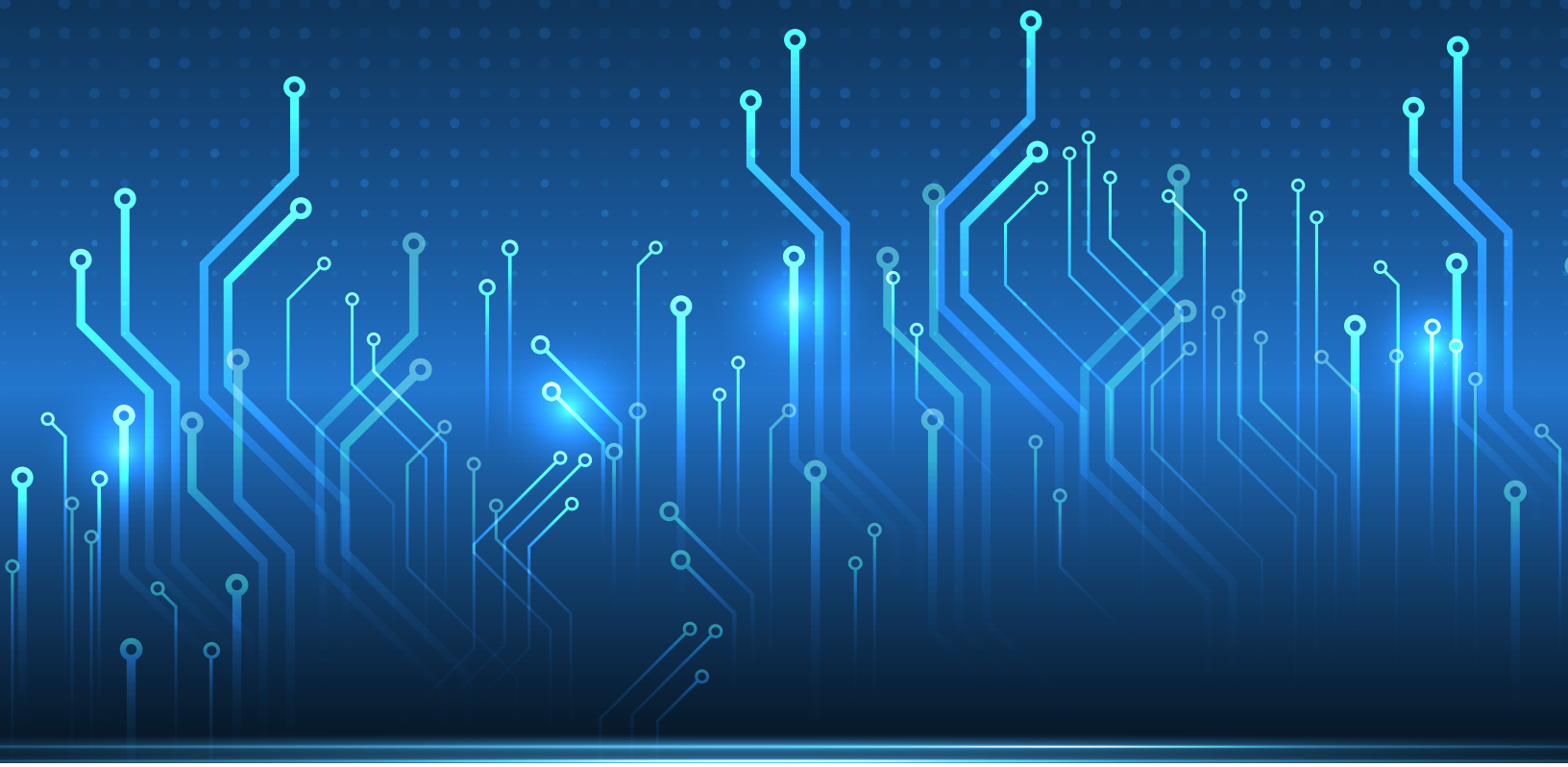
RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

National Technology Onboarding Program

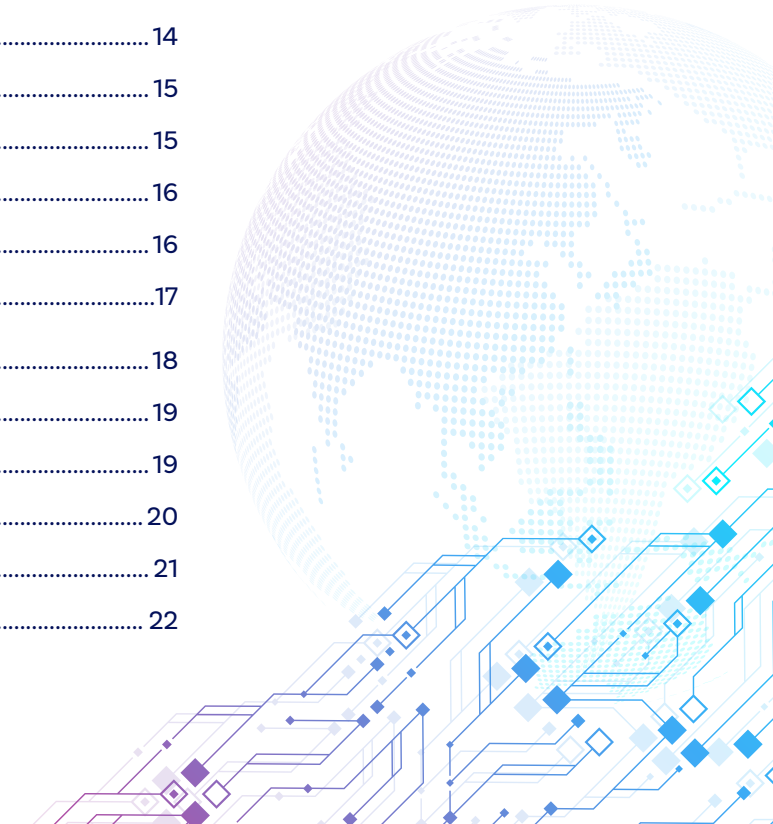
Transparency Blueprint: *Snapshot of Operational Technologies*



Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Table of Contents



Introduction

We have come to enjoy many benefits of a modern connected world with the rapid advancement of communication technologies over the past several years. However, the same technologies that enhance our lives and make them more convenient can also be exploited by criminals who use them to plan and commit crimes and to hide evidence of their criminal activities. To address this, the Royal Canadian Mounted Police (RCMP) needs to constantly consider how new and emerging technologies can be used to fight crime in our effort to ensure the safety and security of all Canadians.

In 2021, the RCMP's National Technology Onboarding Program (NTOP) was established to ensure the responsible use of operational technologies by the RCMP and to encourage more public transparency of those technologies. The *Transparency Blueprint: Snapshot of Operational Technologies* is NTOP's first publication on its work.

