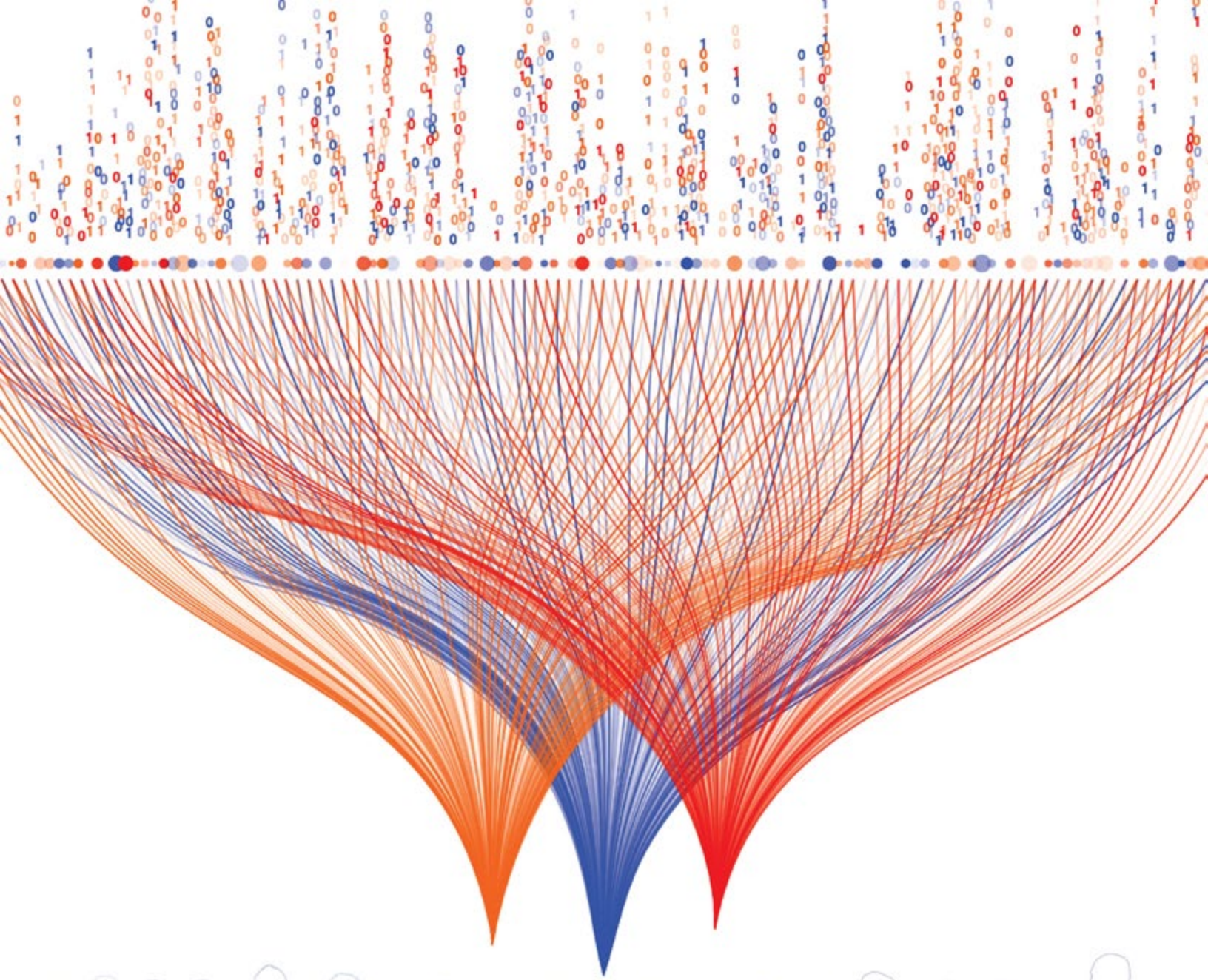


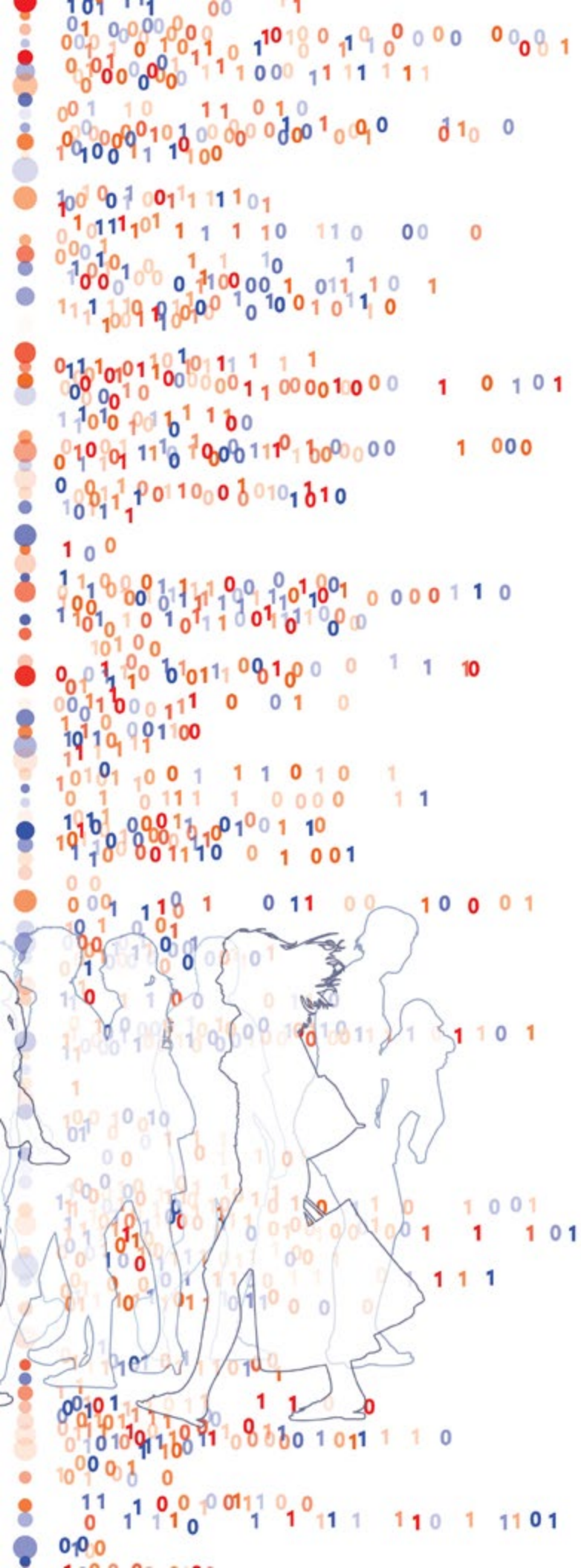
Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT

Law Enforcement Use of Facial Recognition Technology: Vancouver Roundtable Report

December 2025

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO



About the Law Commission Of Ontario

The Law Commission of Ontario (LCO) is Ontario's leading law reform agency.

