TECH INFORMED POLICY

AUGUST 18, 2020

FACIAL RECOGNITION MORATORIUM BRIEFING #1

Implications of a Moratorium on Public Use of Facial Recognition Technology in Canada

Produced by

Taylor Owen, Policy Lead, Beaverbrook Chair in Ethics, Media and Communications, Director of the Centre for Media, Technology and Democracy, and Associate Professor in the Max Bell School of Public Policy, McGill University

Derek Ruths, Tech Lead, Director of the Network Dynamics Lab and Associate Professor of Computer Science, McGill University

Stephanie Cairns, Research Assistant

Sara Parker, Research Assistant

Charlotte Reboul, Research Assistant

Ellen Rowe, Research Assistant

Sonja Solomun, Research Director, Centre for Media, Technology and Democracy, McGill University

Kate Gilbert, Graphic Designer

Centre *for* MEDIA, TECHNOLOGY *and* DEMOCRACY

network dynamics @mcgill
measuring and predicting large-scale human behavior

ABOUT TIP

Tech Informed Policy (TIP) is an initiative spearheaded by two leading McGill researchers—Dr. Derek Ruths, Director of the Network Dynamics Lab and Associate Professor of Computer Science, and Dr. Taylor Owen, Beaverbrook Chair in Ethics, Media and Communications, Director of the Centre for Media, Technology and Democracy, and Associate Professor in the Max Bell School of Public Policy. TIP aims to demystify the technology underlying critical policy issues and to provide valuable, tech-based recommendations to Canadian policymakers.

For enquiries, please contact Derek Ruths.

Glossary of Terms

Artificial Intelligence (AI): Artificial Intelligence is a system designed to accomplish a task that normally requires human intelligence. AI systems "learn" how to do things by processing large amounts of information, finding patterns, and translating that knowledge to tasks.

Algorithm: A set of rules and procedures that a computer can follow to complete a certain task.

Application Programming Interface (API): An Application Programming Interface provides a framework for developers to create their own programs. It is a collection of potential operations that programmers can develop to suit their needs.

Database: A database consists of one or many datasets that have been organized and retained in a system/software program.

Dataset: A collection of data.

Feature vector: A numerical representation of a person's facial features, computed by an AI algorithm.

Match Score: A score between 0 and 1, indicating the likelihood that a pair of images depict the same person.

Match Score Threshold: A value between 0 and 1—pairs with match scores above this value will be flagged as matches.

One-to-many: FR system that compares one photo to many photos of different people. It aims to answer the question: "Who is this person?"

One-to-one: FR system that compares one photo to many photos of the same person. It aims to answer the question: "Is this the same person?"

Publicly Available Information (PAI): Publicly Available Information is information readily available via the internet, social media platforms, etc.

EXECUTIVE SUMMARY:

This briefing is one of two on Facial Recognition (FR) Technology. This briefing addresses how FR works and is used, as well as the implications of a federal moratorium, while briefing #2 explores the conditions for lifting said moratorium.

- Since March 2020, calls for Canada to impose a national moratorium on facial recognition technology, especially for companies providing FR services to law enforcement agencies, have increased.[1] [2] [3]
- A national moratorium would provide legislators time to develop a comprehensive and effective policy regulating the development, use, and distribution of FR technology and the data it collects, uses, and shares.
- Current FR technology is not infallible. FR service cannot be relied on by law enforcement due to its potential to discriminate against certain demographics and exacerbate conditions of inequality.
- This briefing outlines the technological, social, and policy, and legal conditions required to lift a Canadian moratorium on FR systems. Readers will learn the concerns, limitations, and potential harms of FR technology, as well as the technical implications of a federal moratorium. The 2nd briefing will conclude with the technical, social, and policy conditions for lifting a federal moratorium as well as recommendations on safely using FR technology.

WHAT IS FACIAL RECOGNITION (FR) TECHNOLOGY?

Facial recognition is the process of identifying a face from a digital image or video. FR technology uses Artificial Intelligence (AI) to identify specific features of a person's face and look for them in other images.

HOW DOES IT WORK?

FR systems fall under two categories—one-to-one and one-to-many algorithms.

A one-to-one algorithm compares a user's image to multiple images of a single person in order to verify the user's identity. Unlocking a phone through FR is a typical one-to-one example.

A one-to-many algorithm—which compares an image to a database of disparate faces—aims to identify an individual. Facial recognition in policing and border security employ one-to-many systems—as such, this briefing focuses on this latter type of FR.