The *Transparency Blueprint* provides an overview of NTOP's mandate and key principles for the responsible use of operational technologies by the RCMP. It also details the types of operational technologies that NTOP assesses for use by the RCMP and some trends relating to the use of those technologies. The *Transparency Blueprint* also provides more comprehensive explanations about how and why the RCMP uses the following three key operational technologies, describing the situations in which they may be used, the types of information they collect, and the underlying legal authorities for their use:

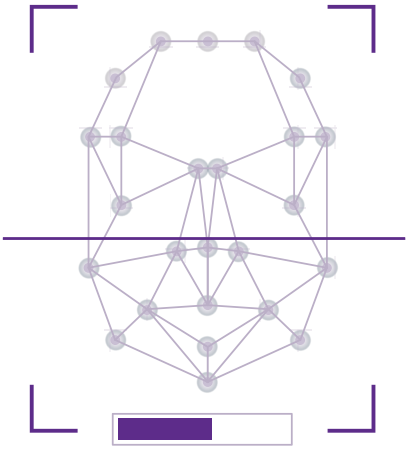
1. On-device investigative tools;
2. Cell-site simulators;
3. Remotely piloted aircraft systems (commonly known as drones).

The RCMP recognizes that the deployment of operational technologies should consider and balance the needs of law enforcement against any privacy and

ethical issues related to their use. While it is not always possible to provide all of the details of how and when certain operational technologies are used, which could negatively impact their effectiveness, NTOP nevertheless promotes transparency as a key consideration for maintaining public trust and confidence in the responsible use of these technologies by the RCMP.

The *Transparency Blueprint* serves as NTOP's first step to inform the public about the RCMP's responsible use of operational technologies. Next steps will include the proactive publication of summaries of NTOP's assessments of certain operational technologies. These efforts align with the RCMP's promise to improve transparency as part of the *Vision150 and beyond: RCMP strategic plan* and with the Government of Canada's National Security Transparency Commitment[1] as well as with the RCMP's obligations to publish summaries of completed Privacy Impact Assessments (PIA) under the Treasury Board Secretariat's Directive on Privacy Impact Assessment.[2]

The National Technology Onboarding Program (NTOP)



NTOP was established in 2021 following the Office of the Privacy Commissioner (OPC)'s investigation into the RCMP's use of Clearview AI facial recognition technology.[3] The OPC found that Clearview AI violated Canada's federal private sector privacy law by creating a databank of billions of images scraped from various websites without the consent of the individuals in the images. Consequently, the OPC found that the RCMP's collection of personal information from Clearview AI did not comply with the requirements of the *Privacy Act*, since that information had not been legally collected by Clearview AI. Those findings also identified concerns related to accountability and transparency as the RCMP did not have procedures in place to ensure that third-party service providers' personal information collection practices were compliant with Canadian privacy law.

In response to the OPC's investigation and findings, the RCMP created NTOP. NTOP's primary goal is to centralize and bring consistency and oversight to how the RCMP identifies, evaluates and tracks its use of operational technologies.

NTOP is responsible for conducting thorough assessments and evaluations of new and existing operational technologies to ensure that they have an operational need, they provide a clear benefit to the public, and they meet privacy, legal, policy, and ethical standards. Operational technologies that are privacy intrusive or contain artificial intelligence are given the highest priority.

According to RCMP policy, all RCMP program areas must consult NTOP when considering the use of operational technologies and/or datasets involving the collection or use of personal information. Close collaboration with RCMP program areas is necessary to ensure compliance with assessment and evaluation requirements for operational technologies.

Moreover, a central theme in recent studies by the House of Commons Standing Committee on Access to Information, Privacy and Ethics around the use of technologies by police was the need for increased transparency and accountability.[4,5] In addition to conducting through assessments as described above, NTOP is also responsible for informing the public about the RCMP's use of operational technologies.

Mandate

NTOP's responsibility for conducting thorough and objective assessments of operational technologies involves the following key components and activities:

- Establish standard procedures for assessing and onboarding operational technologies;
- Assess the effectiveness of new operational technologies;
- Ensure data collection techniques are lawful and ethical;
- Ensure the use of operational technologies is necessary;
- Monitor, track and report on operational technologies used by the RCMP;
- Inform the public about the RCMP's use of operational technologies.

Responsible use of operational technologies – key principles

NTOP evaluates operational technologies in collaboration with a number of internal partners based on 10 key principles. This ensures that technologies are used in a manner that is responsible, necessary, and proportionate, meaning that their use must be directly connected to a clearly defined public safety objective. NTOP ensures that conditions of accountability, privacy and transparency inform the use of operational technologies by the RCMP.

The following principles guide the responsible and effective use of police technology. It also aligns with the International Association of Chiefs of Police - Technology Policy Framework.[6]

1. Accountability

- The accountability structure for RCMP operational technologies should be clearly defined and transparent, while continuing to protect sensitive aspects.
- The roles and responsibilities of RCMP decision-makers and operators should be identified, documented and aligned with the use of operational technologies.

2. Transparency

- Transparency is critical to fostering public trust and confidence in the RCMP's use of operational technologies and ensuring citizens and communities understand the legitimate use of police technology.
- The RCMP will implement new ways to maximize transparency and two-way dialogue with the Canadian public and key stakeholders on operational technologies, such as seeking public feedback on operational policies.

NTOP works closely with subject matter experts from the following RCMP branches/units:

- Access to Information and Privacy
- Legal Services Unit
- Departmental Security Information and Communication Technology Security
- Information Management/ Information Technology Program
- Technical Case Management Program
- Relationship and Portfolio Management

3. Privacy

- Operational technologies may include the lawful collection, use, analysis and disclosure of personal information to advance the RCMP's activities and objectives.[7]
- Operational technologies should undergo privacy analysis and assessment to adequately safeguard the handling of personal information.

4. Specificity

- Operational technologies should be fit-for-purpose and aligned with clear and explainable law enforcement objectives and operational necessities.
- The requirements for an RCMP operational technology should outline all legal, policy and operational considerations to ensure that the deployment and use of the technology is lawful and serves a legitimate policing purpose.

5. Accuracy

- Operational technologies should rely on accurate, complete and up-to-date operational data to support RCMP activities and decisions.
- RCMP operational technologies should have strong data quality attributes, such as procedures and technical mechanisms to ensure data accuracy, including the relevant, timely and consistent use of operational information.

6. Training

- The RCMP's responsible use of operational technologies requires initial and ongoing training to minimize the risk of improper use or misconduct.
- Operational technologies should have appropriate and thorough training protocols for all authorized users, such as basic and advanced training and should use training to improve the RCMP's data literacy on operational technologies.