The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based legislation and policies, and public engagement on important law reform issues. The LCO is independent of stakeholder interests and is committed to a public interest perspective for every project.

Recent LCO reports and submissions addressing AI issues include:

- Human Rights AI Impact Assessment (with the Ontario Human Rights Commission, 2024)
- Submission to Government of Ontario Re Bill 194 (2024)
- *Accountable AI* (2022)
- *Regulating AI: Critical Issues and Choices* (2021)
- *Legal Issues and Government AI Development* (2021)
- The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada (2020)

More information about the LCO and this project is available at: https://www.lco-cdo.org.

Author

Ryan Fritsch, Counsel
Law Commission of Ontario

Disclaimer

The analysis, findings, and recommendations in this paper do not necessarily represent the views of the LCO's funders, supporters, Advisory Committee members, or Issue Paper authors.

Contact

Law Commission of Ontario
2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, ON, M3J 1P3

Tel: (416) 650-8406
E-mail: LawCommission@lco-cdo.org
Web: https://www.lco-cdo.org
LinkedIn: https://linkedin.com/company/lco-cdo
Bluesky: @lco-cdo.bsky.social
Twitter: @LCO_CDO
YouTube: @lawcommissionofontario8724

Funders

The LCO is funded by the Law Foundation of Ontario, Law Society of Ontario, and Osgoode Hall Law School. Funding for the Vancouver Roundtable was provided by the Law Commission of Canada.

How To Read This Event Report

This report summarizes key themes and issues discussed at the LCO's Roundtable on Law Enforcement Use of Facial Recognition Technology, convened in Vancouver on June 26, 2025. As an event report, please consider the following:

- This report summarizes the full range of themes discussed. It does not necessarily reflect the priority or extent of discussion given to any particular theme.
- The summaries reflect the range of views expressed around the discussion table. No position or opinion should be ascribed to any particular participant, be interpreted as a consensus view, or be understood as representative of any final conclusion or recommendation.
- This report does not reflect the conclusions of the LCO. The LCO's AI in Criminal Justice Project will conclude in early 2026 with publication of a Final Report containing a range of law and policy reform recommendations.

Introduction

There is considerable and growing interest within Canadian governments and law enforcement agencies to adopt and deploy facial recognition technology (FRT).

The Law Commission of Ontario (LCO) and many others believe police FRT is a current and important public safety, human rights, and law reform issue. Many artificial intelligence (AI) technologies have potential to improve public safety, improve police investigations, and improve the efficiency and fairness of criminal proceedings. Many AI technologies also appear to have potential to address, at least in part, long-standing concerns about racialized criminal justice and access to justice.

Notwithstanding its potential benefits, the use of AI in criminal justice is controversial. Biometric technologies like FRT have been harshly criticized in many jurisdictions for their impact on racialized and low-income communities, constitutional and human rights, criminal procedure, criminal common law principles, privacy, and access to justice.

Canadian police interest in, and deployment of, FRT appears to be increasing. The LCO's AI in Criminal Justice Project documents known and proposed uses of FRT by law enforcement agencies in Canada, and the accelerating adoption and use of FRT in jurisdictions outside of Canada.

The LCO Project also identifies police FRT questions that are, or soon will be, confronting Canadian police services, courts, and policymakers.

On June 26th, 2025, the LCO brought together a broad range of FRT stakeholders in Vancouver for a frank and collaborative roundtable discussion about FRT benefits, risks, deployment, legal issues, and governance. This report summarizes the Roundtable's key themes and issues discussed.

The LCO Vancouver FRT Roundtable was the first of two LCO roundtables on criminal justice AI issues. A second roundtable on AI Evidence in Criminal Proceedings was held in Toronto on August 14th, 2025. The Toronto Roundtable report and other materials are available on the project website.

The Vancouver Roundtable is part of the LCO's AI in Criminal Justice Project, a groundbreaking survey and analysis of the opportunities, risks, and law reform issues regarding AI in the Canadian criminal justice system. Working together, the LCO and our collaborators believe the LCO project and Vancouver Roundtable are an important contribution towards developing "Trustworthy Criminal AI" in the Canadian justice system.

The LCO's AI in Criminal Justice Project

The LCO AI in Criminal Justice Project is a collaboration of leading practitioners and experts in Canadian criminal justice system. Project authors and advisors include representatives from governments, police services, Crowns, the criminal defence bar, courts administration, legal aid, human rights commissions, civil society organizations, and academics.

In April 2025, the LCO released a project introduction/summary and four Issue Papers. Each Issue Paper considers AI in a distinct phase of the criminal justice process:

Paper 1 Introduction and Summary

Paper 2 Use of AI by Law Enforcement

Paper 3 AI and the Assessment of Risk in Bail, Sentencing, and Recidivism

Paper 4 AI at Trial and on Appeal

Paper 5 AI and Systemic Oversight Mechanisms in Criminal Justice.

The LCO Criminal AI Project is organized around four key themes or topics.

First, the project considers important practical and legal questions that will soon confront Canadian police, courts, policymakers, Crowns, defence counsel, and accused, including:

- What AI tools could be used at each important stage of Canadian criminal justice?
- What legal issues are likely to arise at each stage?
- What is the state of Canadian law to address these issues?