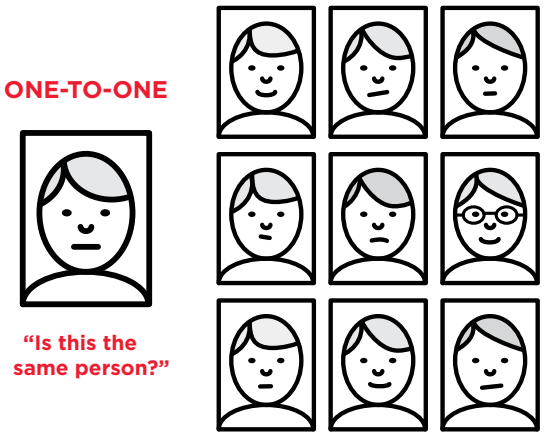
A one-to-many FR system incorporates the following components:

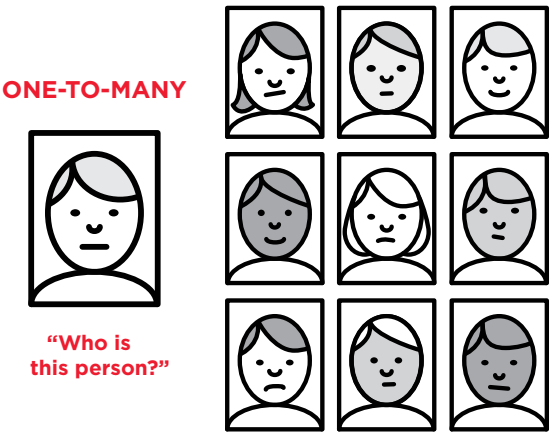
- A search database containing facial images. This database might belong to the government agency using the system (e.g. a police database of mugshots) or it might be provided by the system's developers (e.g. web images collected by the FR company).
- An algorithm, which takes an image of a face and attempts to match it to images in the search database.
- A training dataset of facial images used by developers to train the algorithm to make accurate matches.
- A testing dataset used to test the accuracy of the algorithm.

Step 1 – Feature extraction: An AI-based algorithm creates a numerical representation of a person's face by extracting the shape, size, and relative distance between their features. This numerical representation is called a feature vector. Precisely which features are encoded and how is largely inscrutable, as particular features are not hard-coded by developers but instead are "learned" by the algorithm. Prior to deployment, developers train and test the algorithm on large datasets of images. After deployment, depending on the terms of service of the specific FR technology, user images and other metadata may also be collected by the developers and used for further training.[4]

Step 2 – Comparison: After generating a feature vector, the FR system compares it to the feature vector of every image in a search database. Each pair of compared feature vectors is given a match score; the higher the match score, the more likely it is that the two original images depict the same person. A potential match is flagged if a pair's match score exceeds a given match score threshold. Certain tasks, such as identifying a criminal, require a high degree of certainty and have a low tolerance for error. These tasks necessitate a high match score threshold, so only pairs which are deemed very likely to be matches are flagged as such. For other tasks, like auto-tagging Facebook users in photos, a much lower threshold would suffice. Since a single commercial FR system is often used for different tasks requiring different levels of confidence, no industry-wide match threshold standard can be established.[5] A default match threshold is set by the developer but can be adjusted by the agency.*

* The ACLU found that Amazon's Rekognition matched 28 members of Congress to a database of mugshots when set to Amazon's default threshold of 80%; Amazon responded that the recommended setting for police use is 95%. However, there is currently no mechanism to enforce this recommendation..





RECENT USE OF FR TECHNOLOGY IN CANADA

RECENT USE BY GOVERNMENT

Canadian Border Protection:

At major airports, such as Vancouver International and Toronto Pearson, the Canadian Border Services Agency (CBSA) provides voluntary self-service kiosks at customs to verify the identity of travellers entering the country. NEXUS[6] and CANPASS holders can also be verified via voluntary iris identification.[7] The technology, called BorderXpress, is provided by Innovative Travel Solutions, an affiliate of Vancouver International Airport.[8]

It sends relevant information to the CBSA, but does not collect any personal information itself. Passport Canada agents also use FR technology to compare passport applicants with images of previous applicants to assess the legitimacy of applications.[9]

Municipal police departments:

At least 35 Canadian police departments have used FR technology.[10] The Calgary Police Department (CPD) has been using NeoFace Reveal since 2014 to compare images and videos of persons of interest, like from CCTV footage, to their own mugshot database.[11] The CPD enforces strict rules within the department regarding how the service is used, who is permitted to use it, and that images are only compared with mugshots.[12] The Toronto Police Department has been using FR technology since May 2019 in the same way as the CPD, but has ceased using it and has requested an investigation by the Office of the Privacy Commissioner into Clearview AI, the provider of the technology.[13]

RCMP:

The National Child Exploitation Crime Centre division of the RCMP used FR technology provided by Clearview AI to "identify, locate, and rescue children who have been or are victims of online sexual abuse."[14] As of May 4, 2020, it had used Clearview AI's service 15 times and rescued two children.[15] Additionally, a few units within the RCMP have used the service on a "trial basis" to test its "potential for use in a criminal investigation."[16] The RCMP has stated that it would have used FR technology only "in very limited and specific circumstances."[17]

FR technology is also used in some provinces to compare images to those found in databases of drivers licenses to prevent identity theft and fraud.[18] Some casinos across Canada also use FR-enabled security cameras to detect known cheaters and people who have indicated to the casino that they wish to be stopped from gambling.[19]

PRIVATE SECTOR

FR technology is also used in the private sector. Android and Apple smartphones can be unlocked by the user's face, while Facebook, Google, and Apple use FR technology to tag individuals in photos. Furthermore, some retailers, such as Toronto's Eaton Centre and Canadian Tire, use FR technology to apprehend shoplifters.[20] [21] Bell has also revealed plans to create a FR service, catering to Canadian businesses.[22]

MAJOR COMPANIES INVOLVED IN FR TECHNOLOGY

Amazon:

Amazon provides its own FR service, called Rekognition.[23] Rekognition can detect objects, faces, text, activities, and inappropriate content in images and videos. The service can be adapted to many different uses and functions required by the client. Amazon previously provided Rekognition to law enforcement in the United States, but recently declared a one-year moratorium in light of the Black Lives Matter protests.[24] [25]

Axon:

Despite previously providing AI technology to law enforcement, Axon has determined that current FR technology is not reliable, unbiased, and regulated enough to ethically be used for law enforcement purposes.[26]

Clearview AI:

The largest provider of FR technology to Canadian law enforcement was Clearview AI, an American software company.[27] However, the company has suspended its services to Canadian clients, including the RCMP, in response to ongoing OPC investigations of the company.[28]

Clearview AI offers free service and trials to law enforcement agencies. Clearview AI's software compares inputted images with those in their own database, compiled from 3 billion publicly available photos of faces taken from the internet (Facebook, Instagram, and third party websites) without explicit user consent. The software then returns the other images of the subject and where on the Internet they were found.

Clearview AI's approach to privacy is questionable. Clearview AI's use of pulling images from social media for FR technology purposes violates many social media websites' terms of use, like Facebook and Twitter.[29] Clearview AI does not uphold standards of transparency, as they have not released details of how their technology works or how effective it is in accurately identifying people. Clearview AI also used to provide their service to private companies but has stated that they will only service law enforcement agencies moving forward.[30]

While Clearview AI has agreed to permit user requests to have photos of themselves removed from their database after public scrutiny, this right is only afforded to those who live in jurisdictions with legal requirements governing FR technology, like California, the United Kingdom, and the European Union. Clearview AI recently gave Canadians this opportunity, as well, despite Canada not having the requisite legislation.[31]

Facebook:

Facebook created DeepFace, their own FR algorithm, in 2014.[32] The algorithm was trained using 4 million images uploaded to Facebook of more than 4,000 Facebook users. DeepFace plots the features of a person's face from a two-dimensional image, then uses those vectors to create a three-dimensional representation of the person. It can then use the three-dimensional figure to identify other photos of the person from different angles. DeepFace apparently has a 97.25% accuracy rate.[33]

Facebook uses its FR technology to help users tag images of their friends in photos, notify the user if they are in a photo uploaded to Facebook, and protect users from identity misuse.[34] The US Federal Trade Commission sued Facebook for $5 billion USD in 2012 for, among other privacy violations, not sufficiently informing users about its use of FR.[35]

Facebook does not currently sell DeepFace as a service.

Google:

Google uses a variety of facial detection services. Newer Google phones can be unlocked using FR systems to recognize the user's face;[36] Google Photos uses facial clustering to organize photos containing similar faces;[37] Google's Cloud Vision API can detect key facial features of a person in an image, including emotion;[38] Google Maps detects faces in Street View images to blur them out.[39]

Google's FR technology is reportedly more erroneous when detecting darker skin tones. Consequently, Google technicians allegedly targeted persons of colour to agree to having their picture taken to improve the Google FR database.[40] Google does not sell their FR technology as a publicly available service but does provide other AI-powered systems to law enforcement for surveillance use.[41]

Idemia:

Idemia recently offered their FR services to the Sûreté du Québec. It is one of the largest biometric identification companies in the world, providing FR technology and biometric security to law enforcement, security agencies, financial institutions, and government services all over the world.[42] Idemia offers a variety of biometric identification security services, such as video equipped for FR technology, facial recognition and identification, identity verification, real-time facial recognition tools, and advanced fingerprinting technology.[43]

Idemia is based in France and is therefore subject to the GDPR.[44] Idemia's algorithm has also been shown to be ten times more error-prone when identifying persons of colour than white people.[45]

Microsoft:

Microsoft is also a major provider of FR technology in Canada, but primarily in the private sector. Microsoft offers free trials of its Azure API to encourage app developers to integrate FR in their applications. Microsoft does not provide a search database; rather, the Azure API allows developers to match a person to images within their own private databases of up to 1 million people. It can also recognize similar faces and recurring attributes within images. The Azure API can also detect some facial expressions, such as happiness, anger, and fear.[46]

Microsoft's Azure has more security compliance certifications than any other cloud-based FR service. Microsoft has also declared a moratorium on providing FR technology to law enforcement.[47]

NEC:

NEC's NeoFace Reveal is currently used by the Calgary Police Department and was tested by the Ottawa Police Department.[48] NeoFace is considered the most "accurate" FR technology on the market by the National Institute of Standards and Technology.[49] The system can enhance low-quality images and compare faces, even at unideal angles or in poor lighting, to faces in law enforcement mugshot databases.[50] NEC biometric security solutions are used by security and law enforcement agencies in over 70 countries.[51]

Other major companies that provide FR services:

- Accenture
- Aware
- BioID
- Certibio
- Fujitsu
- Fulcrum Biometrics
- Thales
- HYPR
- Lydos
- M2SYS
- NEC
- Nuance
- Phonexia
- Smilepass

CONCERNS/PROBLEMS AROUND FR TECHNOLOGY:

PRIVACY & DATA PROTECTIONS

While some developers provide only the FR system needed to search a database, others provide the database itself. Companies like Clearview AI engage in web scraping to fill this database, extracting massive amounts of data from social media platforms.[52] These two approaches differ drastically: the former enables police agencies to more easily search their own databases; the latter allows for matches to be made with almost any person who has uploaded a photo online. Web scraping raises obvious privacy concerns; LinkedIn and Twitter are among the tech giants to have retaliated against this practice, sending cease-and-desist letters to Clearview AI.[53] [54] Numerous lawsuits have also been launched against the company.[55] Despite Clearview AI's withdrawal from the Canadian market, its presence, hitherto pervasive among police departments, has highlighted the limitations of existing data protection laws in Canada, particularly the failure to grant Canadians the "right to erasure". Clearview AI may have been able to establish such a strong presence among law enforcement because of a distinct lack of adequate data protection in Canada. To fully protect Canadians' rights to privacy and identity, revised privacy regulation and stronger data protection and a revised privacy regulation is needed—specifically one with the ability to mitigate the harms caused by web scraping and similar practices.

ENCRYPTION AND DATA SECURITY

Given the rise in data breaches, companies that provide FR technology to law enforcement must develop privacy protection measures and improve the security of information databases.[56]

In winter 2020, police stations across Toronto, using Clearview AI's FR technology, reported a security breach, in which "lists of customers, the number of user accounts those customers had set up, and the number of searches its customers have conducted"[57] were compromised.

A similar security incident occurred in the UK in 2019. In hiring penetration testing security consultants, police stations using FR technology by Suprema determined the data was unprotected and the personal information including "fingerprints of over 1 million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees"[58] was easily accessible. The consultants accessed the system's "database by manipulating the URL search criteria in Elasticsearch to gain access to data."[59] These two examples alone demonstrate how crucial encryption and data security practices are to ensuring private information gathered from the FR technology is secure.

STRUCTURAL PROPENSITY TOWARD BIAS RESULTS IN REAL-WORLD HARM

Facial recognition technology—and AI more broadly—has long been susceptible to bias and identity-based discrimination. A seminal study of three leading gender classification algorithms found that despite attaining near-perfect overall accuracy, the algorithms misgendered faces of women with darker skin tone at rates of up to 35%.[60]

A comprehensive report by the US National Institute of Standards and Technology (NIST) focused specifically on facial recognition technology, testing 189 algorithms on 18 million

photos, split between four datasets.[61] The report detected significantly higher rates of false positives (i.e. incorrect matches) among East and West Africans and East Asians when searching Visa photos (except when testing Chinese-made algorithms, in which case low false positive rates for East Asians were observed) and among Indigenous people, African Americans, and Asians when searching mugshots. False positive rates also differed by gender and age, with women, children, and the elderly more likely to be misidentified.

A biased facial recognition system has the potential to do great harm, especially toward racialized groups already disproportionately affected by police scrutiny. In matching images to a mugshot database, NIST reported not only high false positive rates for African Americans, but low false negative rates, implying that facial recognition software is both more likely to make a false match and less likely to make no match.

The wrongful arrest of Robert Williams in Detroit, Michigan is an example of a false match.[62] Williams, a Black man, was wrongly identified by FR software as matching the profile of a wanted criminal and was subsequently arrested and detained for 30 hours; the match by the FR system was the only evidence.[63] Given the heightened risk of police violence faced by Black communities, an algorithm "overeager" to match Black faces is of great concern.

More research is required to determine where this bias enters facial recognition systems; it is unclear if it is the image quality of the search database, the demographic makeup of the training dataset, or the algorithm itself that is most to blame.

Culprit 1: Cameras

A 2019 study showed a strong correlation between algorithmic accuracy and skin reflectance (which in turn correlates with skin tone, as lighter skin is more reflective).[64] While this relationship persisted across systems, it was significantly weaker in systems with high overall accuracy. In fact, error rates among light-skinned men using inferior systems were higher than those for dark-skinned women using superior systems. In particular, researchers inferred that differences in acquisition systems (including image quality) could widen, reduce, or eliminate the accuracy gap between demographics.

Culprit 2: Training and testing datasets

However, this explanation is likely insufficient, as NIST reported that false positive rates differed between demographics even in high-quality well-lit photos. Moreover, the discrepancy between Chinese and western-made algorithms in accurately matching Asian faces indicates that the problem may in fact lie in the algorithms or the training sets used by developers.

Many companies, including Clearview AI and Amazon, are not transparent about the demographic breakdowns of their training sets, making it difficult to concretely assess whether a lack of diversity among training photos is responsible for demographic bias.

Preliminary research indicates that this bias could be reduced by creating synthetic faces to racially diversify the training set.[65]

Culprit 3: Algorithm

But, other researchers have discovered that even balancing a training set may be insufficient to counter gender bias, as facial recognition systems unintentionally "encode" gender-based information regardless of whether their training datasets skew heavily male or are perfectly balanced.[66] [67] A proposed approach is to remove gendered information from facial feature vectors, thereby forcing facial recognition systems to become "gender agnostic".

