Facial Recognition Technology Policy Roundtable

What We Heard

cybersecure policy exchange
Powered by RBC

TIP TECH INFORMED POLICY

November 10, 2020

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is a new 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 made possible by the generous contributions of Royal Bank of Canada, which enable our team to independently investigate pressing public policy issues related to cybersecurity and digital privacy. We are committed to publishing objective findings and ensuring transparency by declaring the sponsors of our work.

Tech Informed Policy

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.

How to Cite this Report
Cybersecure Policy Exchange & Tech Informed Policy. (2021). Facial Recognition Technology Policy Roundtable: What We Heard. Cybersecure Policy Exchange and Tech Informed Policy.
https://www.cybersecurepolicy.ca/reports

Contributors
Taylor Owen, Beaverbrook Chair in Media, Ethics and Communications and Associate Professor, Max Bell School of Public Policy, McGill University
Derek Ruths, Associate Professor, School of Computer Science, McGill University
Sonja Solomun, Research Director, McGill Centre for Media, Technology and Democracy
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Communications and Knowledge Mobilization, Rogers Cybersecure Catalyst
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Yuan Stevens, Policy Lead, Cybersecure Policy Exchange and Ryerson Leadership Lab
Joe Masoodi, Policy Analyst, Cybersecure Policy Exchange and Ryerson Leadership Lab
Fahmida Kamali, Manager of Operations and Special Projects, Ryerson Leadership Lab
Braelyn Guppy, Marketing and Communications Lead, Ryerson Leadership Lab
Raisa Chowdhury, Student Notetaker, Ryerson Leadership Lab
Ellen Rowe, Student Notetaker, McGill University
Zaynab Choudhry, Design Lead, Ryerson Leadership Lab

Cybersecure Policy Exchange: https://www.cybersecurepolicy.ca/
@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

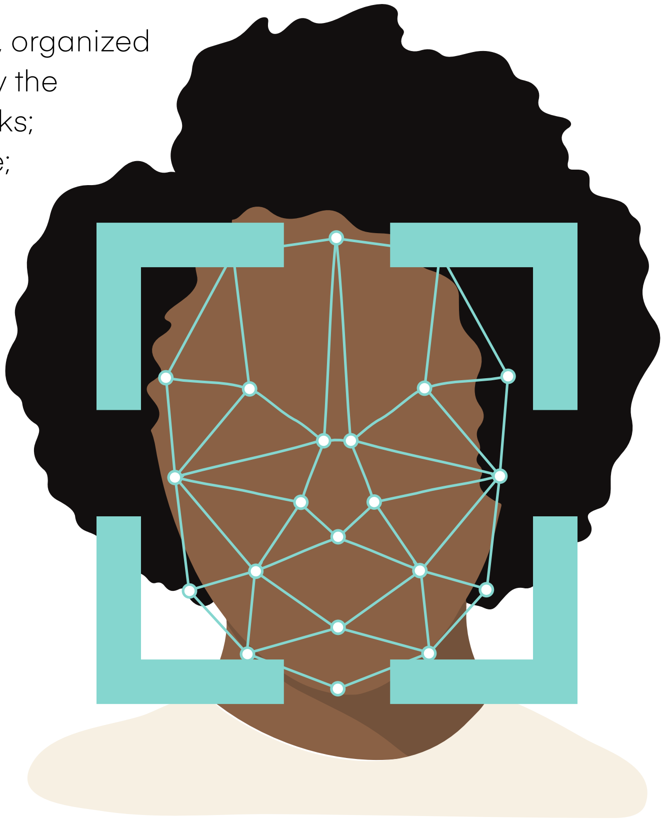
Tech Informed Policy: http://techinformedpolicy.ca/
@tip_mcgill @techinformedpolicy

Executive Summary

In November 2020, the Cybersecure Policy Exchange at Ryerson University and the Tech Informed Policy initiative at McGill University's Centre for Media, Technology and Democracy co-organized a roundtable on the **governance of facial recognition technology** (FRT). The event brought together **30 expert stakeholders and government officials** under Chatham House Rules, to examine the implications of a temporary prohibition on the public sector's use of FRT in Canada.

After significant developments in the last several years regarding the push for — and against — the use of FRT in Canada and the U.S., the Tech Informed Policy initiative released two policy briefings in August 2020. The first briefing describes the implications for a temporary prohibition or moratorium on the Canadian public sector's use of FRT.[1] The second briefing explores conditions under which a moratorium could be lifted.[2] The first of these briefings served as the basis of discussion for the roundtable event.