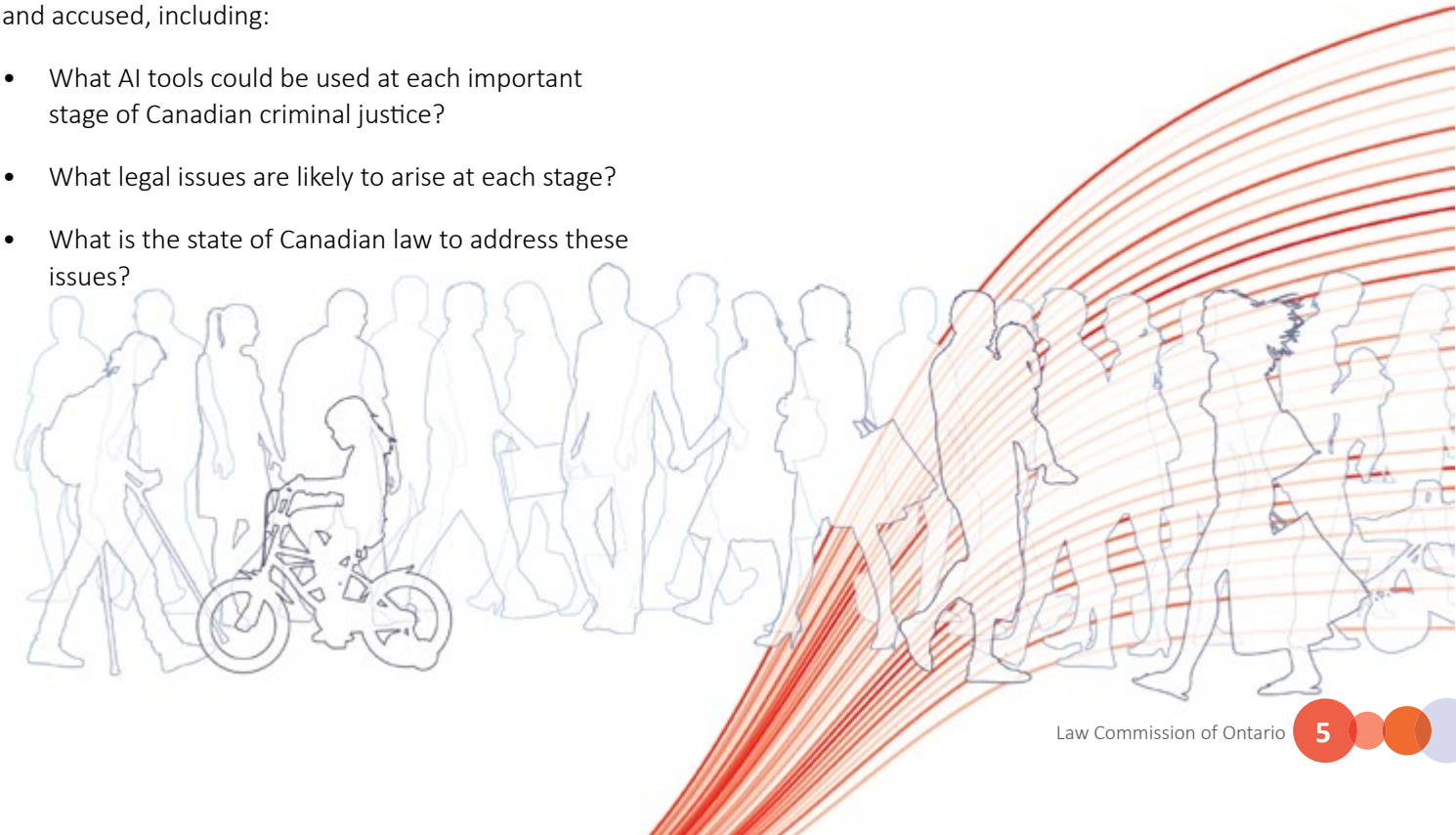
Second, who is likely to be affected by AI in the criminal justice system? What institutions, agencies, organizations, or individuals will be affected?

Third, the project surveys potential solutions at the specific and systemic level, including:

- What we can learn from other jurisdictions that have confronted these issues?
- How Canadian policymakers, courts, and others have responded to AI systems?
- Are there gaps in Canada's current criminal AI regulatory landscape?

Finally, the project tries to foreshadow or predict what is likely to happen in Canadian criminal justice if action is not taken.

All project papers and background materials are available on the LCO website. Detailed background information on FRT practices, policies, and a comparative look at experiences in other jurisdictions is found in the second LCO Criminal AI Project Paper, ***Use of AI by Law Enforcement,*** written by LCO Policy Counsel Ryan Fritsch.



Organization of the Roundtable

The Vancouver Roundtable brought together a broad range of stakeholders for a frank and collaborative roundtable discussion about FRT benefits, risks, deployment, legal issues, and governance. The Roundtable was participatory, constructive and solution-oriented. Participants included representatives from federal and municipal law enforcement, private bar and legal aid defence counsel, provincial human rights and privacy agencies, academics, and public interest advocates.

The half-day discussion was organized into four themes, which were identified by Roundtable participants prior to meeting. Each topic was introduced by leading practitioners and then discussed by the group. Topics discussed included:

Introduction to Police FRT/Biometrics and Stakeholder Perspectives.

- Why are police interested in FRT/biometrics?
- What are potential applications of the technology?
- What are the perceived benefits, risks, and objectives?
- What issues concern defence counsel, public interest groups, and oversight agencies?
- What can be learned from the experience of other jurisdictions?

Validity, Reliability, Bias and Discrimination.

- How are FRT systems validated and calibrated and to what standard?
- What data sources are lawful for FRT training?

Lawful Authority and Procedural Fairness.

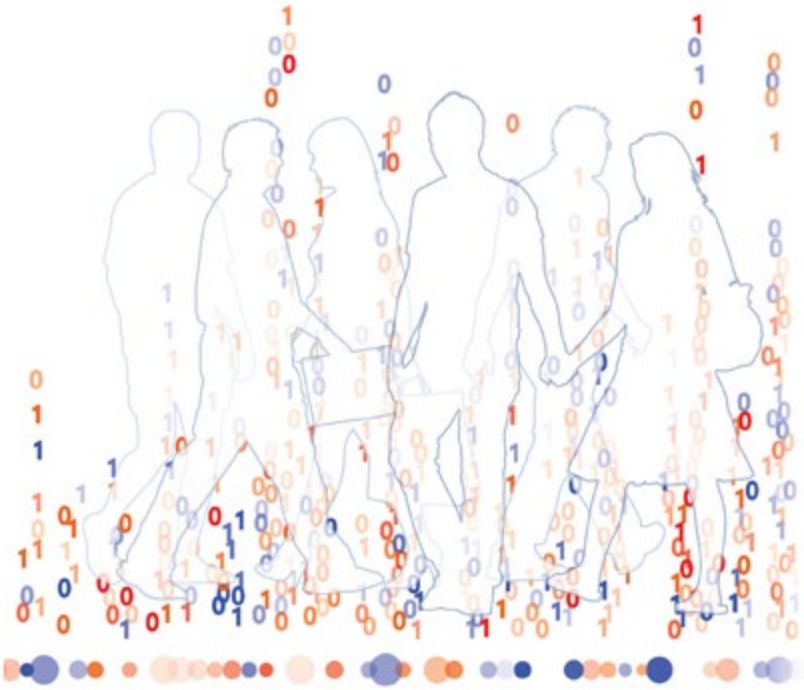
- What are the sources or conditions that trigger lawful authority to use FRT?
- Does Canadian law create presumptive prohibitions on FRT use?

Public Disclosure and Systemic Oversight.

- Does FRT use require public disclosure and reporting?
- Do existing oversight mechanisms create an effective check and balance?
- How can police services, oversight agencies or governments support effective public participation in FRT governance?