7. Impact

- The RCMP's use of operational technologies may disproportionately impact certain populations and groups, such as victims of crime. The level of impact depends on the capabilities of the operational technology, the application of the technology, its scale and scope and other factors.
- The use of operational technologies by the RCMP should fully weigh the impact of the technologies on Canadians, such as any disproportionate impact on individuals, groups and communities.[8]

8. Limitations

- The RCMP's use of operational technologies should have clear links to enabling legislation and/or policy and guardrails to define the authorized scope of use.
- The RCMP will deploy operational technologies in a manner that includes limiting measures and minimization techniques, such as deploying operational technologies for serious crimes only where appropriate.

9. Security

- The RCMP is responsible for the security and safeguarding of all of the information that it collects operational technologies, particularly personal information.
- Operational technologies should include information management and information security measures to safeguard the use of the technologies, including the confidentiality, integrity and availability of data.

10. Evaluation

- The assessment, evaluation, and auditability of operational technologies is fundamental in fostering public confidence and trust and supporting the ongoing review and improvement for the RCMP use of operational technologies.
- The RCMP should regularly monitor and evaluate the performance of its operational technologies and maintain technologies in a manner to support evaluations, reviews and audits by external organizations.

Did you know?

NTOP works closely with the RCMP's Access to Information and Privacy Branch to assess the privacy implications of operational technologies.

This includes the lawful collection, use, retention and disclosure of personal information to ensure compliance with the *Privacy Act*.

Since 2019, the RCMP has been modernizing its approach to access to information and privacy, including improvements to transparency, PIAs and other measures.

For more information, see the RCMP's Access to Information and Privacy - Modernization Strategy.

Snapshot of operational technologies

Operational technologies play a critical role in modern policing. They are used to combat crime, investigate suspects, protect children and vulnerable groups, collect evidence, improve data analytics, strengthen police accountability, and advance law enforcement and public safety objectives.

To keep pace with criminals and to uphold public safety, the RCMP need to continually adapt, innovate, and use new and emerging technologies. At the same time, these technologies need to be used in a responsible and proportionate manner. The use of new and/or potentially invasive technologies for law enforcement requires careful consideration of privacy, ethical, legal and other public interest considerations.

The types of operational technologies that NTOP assesses fall into one or more of the following categories:

1. **Algorithmic Technology** – Algorithm-driven technologies that enable law enforcement agencies to draw inferences from mass data processing with the goal of 'predicting' potential unlawful activity by identifying patterns. Such technologies include license plate readers and other tools that use algorithms and machine-learning.
2. **Artificial Intelligence** – Any software application that uses artificial intelligence algorithms to perform specific tasks or solve problems. Artificial intelligence tools can be used in a variety of contexts to automate tasks, analyze data, and improve decision-making.
3. **Cell-Site Simulators** – Mimics a cell-phone tower and is used to identify cellular devices within the proximity of the cell-site simulator. Collects only identifying numbers – does not intercept private communications. Sometimes referred to as IMSI catchers.
4. **Safety Cameras, video and surveillance** – An electronic video system or device that monitors public spaces to detect and record criminal events or any other threat to public safety. This category includes Body-Worn Cameras and Camera Registry services.
5. **Criminal Group Databases (Dataset)** – Investigative resources to maintain consistent, up-to-date intelligence regarding criminal groups and street gangs.
6. **Cryptocurrency Analysis Tools** – Performs search activities for cryptocurrency addresses across the blockchain, as well as other public data sources on the Internet such as cryptocurrency transaction information.
7. **Digital Forensic Access Tools** – Software and physical devices that are used to access, extract, and process information found on electronic devices. In some cases, the software may also facilitate extraction of information from cloud-based services.
8. **Drones & Drone Detection Systems** – Commonly referred to as drones, the RCMP refers to them as remotely piloted aircraft systems or RPAS. Drone detection systems are used to identify non-RCMP remotely piloted aircraft systems.
9. **Facial Recognition Software** – Facial recognition is a digital technology that is used to compare images obtained during criminal investigations with lawfully obtained photographs of known individuals.
10. **Global Positioning Systems Tracking Devices** – Devices capable of identifying or estimating the geographic position of a device or object that is being tracked.
11. **Internet Attribution Management Infrastructures** – Activities on the Internet and the pieces of information left behind from those activities often result in data, or 'digital footprints.' These tools help identify and interpret that data, which may include IP addresses, advertising IDs, and other data generated by networks and devices.
12. **Media Aggregation Services** – Software platforms that search across thousands of public sources of information on the Internet and alert users to its existence. These alerts may also include a link to the original source of the information on the Internet and the time the information was posted on the Internet.
13. **On-Device Investigative Tools** – A computer program as defined in section 342.1(2) of the *Criminal Code* that is installed on a targeted computing device that enables covert and remote collection of electronic evidence from the device. Commonly referred to as ODITs.
14. **Open Source Intelligence** – The collection and analysis of data gathered from open sources (i.e., the Internet) to produce actionable intelligence. It is primarily used in law enforcement, public safety, and national security contexts for situational awareness and evidentiary purposes.
15. **Social Network Analysis Tools** – Tools that process information on social networking platforms to aid police in discovering information relevant to investigations and to address public safety concerns.

To date, NTOP completed the assessment of 28 technologies that fall within these categories.

Three operational technologies used by the RCMP

NTOP is closely monitoring a number of variables related to the responsible use of the following three potentially invasive operational technologies:

1. On-device investigative tools;
2. Cell-site simulators;
3. Remotely piloted aircraft systems.

This is not meant to be a comprehensive list of all RCMP operational technologies. Through future transparency publications, NTOP will provide details about a broader range of RCMP operational technologies, including body-worn cameras,[9] automated license plate recognition technology, open source intelligence tools, facial recognition,[10] and other key technologies.

On-device investigative tools

What are they?

An on-device investigative tool is a computer program that can be installed on a digital device to allow police to covertly collect electronic evidence. These tools are only used for serious criminal and national security investigations, only after judicial authorization has been obtained.

Once judicial authorization has been granted, the RCMP uses on-device investigative tools to lawfully gather private communications and other information from targeted devices either before they are encrypted or after they have been decrypted on the suspect's device(s), since encryption renders the information unintelligible.

As a result, the information may be collected in a clear and intelligible plain text format and used for law enforcement purposes.[11]

Why are they used?

Traditionally, judicially authorized wiretapping by law enforcement was a relatively straightforward investigative technique. With the advancement of cellular technology and digital communications, this policing activity has increased in complexity and technical sophistication.[12,13]

The criminal use of encryption adds another layer of complexity for police and lawfully intercepting communications. Encryption plays a fundamental role in cyber security and crime prevention, as it protects against unauthorized data access and use. When used by criminals, encryption and other online anonymizing techniques enable the planning and execution of serious criminal activity, such as terrorism, organized crime, financial crime, online child sexual exploitation, and other types of cybercrime. Criminals use these technological capabilities to evade law enforcement and target victims, including Canadian citizens and organizations.

On-device investigative tools – key features for evidence collection

- Intercepting online communications
- Collecting and storing data
- Capturing screenshots
- Keyboard logging
- Activating microphones and camera features

How do they work?