This report summarizes what we heard at the event, organized by: how facial recognition software is being used by the public sector, including its potential benefits and risks; views on the push for a limited prohibition on its use; and options to mitigate risk before and during the use of FRT for consideration, as proposed by the event's participants.



What We Heard

Due to the increasing use of facial recognition by public agencies and police forces in Canada, and the growing body of evidence that these technologies are leading to **real-world harms** and are embedded with **new risks**, policymakers are turning their attention to the potential for either temporary or permanent prohibition of their use. Risks include a lack of transparency and human autonomy over decisions, greater inaccuracy, discrimination and unauthorized access to sensitive personal data.

FRT is **already being used** by Canada's public sector for purposes such as law enforcement, passports, border protection, government ID/licences and casinos.[3] Some law enforcement agencies in Canada are actively using FRT, while other forces have temporarily used FRT software in the past or plan to use it in the future.[4]

Participants raised key policy questions for when and how public sector organizations should be able to use this technology, with two uses highlighted as needing particular scrutiny:

1. FRT in **real-time** (i.e., on-the-spot or dynamic face recognition); and
2. FRT on **images from certain types of databases** (e.g., collected from the Internet or social media, aprovided by companies like Clearview AI).

Participants in our workshop generally responded in three ways regarding the proposal to temporarily prohibit the public sector use of FRT in Canada:

1. **Support of the prohibition** based on the risks inherent in the use of FRT, and belief in the need to provide regulation and/or a policy framework before allowing or expanding government use of FRT;
2. **Pushback on an outright moratorium or prohibition** on government use of FRT, calling instead for greater oversight and governance of current and expanded use; and
3. **Pushes to define and delineate** the subject of prohibition and regulation, and to advance a **risk-based approach.**

Based on what we heard at the event, this report also begins to map out the following ways that policymakers in Canada could better manage and mitigate the risks of FRT, including:

- Requiring public consultations and transparency;
- Conducting audits and risk analysis;
- Improving public procurement practices related to FRT;
- Enhancing user training; and
- Implementing limits on when types of FRT can be used in Canada.

01 Setting the Stage

What is Facial Recognition Technology (FRT)?

Facial recognition technology generally uses computer pattern recognition to find commonalities in images depicting human faces.[5] The analysis of facial similarities between people depicted in images can be done manually (by hand with an index of photos) or in an automated fashion (relying on computer software and databases).

FRT that relies on artificial intelligence refers to software that determines the likelihood that datapoints in a set of images are similar enough to each other, therefore depicting the same person. FRT can be used for identification, authentication, verification or categorization of a person. Datapoints analyzed can be two- or three-dimensional, and typically compare the level of similarity of facial features such as colours, shapes or distances, as depicted in elements of various images.

> **"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."**
>
> **— TIP FRT Policy Briefing #1**

The Use of FRT in Canada

FRT is already being used by governments in Canada. FRT has been used, or is being used, in the following ways by Canadian government agencies:[6]

- Passports;
- Border protection (e.g., NEXUS);
- Government IDs and licences;
- Real-time identification for casinos in Ontario and B.C., for those who opt-in; and
- Law enforcement.

At least two law enforcement agencies in Canada — the Calgary Police Service and Toronto Police Service — have procured and currently use the services of the Japanese tech company NEC Corporation, which provides mugshot facial recognition software called Neoface Reveal.[7] Numerous other police forces across Canada have already implemented or are contemplating the use of facial recognition software (provided by NEC or other companies).[8] Use of such a database by the Toronto Police Services made the news in 2020, in a case involving second degree murder.[9]

There are numerous potential uses of FRT for the public sector in Canada, with examples including the use of drones, in airports, at public events, and for access to government buildings, schools or washrooms.

The Potential Benefits of FRT

Relying on automated decision-making processes can generally result in gains in the amount and variety of data that can be processed, as well as the speed of data analysis.[10] Participants identified that facial recognition software can be appealing for public sector organizations for the following reasons:

- **Efficiency:** Facial recognition software has the potential to increase the speed of the identification and verification process, in comparison to manual searches done only by humans.
- **Scale:** FRT may also increase the amount of data that can be analyzed (e.g., identification in large crowds, or image comparison using a large database).
- **Security and public safety:** Use of biometric data, such as facial features, to verify a person's identity may improve access security (e.g., when logging into bank accounts or personal devices), or it may improve public safety when used to identify people who are alleged to pose safety risks.