The Roundtable was conducted under the Chatham House Rule. Participants were free to share their comments and questions without direct quotation or attribution. This report is consistent with the Chatham House Rule.

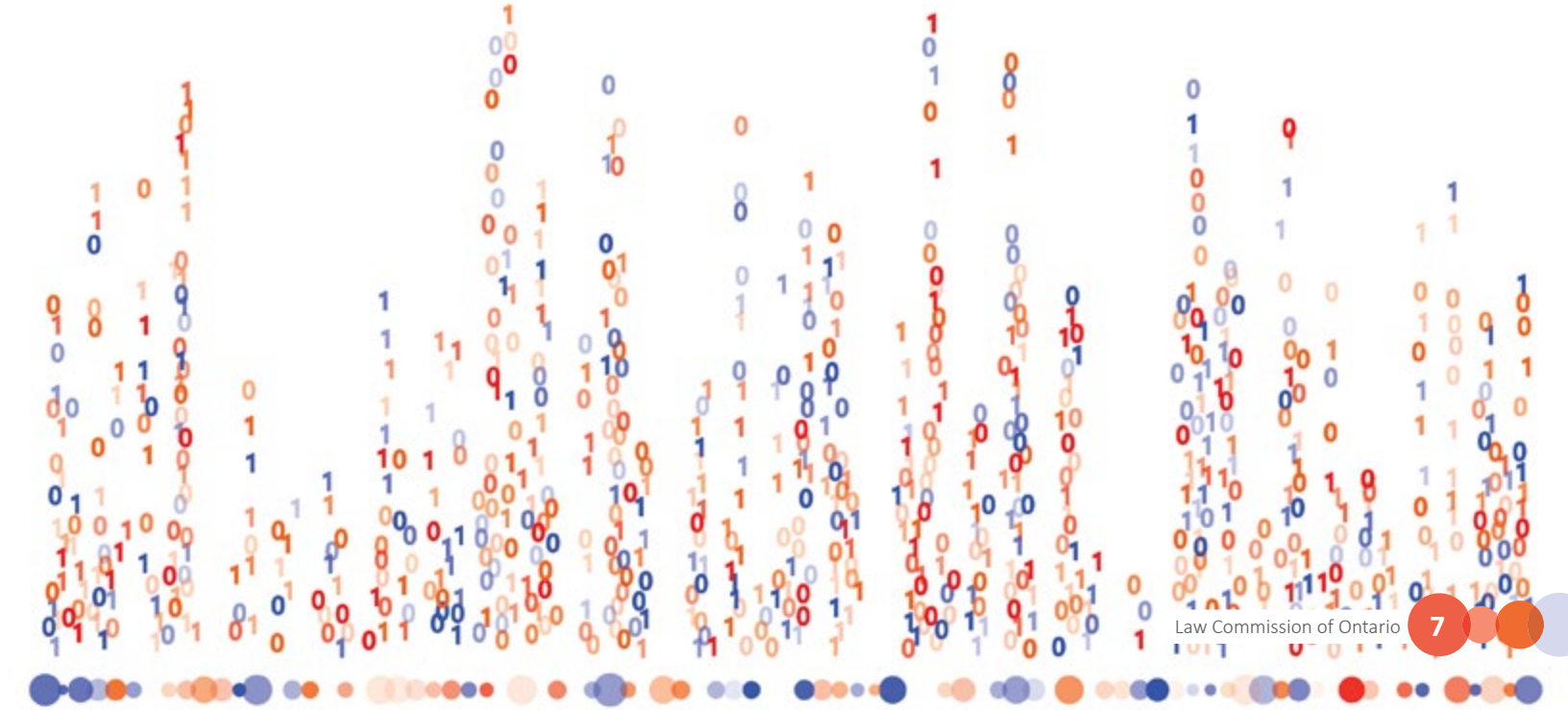
A list of background materials distributed to Roundtable participants is attached to the end of this report.



Roundtable Themes and Insights

The roundtable generated many ideas and recommendations. The table below summarizes 10 key themes and insights. These themes and insights are discussed in more detail in the sections that follow.

FRT Roundtable Theme	*Insight*
1. *Police services see benefits and risks in using FRT.*	Police services believe FRT may greatly expedite the investigation and identification of criminal suspects, missing or trafficked persons, and children at risk of online sexual exploitation. Police services understand the risks and public concerns about FRT and agree that police FRT use must be lawful and trustworthy.
2. *FRT adoption is uneven.*	FRT has not been widely adopted by Canadian police services. There are wide variations in interest, capacity and use of FRT across the country. Larger services may have the resources to support FRT adoption, smaller services will likely need help.
3. *There are many forms of FRT governance. Police policies are a good place to start.*	Police services agree successful FRT adoption depends on robust, transparent and participatory governance. Governance can take many forms. Police services should not wait for FRT legislation. Several police services have developed AI or FRT policies and procedures. These policies are important first steps. Model AI and FRT policies could promote consistent and thoughtful police practices across Canada.
4. *FRT governance must reflect Canadian law.*	FRT governance must reflect and proactively apply Canadian law. This will better ensure FRT use is legal, reflects Canadian and local values, and is more likely to be accepted in court.
5. *FRT governance must be risk-based.*	Not all FRT applications are the same. A "one size fits all" FRT governance model is unlikely to be effective or reflect Canadian law. Risk-based governance is needed to differentiate FRT applications, tailor governance requirements, and align with baseline requirements for all AI systems.



FRT Roundtable Theme	*Insight*
6. *Canadian privacy and evidence law should be updated to address FRT issues.*	Canadian privacy law must be updated to reflect the legal and operational complexities of FRT, including updated expectations of privacy and the rules for storing images. Similarly, Canadian criminal evidence law could adopt higher thresholds for FRT admissibility and updated tests for novel and scientific evidence.
7. *Presumptive AI "red lines" and authorized uses are important regulatory standards.*	A thoughtful list of presumptive AI "red lines" or prohibitions could prevent overbroad use of FRT. Similarly, it would be helpful to list the applications or criteria to authorize lawful FRT, including when FRT could be used legally in exceptional circumstances. Any such list must reflect differences in police service mandates and responsibilities.
8. *Thoughtful policies can foster responsible FRT adoption.*	Governance and procurement policies can promote responsible and consistent police FRT deployment. For example, it would be helpful if police services could purchase FRT systems that were "certified" or pre-tested to meet requirements for reliability and validity, human rights, bias and privacy.
9. *Public accountability is essential for FRT adoption and public trust.*	Successful police FRT adoption depends on public understanding and credibility. Public reporting and transparency are necessary to ensure public trust. At present, there is little public awareness of the "footprint" or impact of law enforcement FRT systems in Canada.
10. *Oversight of police FRT systems could be coordinated more effectively.*	Several factors currently limit the effectiveness of police FRT oversight, including the need for dedicated police AI and FRT impact assessments, the need for skilled "humans-in-the-loop" to evaluate FRT outputs and systems, and the need for provincial policing standards to support model police AI and FRT-related practices and policies.