The technical capabilities of an on-device investigative tool may range and will depend on the law enforcement objective and scope of the judicial authorization, which must be sought prior to the operational use of these tools. Some of the technical capabilities include intercepting communications, collecting and storing data, capturing computer screenshots and keyboard logging, and/or activating microphone and camera features.

When are they used?

The RCMP only deploys on-device investigative tools for serious criminal investigations, such as organized crime, national security and terrorism, cybercrime, or other serious crimes. This technique is only used when other investigative means of collecting evidence have proven to be ineffective.

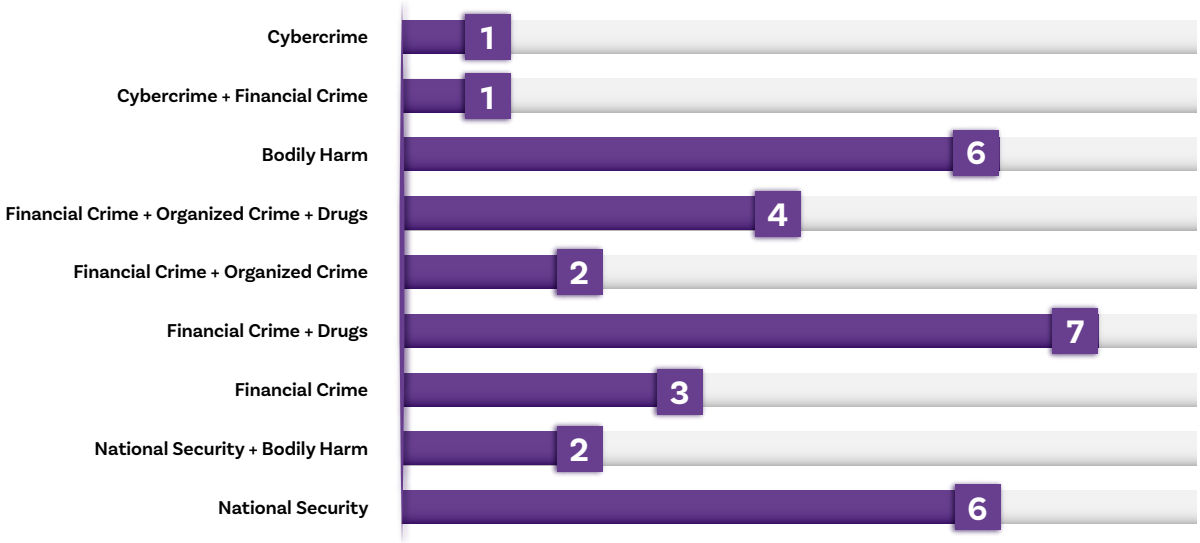
From 2017 to 2022, the RCMP used these tools in 32 criminal investigations, targeting 49 devices in total. During the same period, the RCMP had more than 13 million police-related occurrences.[14,15]

The following chart provides a percentage breakdown of the RCMP's use of on-device investigative tools by criminal offence category, based on deployments from 2017 to 2022. As shown, national security (including terrorism-related offences), bodily harm, financial crime and drug-related offences comprise the majority of criminal investigations where on-device investigative tools were used.[16] In most cases, investigations involving the use of on-device investigative tools involved multiple criminal offences.

Chart 1: Criminal offences for on-device investigative tools

Criminal offences for on-device investigative tools

RCMP use from 2017 to 2022, includes 32 investigations in total



The RCMP's use of on-device investigative tools is consistent with its public protection and crime prevention duties as described in Section 18 of the *Royal Canadian Mounted Police Act*. The specific authorities to intercept private communications using an intercept warrant are provided in Part VI of the *Criminal Code*.

Did you know?

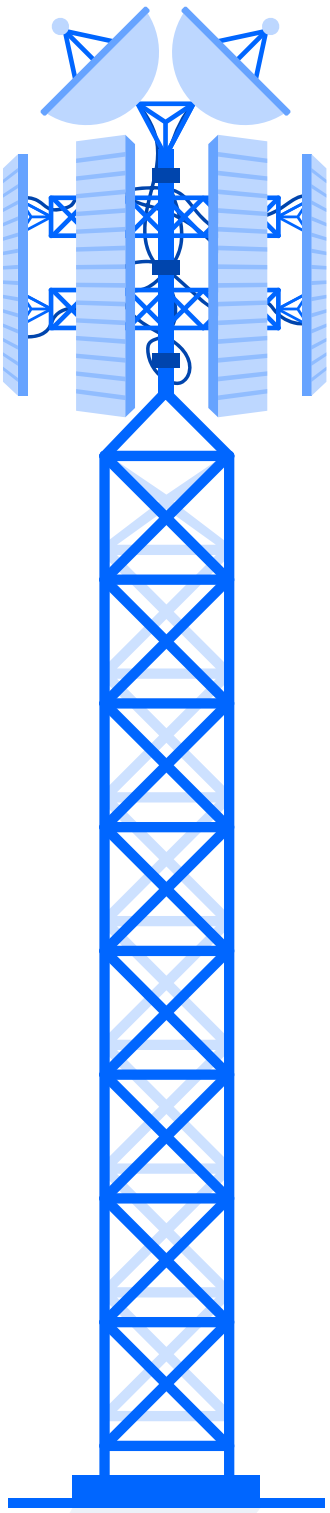
The *Canadian Charter of Rights and Freedoms* (the Charter) protects Canadians against unlawful search and seizure. During a private communication there is a reasonable expectation of privacy therefore its interception is considered to be a search (and seizure) within its meaning in section 8.

The RCMP uses operational technologies and collects personal data in alignment with the Charter and expectations of privacy, including the *Criminal Code*, procedural powers and judicial authorization requirements for evidence collection, such as general warrants, interception warrants for electronic surveillance, in addition to specialized warrants, production orders and other legal instruments.

When applying for an intercept warrant, the police must explain to the judge whether other investigative procedures have been tried and have failed or why it appears that such procedures would be unlikely to succeed. The type of warrant obtained depends on the information that is being sought, the intended use of the tool(s), consent from a party, among other factors. For example, collecting historical communications from a suspect under investigation versus prospective future communications requires different types of court authorization. In most cases, the RCMP's use of on-device investigative tools requires multiple warrants, which are time-limited and subject to further limitations.

The only exception to the RCMP seeking prior judicial authorization is in urgent cases, referred to in section 188 of the *Criminal Code* as exigent circumstances. This involves emergency situations where rapid action by police is required to prevent imminent danger to a person, threat to life, serious damage to property or the potential destruction of evidence.[17] To date, the RCMP has never used exigent circumstances to deploy an on-device investigative tool and has therefore always sought prior judicial authorization.

The data collected using on-device investigative tools is encrypted and stored in a secure manner by the RCMP with strict access controls based on the Government of Canada and the RCMP's security policies and guidelines for information management and evidence handling.