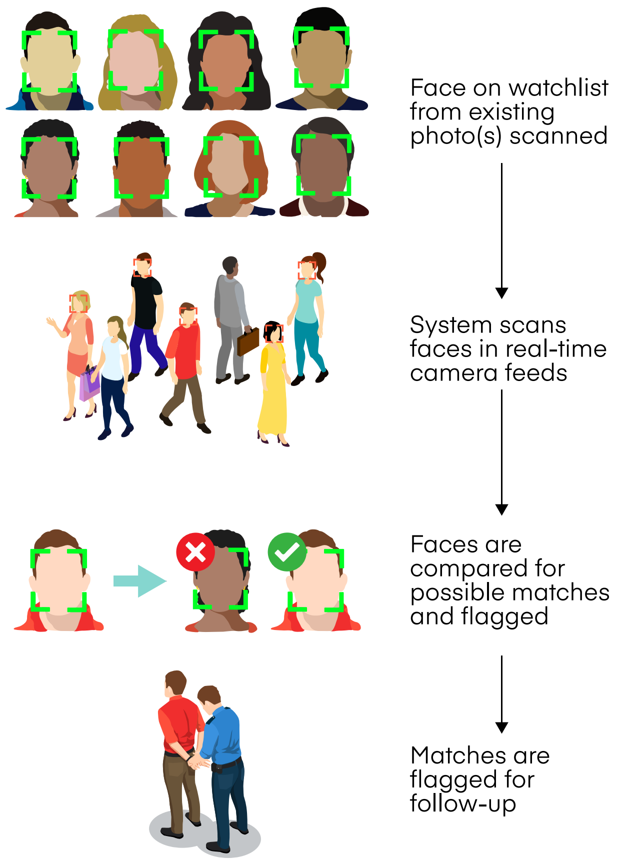
The Risks of Harm Associated with FRT

Relying on computer-automated processes to inform or replace human decisions raises critical ethical and legal issues. The features of automation can also be its flaws. With significant increases in data volume, variety and processing speed come numerous risks to human rights,[11] such as:

- Lack of **human autonomy** over decisions;
- Lack of **transparency** for reasons behind certain results;
- Greater **inaccuracy** (e.g., false negatives);
- **Discrimination** resulting from systems trained on datasets already imbued with prejudice, bias or patterns that should not necessarily inform future decision-making; and
- Risk of **unauthorized sensitive data access** and **manipulation.**

FRT can be used in **real-time (in a live, immediate) setting** or on still images, such as mugshots. The UK Information Commissioner's Office (ICO) found that live FRT is in use by their law enforcement to monitor public spaces for "watchlists" of "subjects of interest."[12] The software monitors camera footage for a certain geographic area and looks for a positive match, which can result in police approaching or apprehending an individual.

Real-time or Live Surveillance



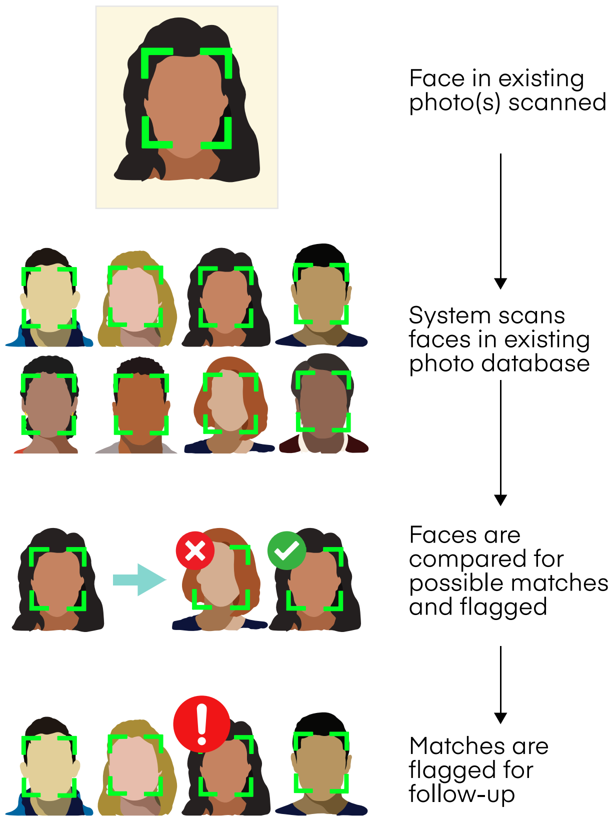
Face on watchlist from existing photo(s) scanned