Roundtable Themes and Insights — Discussion

1. Police Services See Benefits And Risks In Using FRT.

Roundtable participants agreed that FRT technology may greatly expedite the investigation and identification of criminal suspects, missing or trafficked persons, and children at risk of online sexual exploitation.

Participants stressed that policymakers and the public had to appreciate that there are many potential applications of FRT in Canadian policing. As the LCO has noted:

> *FRT and biometric systems can be used for many purposes and in many contexts, including:*
>
> - *To support criminal investigations, including terrorist threats; investigations for missing persons children, human trafficking or sexual exploitation; public order events; etc.*
> - *To scan mugshot databases.*
> - *To provide surveillance in public, private, or secure spaces.*
> - *For real-time personal identification through police body cams or drone videos.*
> - *To analyze images or video collected by third parties.*[1]

Some of these applications are currently in use. For example, the RCMP has publicly stated it uses FRT technology in investigations "for processing, sorting and analyzing large volumes of images and videos" that can number in the hundreds of thousands, including convincing AI-generated images intermingled with photos of real victims.[2]

Participants agreed that investigative and surveillance benefits will only be achievable where evidence has been lawfully obtained and other risks are properly managed. For instance, the RCMP has acknowledged how inappropriate FRT use may "adversely impact privacy and other fundamental rights, such as risks associated with unintended data biases and false identifications," among broader "concerns for the Canadian public."[3] The RCMP also acknowledged that "these types of operational technologies will only be used under specific circumstances in accordance with RCMP policies and Canadian law."[4]

2. Police FRT Adoption Is Uneven.

Despite general interest, very few police services in Canada have deployed FRT systems. LCO's Project Paper 2, ***Use of AI by Law Enforcement***, documents the handful of police agencies in Canada who have adopted FRT technology or announced an intention to do so. This includes the RCMP, the Vancouver Police Department, and the York and Peel Regional police services. Among these, only the York and Peel regional police forces in Ontario have implemented a policy specific to governing the operation of FRT systems.[5]

Roundtable participants stressed that the speed, scale, and potential applications of police FRT are not uniform across Canada. They emphasized that police services often have different mandates, internal capacity, and resourcing. For example, while larger services may have the legal, governance, policy, and administrative capacity to support FRT technology, smaller services will likely need help to ensure high standards of practice and responsible use of the technology.

Local factors, such as warrant application practices or different oversight expectations, may also mean FRT is adopted at different paces, with different rules, and for different applications across the country.

3. There Are Many Forms of FRT Governance. Police Policies Are A Good Place to Start.

Roundtable participants agreed that police services recognize the potential benefits of FRT depend on earning the public's confidence and ensuring robust, transparent and participatory governance. That said, there are many forms of police FRT governance, including legislation, provincial policies or regulations, and dedicated police service policies.

Participants noted that there is currently no dedicated federal or provincial legislation governing law enforcement AI or FRT systems. It was agreed that police services should not wait for FRT legislation and that dedicated police service policies were a good place to start.

Roundtable participants noted that many Canadian police services have taken important first steps to build AI accountability frameworks. Among the leading examples are the RCMP's National Technology Onboarding Program; the Toronto Police Services Board Use of AI Technology policy; and the York and Peel Regional Police Use of the Facial Recognition System policy, the first of its kind in Canada.

It was agreed these policies are important steps. Participants noted, however, that these initiatives tended to be developed locally without the benefit of wider direction or coordination amongst police services. As a result, early AI and FRT governance policies are inconsistent in important respects, including:

- Definitions of key terms and technology.
- Scope of application.
- Reporting structures.
- Legal authorization and review.
- Public accountability, including reporting, data collection and analysis.
- Public participation in FRT policy development and oversight.

Once again, participants stressed that police services across the country range widely in terms of size and capacity. There are, for example, 53 police services in Ontario. Many, perhaps most, police services in the country do not have the resources or staff to develop sophisticated FRT policies internally.

It was broadly felt that through leadership and coordination, there is an opportunity for model policies to engage the public and align local and national practices around high standards of accountability. Various agencies were suggested as potentially facilitating this work, including the Canadian Association of Chiefs of Police; the Ontario Association of Chiefs of Police; police board associations; provincial civilian oversight and police misconduct agencies; provincial inspectors general for policing standards; and the Advisory Council on Policing Standards.

4. FRT Governance Must Reflect Canadian Law.

Many police services have studied police FRT governance policies in other jurisdictions. Participants agreed, however, that police FRT governance must reflect and proactively apply Canadian law. This is necessary to better ensure FRT uses are legal and justiciable; to reflect Canadian public values and expectations; and to avoid long and costly criminal trials that may result in wrongful convictions or deem technology legally unsound.

At the same time, it was recognized that this is no easy task. Many existing and familiar sources of law – including Canada's ***Charter of Rights and Freedoms***, the ***Criminal Code of Canada*** and criminal procedure, federal and provincial human rights codes, federal and provincial privacy legislation, evidence law, and criminal common law precedents – will apply to FRT technology.

Participants agreed, however, that it is not self-evident how Canadian legal rules and requirements can be operationalized. Several participants noted the benefit of having stakeholders discuss these issues

collaboratively in advance before widespread adoption of the technology.

Participants discussed the need for some kind of dedicated impact assessment to evaluate police AI and FRT systems against Canadian criminal and constitutional law. It was noted that privacy assessments are well established for AI systems, but human rights or criminal law impact assessments are not. It was agreed that tools to promote FRT "compliance by design" by would be beneficial. The LCO and Ontario Human Right Commission's recent AI Human Rights Impact Assessment was cited as a good but general precedent.

Finally, it was emphasized that important lessons can be learned from legislation in other jurisdictions. For instance, the European Union's 2024 Artificial Intelligence Act codifies several issues discussed at the Vancouver Roundtable, including:

- Presumptive prohibitions on general use of mass biometric technology including FRT.
- Describing circumstances or exigent circumstances that authorize FRT use.
- Describing when for judicial authorization is required.
- Public reporting and transparency requirements.