Cell-site simulators

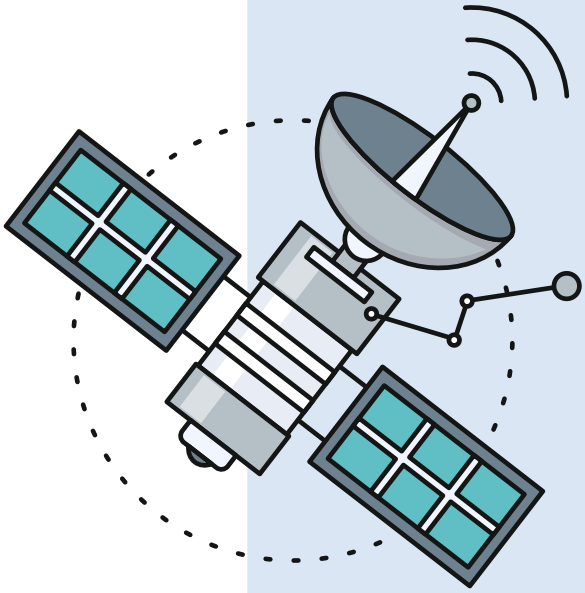
What are they?

Cell-site simulators are electronic devices that, when activated, mimic cellular towers to attract all nearby mobile phones and other cellular devices to connect to them. Unique alphanumeric identifiers[18] are obtained from these mobile devices and can be used to track the location of device(s) of interest or to subsequently identify the owner(s) of the device(s).

Why are they used?

The RCMP may use cell-site simulators to assist in high priority investigations relating to national security, serious and organized crime, and other *Criminal Code* offences that impact the safety and security of Canadians. This technology may also be used in urgent circumstances, such as a missing person or abduction case.[19]

The RCMP obtains judicial authorization prior to the use of a cell-site simulator, excluding exigent circumstances.[20] In most cases, the authorizations obtained include a transmission data recorder warrant and a tracking warrant. In accordance with the *Radiocommunication Act*, the RCMP also obtains a letter of authorization from Innovation, Science and Economic Development Canada to operate cell-site simulator technology in Canada.[21]



Transmission data

The *Criminal Code* defines transmission data as data that:

(a) relates to the telecommunication functions of dialling, routing, addressing or signalling;

(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the *Criminal Code* (Unauthorized use of computer) in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication.

How do they work?

The RCMP's cell-site simulators do not intercept private communications, such as the content of private voice or audio communications, text messages, or email messages. They are only used to capture unique alphanumeric identifiers associated with cellular devices. The RCMP must seek additional judicial authorization to obtain personal subscriber information associated with a mobile device used by a suspect under investigation.

All data collected using cell-site simulator technology is stored in a secure manner in accordance with applicable Government of Canada and RCMP security policies and guidelines.

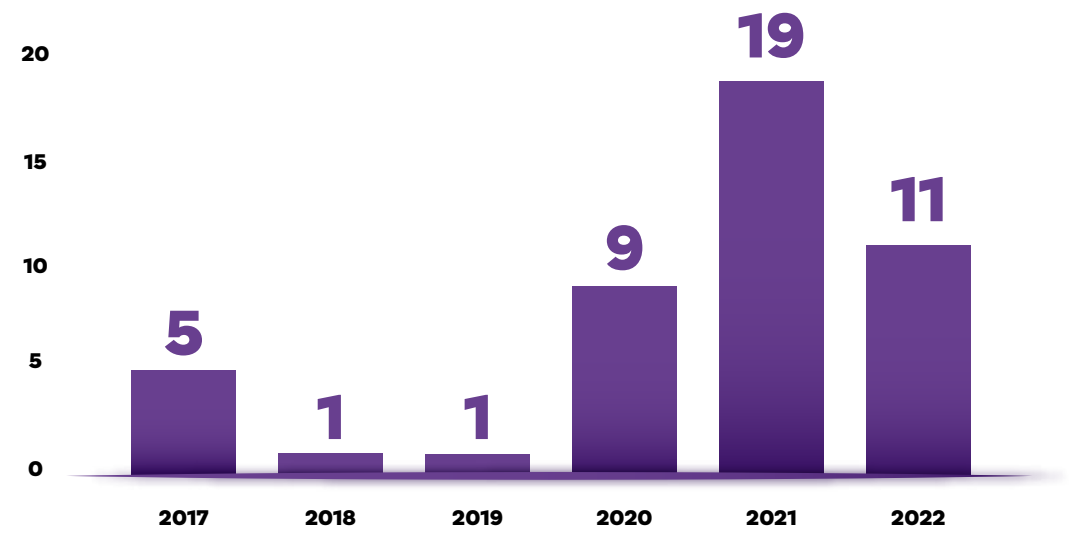
When are they used?

From 2017 to 2022, the RCMP deployed cell-site simulator technology in 46 investigations. The following chart provides a year-to-year breakdown of the RCMP's use of this technology from 2017 to 2022.

Did you know?

In exigent circumstances, such as an abduction, where a victim may be at imminent harm and rapid action is required to prevent danger to life, or serious damage to property or destruction of potential evidence, the RCMP may use cell-site simulator technology without prior judicial authorization. In these cases, judicial authorization would be actively sought as soon as possible, including a full explanation of the exigent circumstances.

Chart 2: Number of cell-site simulator deployments



More information about the RCMP's use of cell-site simulators can be found in the OPC's 2017 report, Cell site simulators used by RCMP not capable of intercepting private communication.

Remotely piloted aircraft systems

What are they?

As rapidly deployable and highly agile aircraft, remotely piloted aircraft systems, commonly known as drones, are used for aerial surveillance activities. These aircraft systems are equipped with electro-optical and/or infrared cameras.[22] These are used to support a multitude of critical RCMP operations, such as major crime scenes, search and rescue missions, traffic collision scenes and high-risk situations involving the RCMP Emergency Response Team.[23]

A PIA was conducted by the RCMP's Remotely Piloted Aircraft System Program to ensure compliance with Canadian privacy laws and regulations.[24] The PIA mandates strict protocols for handling data collected by a remotely piloted aircraft system, emphasizing the protection of personal information. Remotely piloted aircraft system use is specifically focused on supporting investigations, with collected data securely integrated into RCMP systems or deleted according to retention schedules.

Why are they used?

By enhancing situational awareness and the quality of evidence gathered at outdoor police operations, remotely piloted aircraft systems provide valuable information to police, such as locating vulnerable people during a search and rescue. They also reduce the risk to police officers in certain situations by sending the technology into high-risk environments.

How do they work?

The RCMP's use of remotely piloted aircraft systems is in accordance with Section 18 of the *Royal Canadian Mounted Police Act*, which details its public protection and crime prevention duties. The requirement for prior judicial authorization depends on the operational context and intended use. Aerial surveillance activities that infringe upon a reasonable expectation of privacy would require prior judicial authorization. For example, using a remotely piloted aircraft system to capture video of the backyard of a private residence involving a suspect under investigation would require a warrant.