System scans faces in real-time camera feeds

Faces are compared for possible matches and flagged

Matches are flagged for follow-up

Static Image Recognition



Face in existing photo(s) scanned

System scans faces in existing photo database

Faces are compared for possible matches and flagged

Matches are flagged for follow-up

The ICO recognizes the public safety benefits of live FRT, but has made law enforcement's use of such technology a regulatory priority for the following privacy-related reasons, which bear repeating here:

- **Scale of privacy intrusion**, with the potential to affect large numbers of people, in many cases without their knowledge, as they go about their daily lives; and
- The potential for FRT to enable **surveillance on a mass scale**, particularly considering the impact this has on people's human rights, and the rights to the privacy and security of their data.

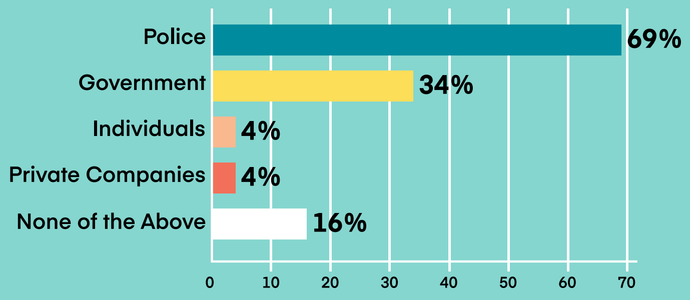
In the Canadian context, the use of live FRT by the government raises the same regulatory concerns. Two of our roundtable participants working in law enforcement spoke against the use of real-time FRT — what they called "live streaming" — citing the privacy concerns of on-the-spot identification and authentication.

Further, the numerous privacy issues that arise from the use of live FRT are compounded when the databases consist of data that are deemed sensitive or of a private (and not public) nature. For example, companies such as Clearview AI (that want governments to buy their services) may rely on the assumption that information on the Internet is 'public' information (akin to that obtained in a public space).[13] However, Canada's federal privacy commissioner (along with the privacy commissioners of Quebec, Alberta and B.C.) confirmed in February 2021 that social media profile information is not 'publicly available' in the context of private sector privacy law, demonstrating that FRT photo databases may be compiled in ways that violate our privacy rights in Canada.[14]

Canadians Divided on the Role of FRT

The Cybersecure Policy Exchange conducted a representative survey of 2,000 Canadian adults in May 2020 to gauge reactions to hypothetical uses of FRT.

Which of the following do you feel should be able to use facial recognition technology, like Clearview AI? (Select all that apply)



Your nearest town or city installs facial scanning cameras in all major intersections and begins using drivers' license photos to identify those breaking the law. Over the next three years, crime rates drop by 5%. Select the statement that best matches your views (Select all that apply):

48% **Significantly reducing crime is worth the loss of privacy**

36% **Despite the significant reduction in crime, it's not worth the loss of privacy**

02 Efforts to Limit the Use of FRT

The Context of a Temporary Prohibition on FRT

There have been significant developments in the last several years regarding the push for — and against — the use of FRT in Canada and the U.S. Major technology companies such as Amazon,[15] IBM[16] and Microsoft[17] released their FRT software for use starting in at least the mid-2010s. In the wake of this push, academic researchers,[18] civil liberties groups[19] and journalists[20] began reporting around 2018 on the legal and ethical risks that came with deploying such technology. Continued anti-FRT efforts led municipalities around the U.S. to ban city departments and police from using FRT in mid-2019.[21]

Then, in early 2020, news media reported that the data scraping and FRT company Clearview AI was working with over 2,000 governments, companies and individuals around the world.[22] By February 2020, it was reported that more than 30 law enforcement agencies in Canada accessed their software, with police officers running 3,400 searches across 150 accounts, relying only on free trials for access.[23] In the same month, several privacy commissioners in Canada began an investigation into Clearview AI for its collection and use of Canadians' personal information through image-scraping without consent.[24]