Testing

It is equally important to examine the datasets used to test systems—while these datasets will not directly affect a system's underlying accuracy, they can warp how that accuracy is reported (for instance, a racially biased algorithm will have a higher accuracy when tested on a largely white dataset). Two popular testing datasets, IJB-A and Audience, were found to be racially homogenous, with 80% and 86% of their photos, respectively, depicting light-skinned subjects, thereby not adequately representing people of colour.[68]

Most commercial FR systems used for policing in Canada have not released demographic information, and Clearview AI, until recently the most widely used, has not revealed any information regarding testing accuracy.

The FR technology research landscape remains sparse, as demonstrated by the varied and sometimes conflicting results outlined above. There is still much to be studied and tested before commercially available facial recognition systems can be deemed sufficiently bias-free.

MORATORIUMS ON FR TECHNOLOGY:

WHY CURRENT LEGAL/ REGULATORY REGIMES ARE INSUFFICIENT

In Canada, the legal frameworks and public policy approaches have not kept up with the rapid growth in surveillance technologies including in FR technology. There are currently no specific regulations around the use of FR systems, nor specific provisions around the collection, use, and retention of data through FR technology. Moreover, there is currently no independent oversight mechanism in place for the use of FR technology by police forces. The lack of clear regulatory frameworks around FR systems risks breaching both privacy and data protection law, which has pushed policymakers in Canada and abroad to consider enacting moratoriums banning the technology for a set period of time. Moratoriums have become the default policy option taken by governments worldwide when it pertains to regulating FR technology use by government agencies and police forces. Moratoriums allow legislators time to develop legal and policy frameworks that can ensure safe and responsible use of FR technology.

INDUSTRY INITIATIVES

In June 2020, Amazon announced a one-year moratorium on police use of its recognition technology by law enforcement.[69] IBM and Microsoft followed suit, with IBM ceasing all FR research, development, and sales.[70] [71] The moratoriums are reportedly intended to provide Congress adequate time to develop robust and comprehensive policy regulating FR technology in the US.

GOVERNMENT INITIATIVES

In Canada, provisions around the protection of privacy and legal frameworks have not caught up with present day technology, with FR technology as an example. Presently, section 8 of The Canadian Charter of Rights and Freedoms and international instruments binding on Canada, such as article 12 of the Declaration of Human Rights, provide insight to privacy protection legislation. The Privacy Act details laws that protect the privacy of individuals with respect to personal information collected, used, and disclosed by federal government institutions.

PIPEDA, on the other hand, covers privacy regulations that apply to the private sector. The ambiguity around the current legal provisions applicability to FR technology is accentuated by the lack of transparency on how the technology is being used, rendering the assessment of its legality contested. The Government of Canada must lead the country forward in determining acceptable use of FR technology by public agencies and law enforcement in order to ensure Canadian's basic human rights are protected. Government departments must work together to develop a robust legal framework and clear policies prior to lifting a moratorium.

In the United States, FR technology was banned for public departments and police use in several cities including San Francisco and Oakland, prohibiting the technology for a three year period.[72] Currently in California, law enforcement officers are not permitted to use body cameras with FR technology.[73] Similarly, the state of Massachusetts introduced a bill putting a moratorium on FR technology and other remote biometric surveillance systems after Brookline and Somerville both voted for bans.[74] [75] This suggests a great deal of policy transfer from municipal to state or provincial levels. The states of New Hampshire and Oregon also banned the technology for police body cameras and, most recently, New Jersey prohibited the use of FR technology for police departments, with New York quickly following suit by introducing a bill to stop all law enforcement use of FR technology.[76] [77] [78] Rather than banning the technology outright, some states including Illinois and Texas simply require companies to obtain consent from individuals prior to collecting facial imaging and any personal information.

The European Union (EU) announced plans for a 5-year moratorium on FR technology earlier this year. The moratorium would provide researchers more time to determine safe practices and minimize "inaccuracies [that potentially might be] used to breach privacy laws and facilitate identity fraud."[79] However, as of June 2020, the EU had shifted its plans. Instead, the European Union will "encourage individual member states to set their own facial recognition rules.[80]

Moratoriums are not the only policy options available to better regulate the use of FR technology. Indeed, moratoriums do not, by definition, address the core privacy or human rights issues around FR technology—they afford time to policymakers to develop adequate standards and laws. Most moratoriums are also limited in scope, only banning FR technology for very specific uses and thereby allowing for widespread use to remain in society, which could even lead to unexpected consequences as usage concentrates in private institutions. Most importantly, it remains unclear when and how moratoriums should be retracted.

An explored policy alternative has been to consider ways in which the technology could be used by government and law enforcement agencies with additional constraints applied. At the US federal level, the Facial Recognition Technology Warrant Act was submitted to the US Congress to limit the use of FR technology by federal agencies, namely through the introduction of warrant requirements.[81]

TECHNOLOGICAL IMPLICATIONS OF A MORATORIUM

Any proposed moratorium would need to clearly establish which specific technologies can and cannot be used and for what purpose, as well as which agencies are prohibited from using said technologies. For instance, a moratorium which bans the use of FR technology by law enforcement does not explicitly ban agencies from acquiring and testing the technology. Moreover, as most law enforcement agencies operate on the provincial/territorial or local level, a federal moratorium would not directly affect most police activity. A provision could instead be included to limit federal funding if provinces and cities do not enforce their own moratoriums.