Did you know?

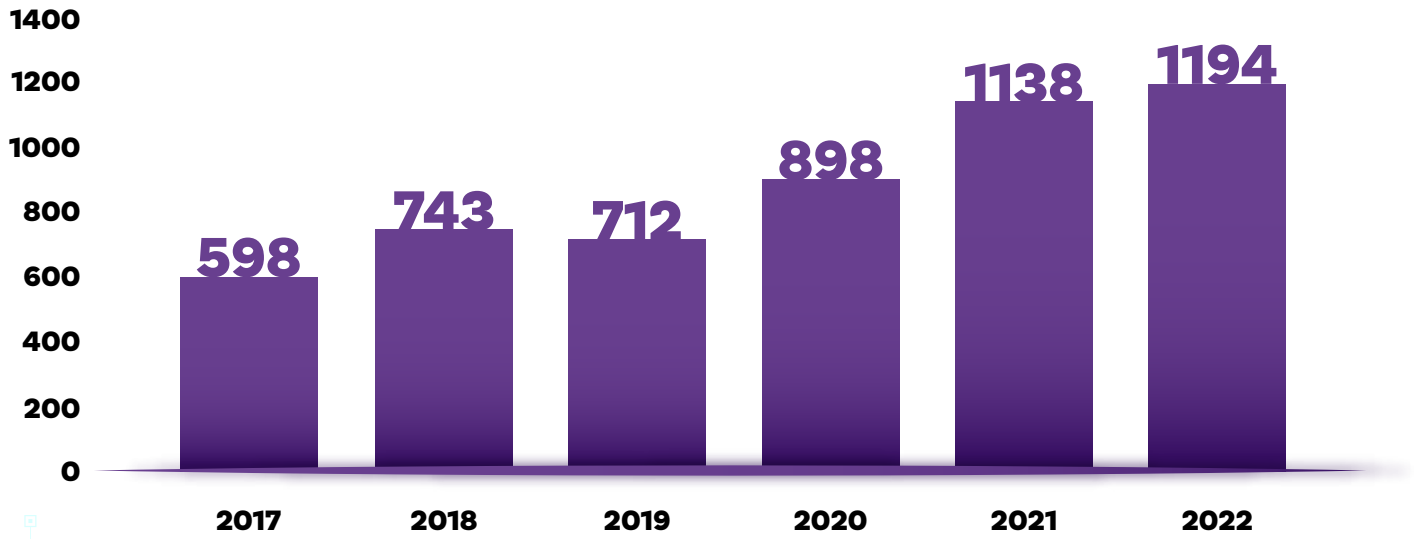
All of the RCMP's remotely piloted aircraft systems are registered with Transport Canada and marked with a unique registration number.

They are operated only by trained and certified RCMP pilots, based on requirements from the RCMP Remotely Piloted Aircraft System Program and in accordance with Transport Canada's Canadian Aviation Regulations.

The RCMP's remotely piloted aircraft system program includes a fleet of 399 registered aircraft systems and nearly 300 trained and certified RCMP pilots across Canada. The chart below illustrates the number of RCMP remotely piloted aircraft system flights from 2017 to 2022.

Chart 3: Number of RCMP remotely piloted aircraft system flights by year

RCMP remotely piloted aircraft systems: operational flights by year

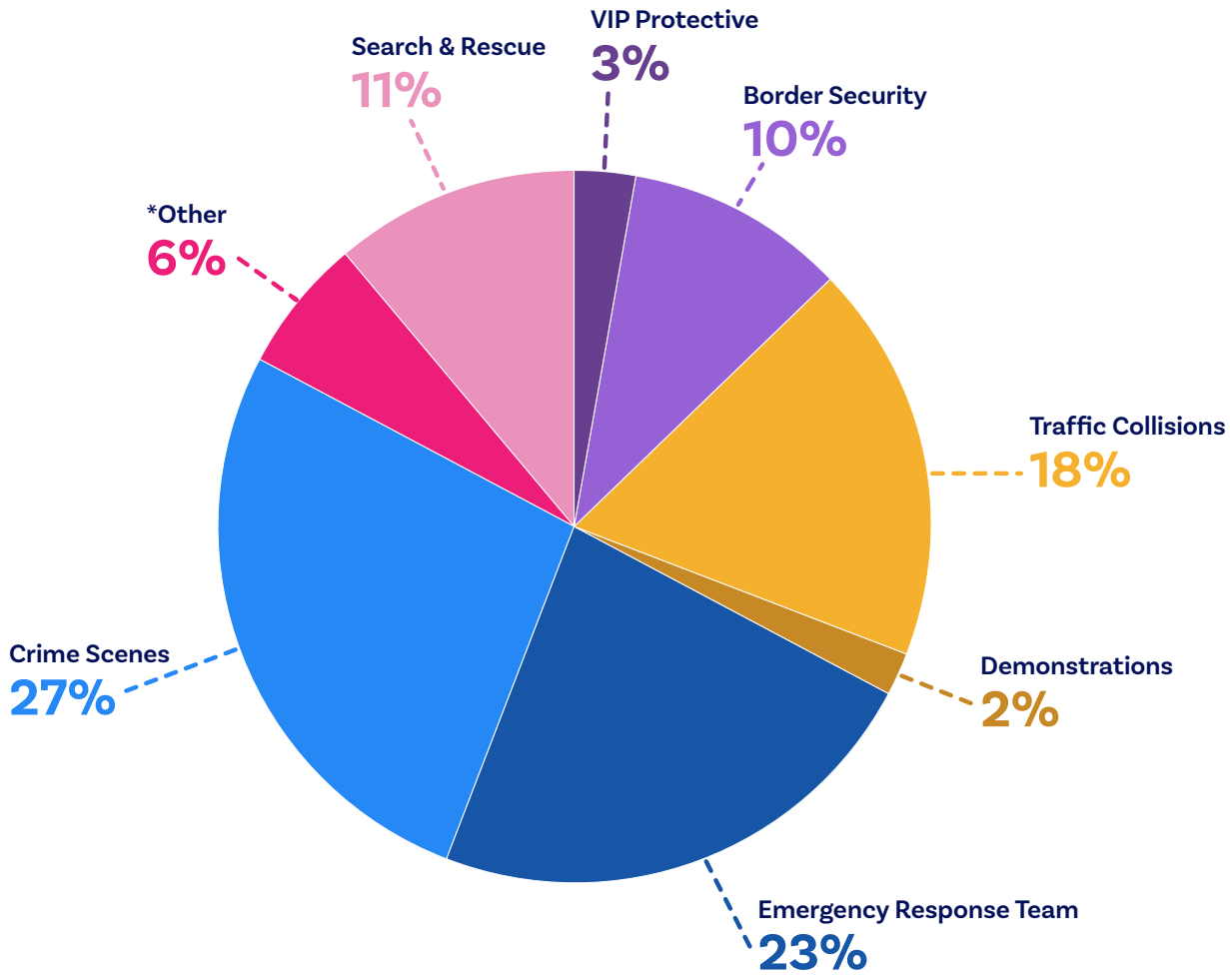


When are they used?