The murder of George Floyd has also served as a significant catalyst: the same tech giants that led the way with the uptake of FRT later publicly announced in mid-2020 that they would implement one-year "moratoriums" on police use of their FRT software.[25] In the European context, the European Commission has not yet ruled out the possibility of a temporary ban on certain uses of facial recognition technology.[26] The push in Canada to prohibit police from using FRT also came to a head in mid-2020, when a group of 77 privacy, human rights and civil liberties advocates called on Public Safety Minister Bill Blair to immediately "ban the use of facial recognition surveillance for all federal law enforcement and intelligence agencies."[27]

The Tech Informed Policy initiative released two policy briefings in August 2020, examining the implications for a broader Canadian moratorium on public sector use of FRT[28] and conditions under which the moratorium should be lifted.[29] The first of these briefings served as the basis of discussion for this roundtable event, which occurred about one week after news broke in Canada that a company behind some of Canada's biggest malls was collecting and analyzing's people's images without proper consent.[30]

Experts Divided: Responses to a Temporary Prohibition on FRT

The roundtable brought to light several types of responses to the idea of implementing a temporary prohibition in Canada on law enforcement's use of FRT, including those who:

1. **Support the prohibition**, based on the risks inherent in the use of FRT, and belief in the need to provide regulation or a policy framework *before* allowing or expanding the Canadian government's use of FRT;
2. **Reject the outright moratorium or prohibition** on public sector use of FRT, calling instead for greater oversight and governance of current and expanded use; and
3. **Push for increased definition and delineation** regarding the subject of prohibition and regulation, advancing a risk-mitigation approach.

Those who tended to support the proposal for a prohibition discussed the human rights issues raised by police use of FRT, including the importance of government transparency, and the rights to privacy and freedom from discrimination.

Those who challenged and rejected FRT prohibition tended to base their rationale on the potential for technological innovation and their trust in police in Canada to protect people's right to privacy. Others cited the cost and efficiency gains associated with automated decision-making. For example, one participant defended the benefits of police using facial recognition technology by stating, "Do you know how much it cost [sic] to solve one murder?"

A commonality in all three types of participant response was the importance of identifying, managing and mitigating the risks of harm that arise from public sector reliance on FRT, which we examine in further depth in the following sections.

03
Experts Weigh In: Mitigating Risks for the Use of FRT

The roundtable generated rich discussion on high-level and concrete solutions that could inform the management and mitigation of risks associated with FRT — before and during public sector organizations' use, or expanded use, of FRT. We used discourse analysis[31] to organize participants' contributions by types of policy issues and solutions for consideration.

Public Consultation, Transparency and Trust

Participants highlighted that there is a need for more transparency around when or how FRT is being used by Canadian government and law enforcement agencies. They also mentioned that government agencies should engage in public consultation on the foreseeable and current uses of FRT and regulations on its use, and agencies should be required to publish lists of FRT software in use.

Public consultation should occur before and during a government organization's (including law enforcement's) initial or expanded use of FRT software. The purpose would be to assess the public's perception of the benefits and costs of the software, and to facilitate transparency, and ensure trust and confidence in the use of such technology by the public sector in Canada.

Auditing and Risk Analysis

Participants identified the need for public sector organizations to undertake cost-benefit analysis on the use of FRT before they use such technology. For the experts we consulted, it is critical to understand and analyze the actual benefits gained from the use of FRT, in order to understand whether using such technology is worth the risks it poses. Some pointed to the Government of Canada's Algorithmic Impact Assessment as an example.[32]

Analysis of benefits could involve identifying an agency's mandate, concrete goals to achieve those mandates, and assessment of whether the use of FRT has been proven to achieve similar or identical goals. Participants identified the risks that could be audited and assessed, including:

- **Inaccuracy and the probability of false positives** (in the context of law enforcement, this could include wrongful convictions, which can cost the government millions[33]).
- The FRT software's potential for **breaches of constitutionally protected rights**, such as the right to freedom from unreasonable search and seizure, as well as discrimination on the basis of gender, sex, race, ethnicity, sexual orientation, etc.[34]
- The impact on the **security and privacy of data** for individuals and organizations that use the FRT software, with a particular focus on two major security risks associated with FRT:
  1. **Possibility of theft or unauthorized data access** involving highly sensitive data that identifies individuals; and
  2. **Data spoofing or manipulation** where FRT software can be "fooled" or deceived through the use of fake or copied biometric information, which can amount to identity theft or fraud.