A possible blueprint for a federal moratorium is the Facial Recognition and Biometric Technology Moratorium Act of 2020, recently introduced in the US Senate.[82] Biometric information systems encompass not only FR technology but are more broadly defined as technologies that capture or infer information about a person, such as identity, emotions, or location, based on their facial features, voice, gait, or other characteristics.

If passed, the bill would ban all federal agencies from buying, using, or indirectly obtaining (via a third party) information from any biometric information system (excluding fingerprint recognition). Agencies that violate the Act could be subject to civil actions from individuals or state attorneys general. State and local agencies would be barred from receiving important federal law enforcement funding if they fail to adopt similar policies or laws. The National Institute of Standards and Technologies (NIST) would be permitted to continue testing and researching FR technology, and particular uses of the technology could be authorized by a future Act of Congress. This future Act would need not only to detail who can use what technology and to what end but also to establish auditing requirements, standards for data retention and use, and minimum demographic accuracy thresholds.

An application of this framework to the Canadian context would involve a specific ban on the use of a FR service by the RCMP, purchased or otherwise. This ban could also potentially expand to the CBSA. Provincial governments should then be encouraged to introduce their own moratoriums, following the standard set by the federal government, restricting FR technology use by their own police departments and other provincial agencies. The limitation of FR service use could also extend to Crown corporations, government-owned businesses, and private-sector use.

NEXT STEPS

A moratorium is not a permanent solution. Rather, it would serve to give policymakers time to conduct the necessary research into and evaluation of FR technology and to thoroughly assess its effects in order to develop a strong policy framework to regulate FR. Briefing #2 in this series focuses on the technology, social, and policy conditions necessary to lift a federal moratorium.

REFERENCES

1 Weise, Karen, and Natasha Singer. "Amazon Pauses Police Use of Its Facial Recognition Software." The New York Times, June 10, 2020. https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html.

2 The Canadian Press. "NDP Calls for Moratorium on Clearview AI Facial Recognition Software." National Post, March 9, 2020. https://nationalpost.com/pmn/news-pmn/canada-news-pmn/ndp-calls-for-moratorium-on-clearview-ai-facial-recognition-software.

3 Taylor Owen and Nasma Ahmed. "Opinion: Let's Face the Facts: To Ensure Our Digital Rights, We Must Hit Pause on Facial-Recognition Technology." The Globe and Mail, February 14, 2020. https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/.

4 "Amazon Rekognition FAQs." Amazon Web Services. Amazon. Accessed July 8, 2020. https://aws.amazon.com/rekognition/faqs/.

5 Partnership on AI. "Understanding Facial Recognition Systems." February 19, 2020. https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

6 "Your Privacy at Airports and Borders." Office of the Privacy Commissioner of Canada, December 17, 2018. https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/your-privacy-at-airports-and-borders/.

7 Ibid.

8 "BorderXpress™." Innovative Travel Solutions. Accessed July 8, 2020. https://www.innovativetravelsolutions.ca/products/borderxpress/.

9 Office of the Privacy Commissioner of Canada, Automated Facial Recognition in the Public and Private Sectors, Gatineau, QC, 2014, https://www.priv.gc.ca/media/1765/fr_201303_e.pdf.

10 Kate Allen, Wendy Gillis, and Alex Boutilier. "Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known." Toronto Star, February 28, 2020. https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html.

11 "Facial Recognition To Aid Investigations." The City of Calgary Newsroom. City of Calgary, November 3, 2014. https://newsroom.calgary.ca/facial-recognition-to-aid-investigations/.

12 David Burke. "Privacy Laws Lag behind as Some Canadian Police Forces Begin to Use Facial Recognition Technology." CBC News. CBC, February 10, 2020. https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749.

13 Bryann Aguilar. "Toronto Police Chief Unaware Officers Have Been Using Controversial Facial Recognition Software for Months." CTV News, February 14, 2020. https://toronto.ctvnews.ca/toronto-police-chief-unaware-officers-have-been-using-controversial-facial-recognition-software-for-months-1.4811434.

14 "RCMP Use of Facial Recognition Technology." Royal Canadian Mounted Police, February 27, 2020. https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-use-facial-recognition-technology.

15 Ibid.

16 Ibid.

17 Catharine Tunney. "RCMP Says It Will Limit Its Use of Facial Recognition Tech—but Won't Stop Using It Entirely." CBC News. CBC, March 23, 2020. https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.5490988.

18 Research Group of the Office of the Privacy Commissioner of Canada. "Automated Facial Recognition in the Public and Private Sectors" March 2013. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/.

19 Ibid.

20 Chris Frey. "Revealed: How Facial Recognition Has Invaded Shops – and Your Privacy." The Guardian, March 3, 2016. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

21 "From facial recognition to extra staff: High and low tech tools used to combat shoplifting in Winnipeg." CTV News, February 21, 2019. https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648.

22 Marie-Claude Malboeuf. "Bell veut vous faire suivre en continu." La Presse, February 27, 2020. https://www.lapresse.ca/actualites/2020-02-27/bell-veut-vous-faire-suivre-en-continu.

23 "Amazon Rekognition." Amazon Web Services, Amazon, Accessed July 8, 2020. https://aws.amazon.com/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc.

24 Jason Del Rey. "Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers." Vox, September 26, 2019. https://www.vox.com/recode/2019/9/25/20884427/jeff-bezos-amazon-facial-recognition-draft-legislation-regulation-rekognition.