5. FRT Governance Must Be Risk-based.

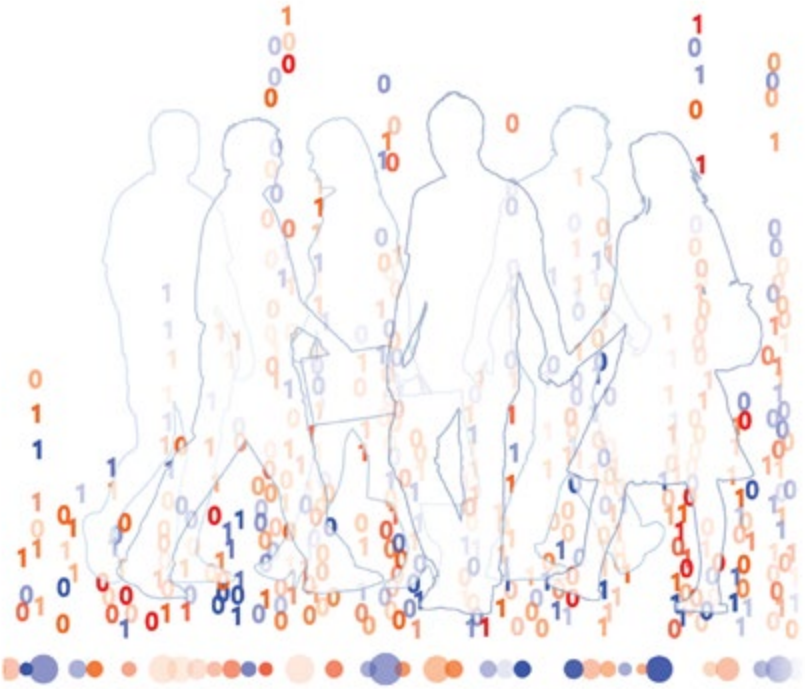
Not all FRT applications are the same.

As the LCO has written,

> *…it is important to note important variations and distinctions between and within policing FRT systems. These distinctions can have wide ranging implications for public safety, police investigations, and individual rights. For example, one of the major concerns about FRT systems is the risk of mass, untargeted, or unjustified surveillance. Surveillance risks are present in all FRT systems, but the scope of that risk depends in part on the potential source of FRT probe and reference images. Sources of FRT probe images could include public or private security cameras, police body cameras, drones, or home security cameras. Potential sources of FRT reference images could include mugshot databases, specialized police databases, internet scraping, or even driver's license pictures. There is also an important distinction between real-time FRT (live face recognition or LFR) and FRT systems used retrospectively (post-event facial recognition).*[6]

As further discussed in theme six below, the context in which an FRT system is deployed or operationalized will affect different legal rights, protections, and prohibitions.

As a result, participants agreed that a "one size fits all" approach to FRT governance is unlikely to reflect Canadian law or be effective. Participants agreed that a risk-based governance model is needed to differentiate FRT applications and tailor governance requirements and performance standards accordingly. This approach will promote more effective FRT adoption, better ensure compliance with Canadian law, and promote public trust.



6. Canadian Privacy and Evidence Law Should be Updated to Address FRT Issues.

Participants discussed how Canadian privacy law needed to be updated to reflect FRT's legal and operational complexities, including:

- The reasonable expectation of privacy in public.
- The reasonable expectation of privacy in images collected for non-investigative purposes.
- The rules for storing images.

Similarly, it was generally agreed that Canadian evidence law had to be updated to account for new issues driven by FRT, including the potential need to adopt higher thresholds for admissibility, the need for rules to address AI-enhanced and AI-generated images, and the need to update tests for novel and scientific evidence.

Participants noted there are many complex challenges to be overcome. For instance, the ease with which AI systems can link otherwise innocuous and disparate pieces of information to create profiles and track activities (as recently adjudicated by the Supreme Court in R. v. Bykovetz) raises practical problems in balancing privacy rights with expedited criminal procedures such as applications for judicial authorization. Participants also discussed if or how warrant application procedures should be updated in light of the technology and a potential increased in applications.

Limitations on the authority of existing AI assessment procedures may continue to grow and create more regulatory oversight "gray zones." For instance, some suggest a trend in which more investigations in organized crime, drug and human trafficking, and border enforcement are related to "national security services," triggering an exemption from the federal Algorithmic Impact Assessment and reporting requirement.

Other recent research suggests a need to consider regulating biometric identification more broadly than just FRT. For instance, in jurisdictions where FRT prohibitions are in place, law enforcement agencies may instead resort to sophisticated object recognition systems to correlate other personal details that may identify and track an individual in real time, such as types of colors of clothing, worn accessories, and stature.[7]

7. AI "Red Lines" And Authorized Uses Are Important Regulatory Standards.

Participants discussed how a thoughtful list of presumptive "red lines" or prohibitions prevent overbroad use of FRT. It was stressed that in general, baseline expectations governing all AI systems would be helpful.

Participants also discussed the benefits of identifying authorized uses of lawful FRT in advance, such as public emergencies, human trafficking, missing persons, or child sexual exploitation cases It was noted, however, that any list of authorized uses should account for exceptional or exigent circumstances.. Participants also noted that any list of authorized uses needed to account for the wide range of police services and responsibilities in Canada. The RCMP, for example, has a protective mandate for domestic and foreign VIPs.

Participants also discussed presumptive prohibitions on biometric surveillance in the EU *Artificial Intelligence Act* (as discussed above in the fourth theme) as the leading example in the world. However, other national and many sub-national legislative bodies have also adopted or are exploring FRT prohibitions, including:

- **United States:** Some 15 US state legislatures have enacted regulations limiting police use of FRT. This includes two states that ban use of facial recognition in combination with police body cameras; four states which prohibit FRT use without a prior warrant, court order, or probably cause; six states that prohibit FRT other than in "serious cases"; five states requiring notice to defendants; two states prohibiting FRT without independent testing and accuracy standards; and seven states that prohibit FRT as the "sole basis" for identifying and arresting an individual.[8]
- **Quebec:** Quebec's privacy reforms under Law 25 requires organizations to conduct privacy impact assessments "for biometric systems, obtain opt-in consent, and notify regulators before creating biometric databases" backstopped by "meaningful enforcement" that may include "administrative penalties of up to $C25M or 4% of global revenue."[9]
- **New Zealand:** New Zealand's Office of the Privacy Commissioner is consulting on a Biometrics Privacy Code of Practice that, if enacted, would have the force of law under the ***Privacy Act***.

8. Thoughtful Policies Can Foster Responsible FRT Adoption.

It was agreed that thoughtful governance and/or procurement policies could promote responsible and consistent police FRT deployment. For example, police services expressed interest in the ability to take an FRT or AI system "off the shelf" that's already been reviewed, validated, and fully assessed for compliance with Charter rights, evidence law, human rights, and validity and reliability requirements.