Participants identified a non-exhaustive list of the following potential data security and privacy requirements for public sector use of FRT:

- Canadian privacy and criminal law should **account for the existence of biometric data and provide extra security protection**, a data type which currently remains unacknowledged and under-protected.
- There should be a general presumption **against the processing of biometric data** of any entity **except in specific circumstances.**
- When instances of **FRT data misuse or breaches** occur, there should be requirements to **notify** those involved and/or the general public.

Improved Procurement Processes for Accountability

Participants observed that there is significant room for improvement in the current process that governments use to procure software such as FRT. At a high level, participants envisioned the possibility for increased accountability measures, to be grafted onto government procurement practices.

More specifically, they flagged that improved accountability could include improved or additional audit, security, accuracy and bias assessments of procured technology. They stated it could also include lowering the minimum monetary threshold for the public disclosure of contracts, and implementing open data and contracting measures to facilitate meaningful accountability.

One expert stated that a solution could include prohibiting the use of free software trials by individuals or groups of employees at government or law enforcement agencies — a regulatory gap that was exploited by Clearview AI, which previously offered free trials to individual police officers at various police forces in Canada.[35]

User Training

Some public employees stated that they're looking for better governance and more guidance from lawmakers in Canada on their use of FRT. For example, one Canadian law enforcement official told the participants that "overall, this [facial recognition] technology requires a lot more governance around it," and that Canada's federal, provincial and municipal levels "need alignment; there needs to be overarching policies and best practices that can be leveraged" by law enforcement that use FRT in Canada.

To this end, we believe it would be important to provide robust training for law enforcement and government workers who (directly or indirectly) use FRT software for their decision-making processes.

Use Limits

One panelist highlighted the importance of setting limits on the types of images that law enforcement should be allowed to submit when using FRT software or service providers. For example, the ability for law enforcement to conduct searches with edited or altered images, or images that approximate the appearance of the accused — tactics used by police in the U.S. to quickly return results.[36] For example, one expert uncovered that an FRT company working for the NYPD uploaded a photo of Woody Harrelson for a database search in order to generate investigative leads because of his resemblance to the accused.

Our event participants observed that there are other limits that policymakers in Canada should consider implementing in order to mitigate the risks that could arise from reliance on FRT, particularly when it comes to the need to protect Canadians' ability to consent to the use and collection of their data. Participants encouraged policymakers to consider the following types of solutions and answers to related questions:

- The need to limit **the circumstances in which** police can rely on FRT:
    - Should police be allowed to use live FRT to identify people in **real time** and on the spot (e.g., in the public, at an event, on social media)?
    - Should law enforcement be required to **obtain a warrant** to use FRT software in the context of an investigation, similar to the Criminal Code provisions regarding forensic DNA analysis? Would this curtail the use of real-time FRT?
    - When **certain crimes** are involved:
        - Should there be a certain threshold that must explicitly be met in order for law enforcement to be allowed to use FRT for the identification of an accused person (e.g., crimes involving physical violence, terrorism, etc.)?
        - Should the public be made aware of this threshold?
        - Would setting a threshold incentivize police to search for evidence of more serious crimes when they did not necessarily occur?
- The need for limits on **the types of databases** that can be used:
    - Should law enforcement be allowed to use image search engines like Google for their investigations? Do they already do this? What are the parameters?
    - Should police be allowed to use the services of FRT companies like Clearview AI, which scrape and compile Internet and social media images? What are the parameters?
    - What other types of image databases should be prohibited or limited in use (e.g., driver's licence databases)?
- The need to limit **how** prosecutors and judges can rely on FRT software and the results of its data analysis:
    - Should FRT only be used for positive identification of the accused in tandem with the totality of other available evidence (e.g., direct, circumstantial, forensic evidence, etc.)? Should relying on FRT database evidence alone for the positive identification of a person be significantly limited or curtailed?
    - Before such evidence potentially makes its way before a court, how should standards of proof in criminal procedure (e.g., requirement for reasonable suspicion) inform a judge's decision to admit evidence about an accused person's identity that is informed by FRT?

Conclusion

Finally, many of our event's participants highlighted the need for various kinds of work to be done in pursuit of any prohibition in Canada on public sector use of FRT, as well as on the expanded use of FRT by law enforcement and other bodies. In particular, participants flagged the need for increased policy research and activation around the private sector's use of FRT in Canada.