25 Karen Weise and Natasha Singer. “Amazon Pauses Police Use of Its Facial Recognition Software.” The New York Times, June 10, 2020. https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html.

26 “First Report of the Axon AI & Policing Technology Ethics Board.” The Policing Project. Accessed July 8, 2020. https://www.policingproject.org/axon-fr.

27 Kate Allen, Wendy Gillis, and Alex Boutilier. “Facial Recognition App Clearview AI Has Been Used Far More Widely in Canada than Previously Known.” Toronto Star, February 28, 2020. https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html.

28 “Clearview AI ceases offering its facial recognition technology in Canada.” Office of the Privacy Commissioner of Canada, July 6, 2020. https://priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/.

29 Kashmir Hill. “The Secretive Company That Might End Privacy as We Know It.” The New York Times, January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

30 Rebecca Heilwiel. “The world’s scariest facial recognition company, explained.” Vox, May 8, 2020. https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

31 Thomas Daigle. “Canadians can now opt out of Clearview AI facial recognition, with a catch” CBC News. July 10, 2020. https://www.cbc.ca/news/technology/clearview-ai-canadians-can-opt-out-1.5645089.

32 Yaniv Taigman, Ming Yang, Marc Aurelio Ranzato, and Lior Wolf.” DeepFace: Closing the Gap to Human-Level Performance in Face Verification.” (paper presented at the Conference on Computer Vision and Pattern Recognition, Greater Columbus Convention Center, Columbus, Ohio, June 24, 2014), https://research.fb.com/wp-content/uploads/2016/11/deepface-closing-the-gap-to-human-level-performance-in-face-verification.pdf.

33 Ibid.

34 Sigel Samuel. “Facebook will finally ask permission before using facial recognition on you.” Vox, September 4, 2019. https://www.vox.com/future-perfect/2019/9/4/20849307/facebook-facial-recognition-privacy-zuckerberg.

35 Lesley Fair. “FTC’s $5 billion Facebook settlement: Record-breaking and history-making.” Federal Trade Commission, July 24, 2019. https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

36 “Unlock your Pixel phone with your face.” Pixel Phone Help. Google. Accessed July 8, 2020. https://support.google.com/pixelphone/answer/9517039?hl=en.

37 “Search by people, things & places in your photos.” Google Photos Help. Google. Accessed July 8, 2020. https://support.google.com/photos/answer/6128838?co=GENIE.Platform%3DAndroid&hl=en.

38 “Detect faces.” Google Cloud. Google. Accessed July 8, 2020. https://cloud.google.com/vision/docs/detecting-faces.

39 “How Google uses pattern recognition to make sense of images.” Google. Accessed July 8, 2020. https://policies.google.com/technologies/pattern-recognition?hl=en-US.

40 Julia Carrie Wong. “Google reportedly targeted people with ‘dark skin’ to improve facial recognition.” The Guardian, October 3, 2019. https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color.

41 Jennifer Elias. “Google employees petition company to cancel police contracts.” CNBC, June 22, 2020. https://www.cnbc.com/2020/06/22/google-employees-petition-company-to-cancel-police-contracts.html.

42 Dave Gershgorn. “A Single Company Will Now Operate Facial Recognition for Nearly 800 Million People.” OneZero, June 5, 2020. https://onezero.medium.com/idemia-will-operate-facial-recognition-for-nearly-800-million-people-69b72582202b.

43 “Public security & law enforcement.” IDEMIA. Accessed July 8, 2020. https://www.idemia.com/public-security-law-enforcement.

44 “General Data Protection Regulation.” Intersoft Consulting. Accessed July 8, 2020. https://gdpr-info.eu/.

45 Tristan Péloquin. “Reconnaissance faciale: la SQ pourrait acquérir une technologie controversée.” La Presse, June 22, 2020. https://www.lapresse.ca/actualites/justice-et-faits-divers/2020-06-22/reconnaissance-faciale-la-sq-pourrait-acquerir-une-technologie-controversee.

46 “Face.” Microsoft Azure. Microsoft. Accessed July 8, 2020. https://azure.microsoft.com/en-ca/services/cognitive-services/face/#overview.

47 Nani Jansen Reventlow. “How Amazon’s Moratorium on Facial Recognition Tech Is Different From IBM’s and Microsoft’s.” Slate, June 11, 2020. https://slate.com/technology/2020/06/ibm-microsoft-amazon-facial-recognition-technology.html.

48 “OPS tested facial recognition software, but doesn’t use it.” CBC News. CBC, February 15, 2020. https://www.cbc.ca/news/canada/ottawa/ottawa-police-facial-recognition-1.5464964.

49 “Third-Party Authenticated.” NEC. Accessed July 8, 2020. https://www.necam.com/AdvancedRecognitionSystems/NISTValidation/FingerprintFacial/.

50 NEC, Advanced Criminal Investigative Solution Using Face Recognition Technology: NeoFace® Reveal, Irving, Texas, 2017. https://www.necam.com/Docs/?id=e838a769-4fa5-4264-bd1c-d9eeedf7b527.

51 "Bio-IDiom." NEC. Accessed July 8, 2020. https://www.nec.com/en/global/solutions/biometrics/index.html.

