agencies' use of facial recognition" (2 May 2022), https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/.
2. Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Machine Learning Research* 81 (2018): 1-15 (paper presented at the Conference on Fairness, Accountability and Transparency, New York, 23-24 February 2018),
3. International Center for Not-for-profit Law, *The Impact of Artificial Intelligence Technologies on the Right to Privacy and Civic Freedoms* (submission to the Office of the High Commissioner for Human Rights, 2021),
4. Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, *Facial Recognition Moratorium Briefing #1,* Tech Informed Policy Initiative (August 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1.
5. Christiane Wendehorst & Yannic Duller, *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,* European Parliament (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.
6. See e.g., *R . v. Spencer,* 2014 SCC 43 (CanLII), [2014] 2 SCR 212, para 24; *R. v. Tessling*, 2004 SCC 67 (CanLII), [2004] 3 SCR 432, para 25; *R. v. Plant,* 1993 CanLII 70 (SCC), [1993] 3 SCR 281.
7. Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable: What We Heard* (February 2021), https://www.mediatechdemocracy.com/work/facial-recognition-technology-policy-roundtable-what-we-heard.
8. Pete Fussey and Daragh Murray, *Independent Report Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology,* Human Rights, Big Data and Technology Project, University of Essex (2019), https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.
9. Kashmir Hill, "Wrongfully accused by an algorithm," *The Seattle Times* (24 June 2020), https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/; Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives," *WIRED* (7 May 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
10. See Buolamwini & Gebru, "Gender Shades.".
11. Ridhi Shetty & Hannah Quay-de la Vallee, C*DT Comments to OSTP Highlight How Biometrics Impact Disabled People,* Center for Democracy & Technology (2022), https://cdt.org/insights/cdt-comments-to-ostp-highlight-how-biometrics-impact-disabled-people/.
12. See Chaim Gartenberg, "Twitter plans to change how image cropping works following concerns over racial bias," *The Verge* (2 October 2020), https://www.theverge.com/2020/10/2/21498619/twitter-image-cropping-update-racial-bias-machine-learning.
13. Office of the Privacy Commissioner of Canada, Office, "News release: Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say" (3 February 2021), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/?=february-2-2021.
14. See Tom Cardoso & Colin Freeze, "Ottawa tested facial recognition on millions of travellers at Toronto's Pearson airport in 2016," *The Globe and Mail* (19 July 2021), https://www.theglobeandmail.com/canada/article-ottawa-tested-facial-recognition-on-millions-of-travellers-at-torontos/.
15. Jennifer Bryant, "Facebook's $650M BIPA settlement 'a make-or-break moment,'" *IAPP* (5 March 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/; Katherine Anne Long, "Amazon and Microsoft team up to defend against facial recognition lawsuits," *The Seattle Times* (15 April 2021), https://www.seattletimes.com/business/technology/facial-recognition-lawsuits-against-amazon-and-microsoft-can-proceed-judge-rules/.

16. "Privacy guidance on facial recognition for police agencies," Office of the Privacy Commissioner of Canada (May 2, 2022), https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/.

17. Giorgio Resta, "Personnalité, Persönlichkeit, Personality," *European Journal of Comparative Law and Governance* 1, no. 3 (2008): 215-243, doi: https://doi.org/10.1163/22134514-00103002; Jane Bailey, "Towards an Equality-Enhancing Conception of Privacy," *Dalhousie Law Journal* 31, no. 2 (2008): 267-309.

18. See Owen et al., *Facial Recognition Moratorium Briefing #1*.

19. *The Constitution Act,* 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11, https://canlii.ca/t/ldsx (the Charter); *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 SCR 281, para 93, http://canlii.ca/t/1fs0w; *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44 (CanLII), [2000] 2 SCR 307, https://canlii.ca/t/525t, para 50, citing *R. v. Morgentaler*, 1988 CanLII 90 (SCC), p. 166.

20. Yuan Stevens & Sonja Solomun, *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act* (Centre for Media, Technology and Democracy, February 17, 2021), https://www.mediatechdemocracy.com/work/facing-the-realities-of-facial-recognition-technology; *R. v. Oakes*, 1986 CanLII 46 (SCC), [1986] 1 SCR 103, https://canlii.ca/t/1ftv6.

21. Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, *Facial Recognition Briefing #1*, Tech Informed Policy Initiative (August 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1.

22. Tim McSorley, "Open Letter: Canadian Government Must Ban Use of Facial Recognition Surveillance by Federal Law Enforcement, Intelligence Agencies" *Amnesty International Canada News* (July 8, 2020), https://www.amnesty.ca/news/open-letter-canadian-government-must-ban-use-of-facial-recognition-surveillance-by-federal-law-enforcement-intelligence-agencies/; Other Canadian advocates for some form of FRT moratorium include Cynthia Khoo, Associate at the Center on Privacy & Technology at Georgetown Law; Brenda McPhail, Director of Privacy, Technology & Surveillance Program at the Canadian Civil Liberties Association; Ana Brandescu, McConnell Professor of Practice, Centre for Interdisciplinary Research on Montreal, McGill University; and Yuan Stevens, Policy Lead on Technology, Cybersecurity and Democracy, Leadership Lab and Cybersecure Policy Exchange at Toronto Metropolitan University.

23. See Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable*.

24. Several US state governments, as well as the EU, have instituted prohibitions. See Owen et al., *Facial Recognition Moratorium Briefing #1*.

25. More details in Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe & Sonja Solomun, *Facial Recognition Moratorium Briefing #2,* Tech Informed Policy Initiative (August 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1-wfgs7.

26. Ibid.

27. See Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable*.

28. Sam Andrey, Sonja Solomun & Yuan Stevens, *Regulating Face Recognition to Address Racial and Discriminatory Logics in Policing | EPIC AI Symposium,* Centre for Media, Technology and Democracy (2021), https://www.mediatechdemocracy.com/work/regulating-face-recognition-to-address-racial-and-discriminatory-logics-in-policing-epic-ai-symposium; Yuan Stevens, N*ow You See Me? Advancing Data Protection and Privacy for Police Use of Facial Recognition in Canada*, Cybersecure Policy Exchange (2021), https://www.cybersecurepolicy.ca/now-you-see-me.

29. European Digital Rights (EDRi), *An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement* (2021), https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf; Asha Allen & Ophélie Stockhem, "EU Tech Policy Brief: January 2022 Recap," Center for Democracy & Technology (2 February 2022), https://cdt.org/insights/eu-tech-policy-brief-january-2022-recap/.

30. EU, *Directive 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, [2018] OJ L/119, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680, articles 10 and 11.

31. European Data Protection Board, "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" (21 June 2021), https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

32. Jake Parker, "Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition," Security Industry Association (9 July 2021), https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/.

33. *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.