The RCMP's remotely piloted aircraft system program has increased in recent years, logging 1,194 operational missions in 2022. These missions included crime scene investigations, Emergency Response Team operations, traffic collision scenes, border security, search and rescue and other policing activities. The data collected from remotely piloted aircraft systems is assessed to determine whether it has evidentiary or administrative value or whether it is transitory in nature. All information is maintained based on the applicable Government of Canada and RCMP information management and evidence handling policies and guidelines. The RCMP currently does not use facial recognition technology on any photos or videos captured by remotely piloted aircraft systems.

The following chart provides a breakdown of RCMP remotely piloted aircraft system flights in 2022 by the type of mission.

Chart 4: RCMP remotely piloted aircraft system flights in 2022 by mission type



***Other** includes video production, radio tower inspections, traffic monitoring, mapping sites for security planning, drone images for active shooter contingency plans, and other police-related occurrences for RCMP remotely piloted aircraft system missions.*

Emerging technologies

The RCMP is committed to examining and deploying new and emerging technologies in an ethical and responsible manner. NTOP will continue to publish information on the RCMP's use of key operational technologies, such as artificial intelligence and facial recognition, body-worn cameras,[25] automated license plate recognition technology,[26] and information sources such as open source intelligence, as part of its mandate.

Open source intelligence considerations

Open source intelligence refers to the lawful collection and analysis of publicly available information for the purpose of law enforcement and crime prevention. This encompasses a broad range of sources, including news websites, social media platforms, public records, academic publications, and other online resources that are freely accessible to anyone. The RCMP recognizes that this may include personal information and that there may be an expectation of privacy even when such information is shared publicly.

The RCMP strategically leverages open source intelligence for various investigative and public safety purposes. These applications contribute to threat identification and monitoring, locating persons of interest, providing investigative support, and facilitating community engagement and awareness.

The RCMP employs a variety of specialized tools and techniques for analyzing open source information in order to create open source intelligence. For example, one such tool is called Babel X, for which the RCMP conducted a detailed PIA.[27]

This type of technology also includes many tools that are powered by artificial intelligence. As described in the following section, the RCMP takes a number of steps to ensure that the use of such tools is legal, ethical, and complies with Canadian privacy laws.

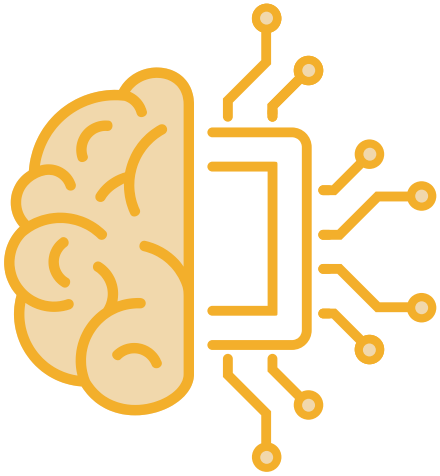
Artificial intelligence considerations

Artificial intelligence (AI) is increasingly being used in law enforcement to improve the efficiency of many different functions or tasks, such as crime forecasting, classifying and editing large amounts of photo and video evidence, gunshot detection, transcription/translation services, and many others. The use of AI by law enforcement raises privacy issues and ethical concerns with respect to potential bias. To ensure that AI is used legally, ethically and responsibly, it is important to consider that:

- An artificial intelligence system should be transparent about how it makes decisions. It must be easy for humans to understand how a machine learning algorithm arrived at a particular decision, making it easier to identify and correct errors or biases.
- Accountability measures must be in place to ensure that artificial intelligence systems are functioning as intended. This

requires strict oversight, ongoing research and evaluation.

- Artificial intelligence systems must be designed to avoid continuing existing biases and discriminatory practices. A bias can lead to unfair outcomes for marginalized groups and perpetuate injustices in the criminal justice system.
- Artificial intelligence systems are capable of collecting and/or analyzing vast amounts of personal information from a variety of sources, which raises questions about the right to privacy and the potential for abuse by law enforcement agencies. It is important to ensure that privacy rights are respected when using AI through effective policies and procedures.



These considerations align with NTOP's 10 key principles to assessing and evaluating technologies. The RCMP's use of AI must also conform with the Government of Canada's applicable policies and directives.

Additionally, NTOP recently coauthored the RCMP's Interim Guidance on Generative Artificial Intelligence Tools to guide RCMP employees while an official AI policy is being finalized.

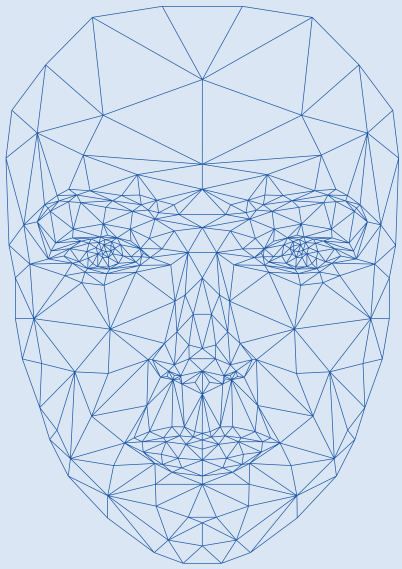
Facial recognition technology considerations

Facial recognition technology is powerful. The technology uses advanced algorithms to process facial images and analyze biometric facial features for identity verification purposes. Its inappropriate use could adversely impact privacy and other fundamental rights, such as risks associated with unintended data biases and false identifications.

For law enforcement and public safety, facial recognition technology may support the investigation and identification of criminal suspects, missing persons, children at risk of online sexual exploitation, or may assist in mitigating imminent threats to public safety.

The RCMP understands that the use of facial recognition technology by police may create concerns for the Canadian public. The RCMP will be using a type of facial recognition technology called face matching, which is a functionality built into certain software applications that are used for processing, sorting and analyzing large volumes of images and videos. The RCMP will use this technology only for processing evidence that has been lawfully obtained in the course of an investigation.

However, the RCMP anticipates using operational technologies for facial identification purposes in the future to aid investigators in identifying criminals and victims of crime. These types of operational technologies will only be used under specific circumstances in accordance with RCMP policies and Canadian law.



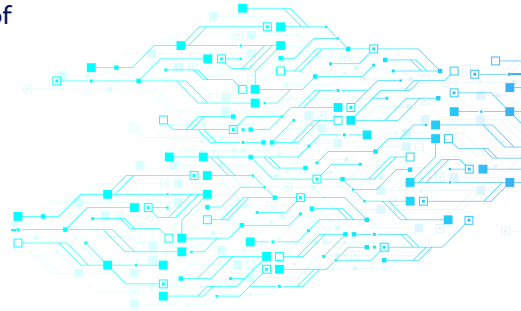
What is the difference between face matching and facial identification?