52 Louise Matsakis. "Scraping the Web Is a Powerful Tool. Clearview AI Abused It." Wired. January 25, 2020. https://www.wired.com/story/clearview-ai-scraping-web/.

53 Jon Porter. "Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech." The Verge. February 6, 2020. https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.

54 Kashmir Hill. "Twitter Tells Facial Recognition Trailblazer to Stop Using Photos." The New York Times. January 22, 2020. https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

55 Nick Statt. "ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy" The Verge. May 28, 2020. https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws.

56 Identity Theft Resource Center (ITRC). "2019 End of Year Data Breach Report." Identity Theft Resource Center, January 28, 2020. https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

57 Bryann Aguilar. "Company behind controversial facial recognition software used by Toronto police suffers data breach." CTV News, February 26, 2020. https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200.

58 Josh Taylor. "Major breach found in biometrics system used by banks, UK police and defence firms." The Guardian, August 14, 2019. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms?CMP=share_btn_tw.

59 Ibid.

60 Joy Buolamwini and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," (paper presented at 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research), 81:77-91, 2018. https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf.

61 National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, by Patrick Grother, Mei Ngan, and Kayee Hanaoka, Rep. 8280, US Department of Commerce, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (accessed July 8, 2020).

62 Bobby Allyn. "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man." NPR, June 24, 2020. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

63 Kashmir Hill. "Wrongfully Accused by an Algorithm." The New York Times, June 24, 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

64 Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton, and Arun R. Vemury. "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," IEEE Transactions on Biometrics, Behavior, and Identity Science, 1, no. 1 (2019), 32-41, http://jjhoward.org/wp-content/uploads/2019/02/demographic-effects-image-acquisition.pdf (accessed July 8, 2020).

65 Adam Kortylewski et al. "Analyzing and Reducing the Damage of Dataset Bias to Face Recognition with Synthetic Data" (paper presented at the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, June 16-20, 2019), 2261-2268. https://openaccess.thecvf.com/content_CVPRW_2019/papers/BEFA/Kortylewski_Analyzing_and_Reducing_the_Damage_of_Dataset_Bias_to_Face_CVPRW_2019_paper.pdf.

66 Prithviraj Dhar, Joshua Gleason, Hossein Souri, Carlos D. Castillo, and Rama Chellappa. "An adversarial learning algorithm for mitigating gender bias in face recognition." June 14, 2020. https://arxiv.org/pdf/2006.07845.pdf.

67 Tianlu Wang, Jieyu Zhao, Mark Yatskar, Kai-Wei Chang, and Vicente Ordonez. "Balanced Datasets Are Not Enough: Estimating and Mitigating Gender Bias in Deep Image Representations" (paper presented at the 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, South Korea, October 27-November 2, 2019), 5309-5318. https://arxiv.org/pdf/1811.08489.pdf (accessed July 8, 2020).

68 Joy Buolamwini and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," (paper presented at 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research), 81:77-91, 2018. https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf.

69 Nani Jansen Reventlow. "How Amazon's Moratorium on Facial Recognition Tech Is Different From IBM's and Microsoft's." Slate, June 11, 2020. https://slate.com/technology/2020/06/ibm-microsoft-amazon-facial-recognition-technology.html.

70 Jay Peters. "IBM will no longer offer, develop, or research facial recognition technology." The Verge, June 8, 2020. https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software.

71 Jay Greene. “Microsoft Won’t Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM.” The Washington Post, June 11, 2020. https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

72 Kate Conger, Richard Fausset and Serge F. Kovaleski. “San Francisco Bans Facial Recognition Technology.” The New York Times, May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

73 Rachel Mentz. “California lawmakers ban facial-recognition software from police body cams.” CNN Business. CNN, September 13, 2019. https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html.

74 Bill S.1385. “An Act establishing a moratorium on face recognition and other remote biometric surveillance systems.” Commonwealth of Massachusetts. https://malegislature.gov/Bills/191/S1385.

75 Nik DeCosta-Klipa. “Brookline becomes 2nd Massachusetts community to ban facial recognition.” Boston.com. December 12, 2019. https://www.boston.com/news/local-news/2019/12/12/brookline-facial-recognition.

76 ACLU NorCal. “California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams.” October 8, 2019. https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams.

77 Max Read. “Why We Should Ban Facial Recognition Technology.” Intelligencer. January 30, 2020. https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html.

78 Jane Wester. “NY State Senate Bill Would Ban Police Use of Facial Recognition Technology.” Law.com. January 27, 2020. https://www.law.com/newyorklawjournal/2020/01/27/ny-state-senate-bill-would-ban-police-use-of-facial-recognition-technology/?slreturn=20200608172543.

79 Javier Espinoza and Madhumita Murgia. “EU backs away from call for blanket ban on facial recognition tech.” Financial Times, February 11, 2020. https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5

80 Christine Fisher. ‘EU backs away form proposed five year facial recognition ban.’ Engadget, February 11, 2020. https://www.engadget.com/2020-02-11-european-commission-facial-recognition-guidelines.html

81 ALB19A70. “A Bill to limit the use of facial recognition technology by Federal agencies, and for other purposes.” https://www.coons.senate.gov/imo/media/doc/ALB19A70.pdf.

82 Ibid.