Other participants called for the mitigation of risks associated with FRT, with the assumption that its continued implementation in the public sector is inevitable or desirable. We echo the experts who stated that risk-oriented research and scenario analysis at the departmental level is sorely needed, as well as government-wide and society-wide engagement.

We thank all the experts who attended our roundtable event and contributed their valuable insights. As eloquently stated by one of our participants, "Canada has the opportunity to take a lead on the rollout of such policies" related to the governance of facial recognition technology. It is clear that increased public sector use of facial recognition technologies needs to be carefully — yet swiftly — regulated as a matter of security and privacy; and in order to facilitate accountability for both the public and private sectors' use of our highly sensitive and biometric personal data.

Appendix: About the Event

Held on November 10, 2020, the Cybersecure Policy Exchange at Ryerson University and Tech Informed Policy at McGill University co-organized a policy roundtable to bring together expert stakeholders under Chatham House Rules, to weigh in on the implications of a prohibition on the use of facial recognition technology by public sector organizations in Canada.

Law enforcement's use of FRT was a dominant theme in the event's opening roundtable panel and breakout discussions, likely influenced by two of the opening panelists working in law enforcement.

Roundtable participants included:

- Federal and provincial government officials;
- Academics and researchers;
- Civil society advocates;
- Lawyers;
- Law enforcement officials; and
- People working for technology companies, including FRT companies.

A list of participants (who consented to having their names made publicly available) is as follows:

David Abrahamson, Captain, Portland Police Bureau
NM Amadeo, Co-Founder, Coalition for Critical Technology
Vass Bednar, Executive Director, Master of Public Policy in Digital Society Program, McMaster University
Asia Biega, Tenure Track Faculty, Max Planck Institute for Security and Privacy
Ana Brandusescu, 2019-2021 McConnell Professor of Practice, Centre for Interdisciplinary Research on Montreal, McGill University
Fred Carter, Senior Policy & Technology Advisor, Information and Privacy Commissioner of Ontario
Michelle Chibba, Research Associate, Privacy and Big Data Institute, Ryerson University
Rumman Chowdhury, CEO, Parity
Noel Corriveau, Senior Counsel, INQ Data Law
Clare Garvie, Senior Associate, Center on Privacy and Technology, Georgetown Law
Kevin Haskins, Senior Sales Director, Clearview AI
Rim Khazall, Analyst for Responsible AI, Treasury Board of Canada Secretariat
Ritesh Kotak, Speaker and Digital Strategist in Cybersecurity
Ian Mann, Senior Director & Head of Identity and Access Management Strategy, Royal Bank of Canada
Ellie Marshall, Privacy lawyer (participating in personal capacity)
Brenda McPhail, Director of Privacy, Technology & Surveillance, Canadian Civil Liberties Association
Cathy O'Neil, CEO, O'Neil Risk Consulting & Algorithmic Auditing
Ngozi Okidegbe, Assistant Professor of Law, Cardozo School of Law
Daniel Ribi, Policy Advisor, Information and Privacy Policy Division, Treasury Board of Canada Secretariat
Sherry Rumbolt, National Information System Security Officer, Department of National Defence
Katherine Rusk, Associate, Osler, Hoskin & Harcourt LLP
Spencer Russell, Policy Analyst, Public Safety Canada
Teresa Scassa, Canada Research Chair in Information Law, University of Ottawa
Dana Somerville, Policy Analyst, Border Law Enforcement, Public Safety Canada
Vincent Southerland, Executive Director for the Center on Race, Inequality and the Law, NYU School of Law
Luke Stark, Assistant Professor, Faculty of Information and Media Studies, University of Western Ontario
Ian Williams, Head of Analytics and Innovation, Toronto Police Service
Donna Young, Dean, Ryerson University Faculty of Law

References

[1] Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, "Facial Recognition Briefing #1" (August 2020), TIP – Tech Informed Policy, online: http://techinformedpolicy.ca/facial-recognition-briefing-1/

[2] Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun & Kate Gilbert, "Facial Recognition Briefing #2" (August 2020), TIP – Tech Informed Policy, online: http://techinformedpolicy.ca/facial-recognition-briefing-2/

[3] Owen et al, supra note 1.

[4] Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto, online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

[5] Owen et al, supra note 1.

[6] Ibid.