Facial recognition technology refers to the use of sophisticated software applications to detect and analyze faces appearing in digital media in order to compare the facial features of the individuals whose faces are detected with those appearing in other photos or videos.

Face matching is the use of facial recognition technology for the purpose of comparing and grouping digital media in which the same or similar faces appear. It is not used as a direct means to identify unknown individuals appearing in photos or videos. Face matching can be achieved with less sophisticated algorithms and computational power compared to facial identification. It is generally used for processing large numbers of lawfully obtained images or video recordings.

Facial identification is the use of facial recognition technology to perform the automated searching of a face or "probe image" of an unknown individual against a collection or database of digital images of known individuals for identification or verification purposes. Facial identification employs sophisticated algorithms, machine learning, and significant computational power to analyze facial features, distances, and patterns for accurate identification.

NTOP established a facial recognition technology working group to assist in the development of an operational policy to guide its use by the RCMP. The policy will be informed by legal, privacy, civil society stakeholders, and other subject matter experts to help ensure the lawful, necessary and proportionate use of facial recognition technology by the RCMP.



Conclusion

Transparency is critical to fostering trust and confidence in the RCMP, and greater transparency on new and evolving operational technologies plays a critical role. The OPC, the House of Commons Standing Committee on Access to Information, Privacy and Ethics, and many others have made it clear that Parliament and the general public have a right to know how new technologies are being used in law enforcement and how the privacy implications of those technologies are being addressed.

The RCMP's NTOP will, in collaboration with other police forces and key stakeholders, take significant measures to improve accountability through transparency with respect to the RCMP's use of operational technologies.

The publication of the *Transparency Blueprint: Snapshot of Operational Technologies* is an initial and important step towards greater transparency. Improvements cannot be measured by any single effort, nor should it be viewed as a checklist exercise. NTOP will continue to support the RCMP's ongoing efforts to improve transparency and public understanding of its use of operational technologies.

Endnotes

1 The Government of Canada's National Security Transparency Commitment is available at: https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html

2 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308

3 The National Technology Onboarding Program was established following the Office of the Privacy of Commissioner's June 2021 report, "Police use of Facial Recognition Technology in Canada and the way forward". More information is available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

4 https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-6/

5 https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-7/

6 The International Association of Chiefs of Police released a Technology Policy Framework (2014) to guide the responsible and effective deployment of operational technologies by police. The framework is available at: https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf

7 Summaries of RCMP Privacy Impact Assessments are available at: https://www.rcmp-grc.gc.ca/en/privacy-impact-assessments

8 The use of Gender-Based Analysis helps ensure that RCMP policies, programs and processes are inclusive and foster a safe and healthy work environment. Additional information on RCMP Gender-Based Analysis efforts are available at: https://www.rcmp-grc.gc.ca/en/change-the-rcmp/support-modern-policing/increase-use-gender-based-analysis-gba-the-rcmp

9 Information on the RCMP's planned roll-out of body-worn cameras is available at: https://rcmp.ca/en/body-worn-cameras

10 Information on the Automated License Plate Recognition Program in British Columbia is available at: https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=23&languageId=1&contentId=11953

11 In November 2022, the House of Commons Standing Committee on Access to Information, Privacy and Ethics, presented in the House of Commons a report entitled *On-Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*. The report is available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-7/

12 Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, 12 Nw. J. Tech. & Intell. Prop. 1 (2014). https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/

13 The *Criminal Code* requires the Minister of Public Safety and Emergency Preparedness to prepare and present to Parliament an annual report on the use of electronic surveillance under Part VI of the *Criminal Code* for offences that may be prosecuted by, or on behalf of, the Attorney General of Canada. This requirement includes the RCMP and the broader Canadian law enforcement community. The *2020 Annual Report on the Use of Electronic Surveillance*, which covers a five-year period from 2016 to 2020, is available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-nnl-rprt-lctrnc-srvllnc/index-en.aspx

14 RCMP Occurrence Report – 2021. Available at: https://www.rcmp.gc.ca/transparenc/police-info-policieres/calls-appels/occurence-incident/2021/index-eng.htm

15 An occurrence can be any type of police-related event or activity that is entered into a police records management system.

16 The *Criminal Code*, section 183, provides a full list of criminal offences that may apply to the RCMP's use and deployment of on-device investigative tools. Available at: https://www.laws-lois.justice.gc.ca/eng/acts/C-46/section-183.html

17 In urgent cases (often referred to as "exigent circumstances"), the RCMP may use an on-device investigative tool without prior judicial authorization, such as a kidnapping, where a victim may be at imminent harm and by reason of exigent circumstances it would be impracticable to obtain a warrant. The *Criminal Code*, section 529.3, includes a definition of "exigent circumstances" for the purposes of entering a dwelling without a warrant, in addition to Canadian case law interpretations. While this scenario is possible, to date, the RCMP has never deployed an on-device investigative tool without prior judicial authorization.

18 Unique identifiers include international mobile subscriber identity and international mobile equipment identity numbers associated with mobile (cellular) devices.

19 In 2017, the Office of the Privacy Commissioner of Canada investigated the RCMP's use of cell-site simulator technology, pursuant to the *Privacy Act*. A summary of the investigation and its findings are available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/

20 In urgent cases (often referred to as "exigent circumstances"), the RCMP may use cell-site simulator technology without prior judicial authorization, such as a kidnapping, where a victim may be at imminent harm and by reason of exigent

circumstances it would be impracticable to obtain a warrant. The *Criminal Code*, section 529.3, includes a definition of "exigent circumstances" for the purposes of entering a dwelling without a warrant, in addition to Canadian case law interpretations.

21 Innovation, Science and Economic Development Canada is responsible for managing and regulating the radio frequency spectrum in Canada.

22 The RCMP Remotely Piloted Aircraft System Program does not use facial recognition technology as part of its technical capabilities for aerial surveillance.

23 The RCMP Emergency Response Team police officers use tactics, specialized weapons and equipment to resolve high-risk situations. More information on the RCMP Emergency Response Team is available at: https://www.rcmp-grc.gc.ca/ert-gti/index-eng.htm

24 https://www.rcmp-grc.gc.ca/en/remotely-piloted-aircraft-system-rpas-program

25 Information on the RCMP's planned roll-out of body-worn cameras is available at: https://rcmp.ca/en/body-worn-cameras

26 Information on the Automated License Plate Recognition Program in British Columbia is available at: https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=23&languageId=1&contentId=11953

27 https://www.rcmp-grc.gc.ca/en/babel-x-platform

Cat. No. PS64-231/2024E-PDF
ISBN 978-0-660-72509-3