Similar initiatives are discussed in greater detail in LCO Project Paper 4, ***AI at Trial and On Appeal***. This paper discusses how investigative technology such as intoxilyzers can be used efficiently and generate presumptively reliable evidence because they are regulated through a detailed, codified scheme set out in the Criminal Code and evidence law. This scheme includes features like:

- Technology performance and certification standards and associated trustmarks.
- Training and certification standards to achieve reliable and professional calibration and deployment.
- A clear and codified scheme to balance investigative expediency and public safety with procedural fairness and Charter compliance.
- National consistency and predictability.

The suggestion was that a similarly rigorous approach to designating, measuring, training and certifying different AI-enabled technologies would centralize these functions and allow law enforcement to rely on them without requiring detailed and differentiated local practices and policies.

9. Public Accountability Is Essential For FRT Adoption and Public Trust.

Roundtable participants discussed how many existing AI governance policies, including those adopted by the RCMP and Toronto Police Service, commit to a principle of transparency "as a key consideration for maintaining public trust and confidence in the responsible use of these technologies."[10]

The Roundtable also heard that that many US legislatures have enacted police AI or FRT laws or policies that include wide ranging transparency requirements, including mandatory disclosure to defendants and published privacy and legal impact assessment reports.

It was further agreed there is very little awareness of the overall "footprint" or use of law enforcement FRT systems in Canada. Nor is there any single authority or organization responsible for collecting such information. As a result, both the public and law enforcement agencies lack information about the deployment of FRT systems across the country.

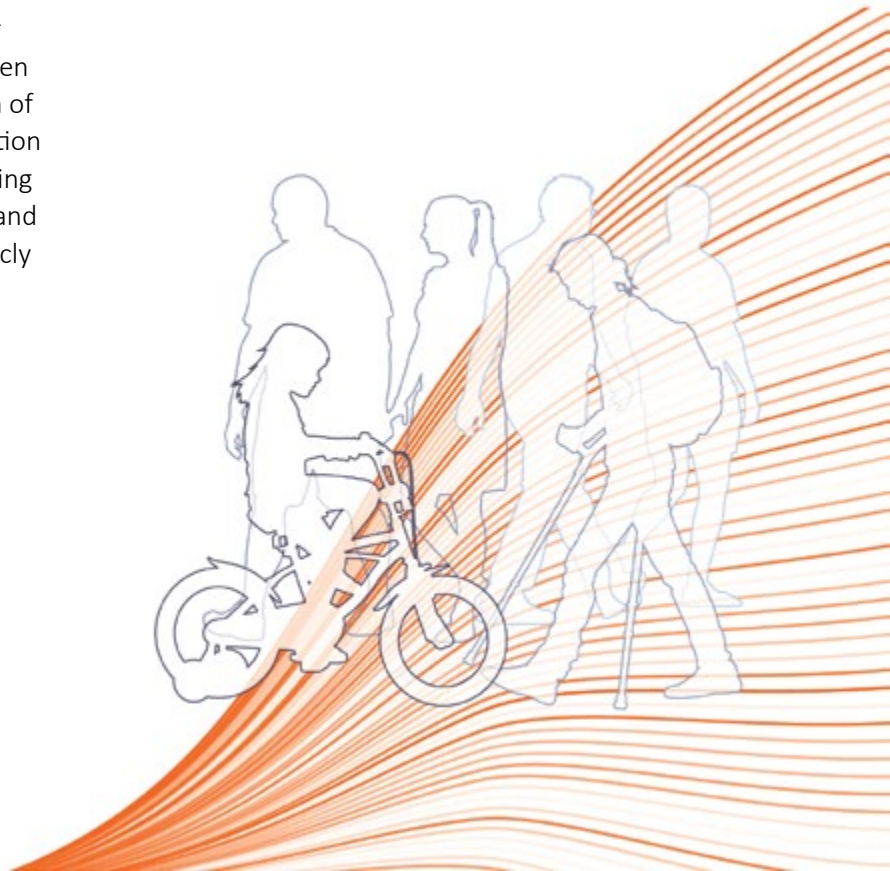
Once again, the European Union's 2024 Artificial Intelligence Act provides a leading example of how this might be implemented. For instance, the EU prohibits real-time biometric identification in the absence of prior judicial authorization, and only for certain classes of "serious cases." The legislation then commits national authorities to receive notification of the use of any such system and any judicial application for authorization (whether approved or not) including information on the number of the decisions taken and their result. All of which must be published in publicly available annual reports.[11]

10. Oversight of Police FRT Systems Could Be Coordinated More Effectively.

The Roundtable discussed how several factors limit the effectiveness of existing internal and external oversight functions of FRT and AI systems, including:

- The lack of dedicated AI and FRT impact assessments, including independently qualified people qualified to write them, and recognition that impact assessments are not "evergreen" and need frequent re-evaluation.
- The need for skilled "humans-in-the-loop" with independence or "contrarian" mandates to be meaningful and effective.
- The need for provincial policing standards organizations to assume a leadership role in standardizing more AI-related practices and policies.

It was also agreed that Crown prosecutors, privacy commissioners, and human rights commissioners should be more available to give the police proactive and timely advice.



Next Steps and Getting Involved

Consultations

Individuals or organizations interested in working with the LCO on FRT issues or our AI in Criminal AI project should contact LCO Policy Counsel Ryan Fritsch. Ryan can be contacted at rfritsch@lco-cdo.org.

More information about the LCO and AI in Criminal Justice Project is available here.

Contact

The LCO can be contacted at:

Law Commission of Ontario
Osgoode Hall Law School, York University
2032 Ignat Kaneff Building
4700 Keele Street Toronto
ON M3J 1P3

Telephone: (416) 650-8406
Email: lawcommission@lco-cdo.org
Web page: www.lco-cdo.org
X/Twitter: @LCO_CDO
LinkedIn: https://linkedin.com/company/lco-cdo

Vancouver Roundtable Materials

The following materials were collected as background material for the Vancouver Roundtable. Links to the full documents are embedded below.

- LCO excerpts from AI in Criminal Justice project Use of AI by Law Enforcement (April 2025)
- OPC Privacy guidance on facial recognition for police agencies (May 2022)
- RCMP FRT excerpts from NTOP Transparency Blueprint (2024)
- RCMP Griffeye AI Assessment Report (March 2024)
- York / Peel Police (Ontario) FRT Policy (May 2024)
- Toronto Police Service Use of AI Policy (updated Jan 2024)
- NYU Policing Project FRT Overview and Evaluation
- International Network of Civil Liberties Organizations (INCLO) Eyes on the Watchers Report
- ACLU Amicus Brief Parks v McCormac (available via Prof. Ben Perrin's 2024 AI & Criminal Justice: Cases and Commentary).