[7] Robertson, Khoo, and Song, supra note 4.

[8] Ibid.

[9] Betsy Powell, "How Toronto police used controversial facial recognition technology to solve the senseless murder of an innocent man", *The Toronto Star* (13 April 2020), online: https://www.thestar.com/news/gta/2020/04/13/how-toronto-police-used-controversial-facial-recognition-technology-to-solve-the-senseless-murder-of-an-innocent-man.html

[10] Alison Brooks, "Law Enforcement Information Management Study" (October 2014) IDC at 12-22, online: https://cacp.ca/index.html?asst_id=977.

[11] Robertson, Khoo, and Song, supra note 4.

[12] Information Commissioner's Office, "ICO investigation into how the police use facial recognition technology in public places" (October 2019), Information Commissioner's Office, online: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

[13] CBS News, "Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement", CBS News (5 February 2020), online: https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/

[14] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Report of Findings #2021-001, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[15] Elizabeth Dwoskin, "Amazon is selling facial recognition to law enforcement — for a fistful of dollars", *The Washington Post* (22 May 2018), online: https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/

[16] Katherine Noyes, "In this online demo, IBM's Watson will tell you what's in your photos", *Computerworld* (21 March 2016), online: https://www.computerworld.com/article/3046451/try-this-online-demo-and-ibms-watson-will-tell-you-whats-in-your-photos.html

[17] Hannah Jane Parkinson, "Happy? Sad? Forget age, Microsoft can now guess your emotions", *The Guardian* (11 November 2015), online: https://www.theguardian.com/technology/2015/nov/11/microsoft-guess-your-emotions-facial-recognition-software/

[18] Larry Hardesty, "Study finds gender and skin-type bias in commercial artificial-intelligence systems", *MIT News* (11 February 2018), online: https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[19] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", *American Civil Liberties Union* Blog (26 July 2018), online: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

[20] Sam Levin, "Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says", *The Guardian* (26 July 2018), online: https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu

[21] Jillian D'Onfro, "This Map Shows Which Cities Are Using Facial Recognition Technology — And Which Have Banned It", *Forbes* (18 July 2019), online: https://www.forbes.com/sites/jilliandonfro/2019/07/18/map-of-facial-recognition-use-resistance-fight-for-the-future/

[22] Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart And The NBA," *BuzzFeed News* (27 February 2020), online: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

[23] Ibid.

[24] Office of the Privacy Commissioner of Canada, "Announcement: Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology", *Office of the Privacy Commissioner News & Announcements* (21 February 2020), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/

[25] Larry Magrid, "IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology", *Forbes* (12 June 2020), online: https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/

[26] Samuel Stolton, "Commission will 'not exclude' potential ban on facial recognition technology", *EURACTIV* (3 September 2020), online: https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/

[27] Amnesty International, "Open Letter: Canadian Government Must Ban Use of Facial Recognition Surveillance by Federal Law Enforcement, Intelligence Agencies", *Amnesty International Canada News* (8 July 2020), online: https://amnesty.ca/news/open-letter-canadian-government-must-ban-use-facial-recognition-surveillance-federal-law

[28] Owen et al, supra note 1.

[29] Owen et al, supra note 2.

[30] Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia, 2020 CanLII 83156 (PCC), online: http://canlii.ca/t/jbcq8

[31] Teun A van Dijk, "Editor's Introduction: The Study of Discourses: An Introduction: The Emergency of a New Cross-Discipline" in Teun van Dijk, ed, Discourse Studies (London, UK: Sage, 2007) 1.

[32] "Algorithmic Impact Assessment (AIA)", Government of Canada — *Responsible Use of Artificial Intelligence*, online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

[33] "Other settlements for the wrongly convicted", *The Globe and Mail* (16 February 2007), online: https://www.theglobeandmail.com/news/national/other-settlements-for-the-wrongly-convicted/article679186/

[34] Robertson, Khoo & Song, supra note 4.

[35] Catharine Tunney, "RCMP denied using facial recognition technology — then said it had been using it for months", CBC News (4 March 2020), online: https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266

[36] Russell Brandom, "The NYPD uses altered images in its facial recognition system, new documents show", *The Verge* (16 May 2019), online: https://www.theverge.com/2019/5/16/18627548/nypd-facial-recognition-altered-faces-privacy

cybersecure
policy
exchange
Powered by RBC

TIP TECH INFORMED POLICY