Endnotes

1 See Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* (2024) at 21-29, online: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing, as discussed in Law Commission of Ontario, LCO Criminal AI Project: Introduction and Summary (April 2025) at 13-14, online: https://www.lco-cdo.org/wp-content/uploads/2025/04/LCO-AI-in-Criminal-Justice-Paper-1-Introduction.pdf.

2 RCMP National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), online: https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint. See also RCMP, "Algorithmic Impact Assessment Results - Griffeye Tool" (March 26, 2024), online: https://opencanada.blob.core.windows.net/opengovprod/resources/dd50ce04-3150-4f26-b8ab-0ad067489593/griffeye-aia-en.pdf?se=2025-09-12T18%3A06%3A10Z&sp=r&sv=2024-08-04&sr=b&sig=njlbsUkvrWbbQT6%2BeRsL-b4Y9S1ASxgCnN6jLmLqgERs%3D.

3 RCMP National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), online: https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint.

4 RCMP National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), online: https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint.

5 See Peel Regional Police Directive, "Use of the Facial Recognition System" (May 8, 2024), online: https://www.peelpolice.ca/en/who-we-are/resources/Documents/IB174F-002-REDACTED.pdf.

6 Law Commission of Ontario, *LCO Criminal AI Project: Introduction and Summary* (April 2025) at 17, online: https://www.lco-cdo.org/wp-content/uploads/2025/04/LCO-AI-in-Criminal-Justice-Paper-1-Introduction.pdf. For a fuller discussion of privacy implications of FRT use in different contexts, as well as an encapsulation of legislation and case law, see Law Commission of Ontario, *Use of AI by Law Enforcement* (April 2025) at Part 3, online: https://www.lco-cdo.org/wp-content/uploads/2025/04/LCO-AI-in-Criminal-Justice-Paper-2-Law-Enforcement-Use.pdf.

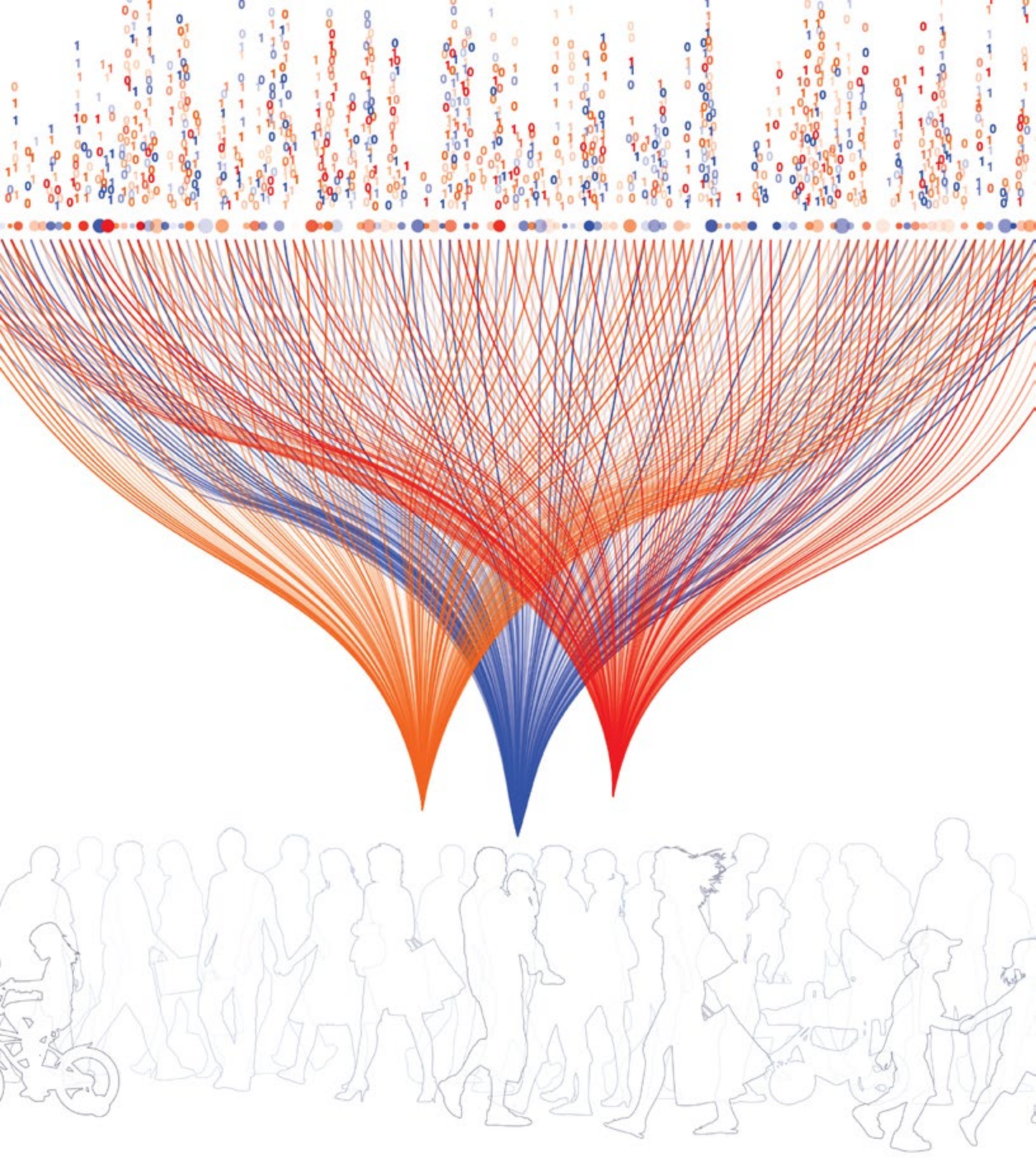
7 See Futurism.com, "The Hot New AI Tool in Law Enforcement Is a Workaround for Places Where Facial Recognition Is Banned" (May 17, 2025), online: https://futurism.com/track-facial-recognition-ai-tool.

8 See TechPolicy.press, "Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations" (January 6, 2025), online: https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/.

9 See International Association of Privacy Professionals, "Biometric promises, regulatory gaps: Why Canada needs a new approach to facial recognition technology" (May 2, 2025), online: https://iapp.org/news/a/biometric-promises-regulatory-gaps-why-canada-needs-a-new-approach-to-facial-recognition-technology.

10 RCMP National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), online: https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint.

11 See EU Artificial Intelligence Act, "Article 5: Prohibited AI Practices" at sections 5-7, online: https://artificialintelligenceact.eu/article/5/. See also the discussion in Rectials 35 and 36, online: https://artificialintelligenceact.eu/recital/35/ and https://artificialintelligenceact.eu/recital/36/.



LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, Ontario, Canada M3J 1P3