The Digital Panopticon on the Rock: An Analysis of Surveillance, Profiling, and Justice in Canada and Newfoundland and Labrador

Executive Summary

The proliferation of low-cost, high-power digital surveillance technologies has fundamentally altered the relationship between the citizen and the state, creating unprecedented capabilities for monitoring and profiling. This report provides an exhaustive analysis of the architecture, logic, and impact of these systems within the Canadian legal and social context, with a specific focus on the province of Newfoundland and Labrador. The central thesis of this analysis is that the rapid, scalable nature of digital surveillance, combined with lagging legislative and judicial frameworks, creates a significant and growing risk of systemic injustice, manifested in wrongful profiling, the erosion of fundamental privacy rights, and devastating miscarriages of justice.

Part I deconstructs the technical architecture of modern surveillance. It details how commercial data collection techniques—leveraging everything from web trackers to Internet of Things (IoT) devices—have been repurposed for state security, creating sophisticated user profiles through algorithmic inference. These profiles, which treat statistical predictions as factual predicates, are then used by law enforcement agencies employing a new generation of tools. Technologies like geofence warrants, facial recognition, and mass social media monitoring invert traditional investigative principles, shifting from a model of individualized suspicion to one of generalized, data-driven population screening.

Part II examines the Canadian legal landscape, analyzing the tension between these new technologies and the constitutional guarantee of privacy under Section 8 of the *Charter of Rights and Freedoms*. Landmark Supreme Court of Canada decisions, such as *R. v. Spencer* and *R. v. Marakah*, have established a robust, proactive interpretation of the "reasonable expectation of privacy" in the digital realm, emphasizing the

importance of anonymity and control over personal information. This jurisprudence stands in contrast to the often-reactive legal struggles seen in other jurisdictions. The report also scrutinizes the statutory frameworks of the federal *Privacy Act*, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, and the proposed *Artificial Intelligence and Data Act (AIDA)*, highlighting both their protections and their limitations in the face of algorithmic policing.

Part III grounds this national analysis in a detailed case study of Newfoundland and Labrador. It assesses the provincial oversight framework, including the *Access to Information and Protection of Privacy Act, 2015 (ATIPPA)* and the role of the Office of the Information and Privacy Commissioner (OIPC). The technological capabilities of the Royal Newfoundland Constabulary (RNC) and the Royal Canadian Mounted Police (RCMP) are examined, revealing an "oversight paradox" where the most powerful surveillance systems deployed in the province are often procured and overseen at a national level, creating potential gaps in local accountability. This section is contextualized by the legacy of the Lamer Inquiry into the wrongful convictions of Gregory Parsons and Randy Druken, which exposed deep-rooted systemic failures like "tunnel vision" that are at risk of being amplified by biased surveillance technologies.

Part IV explores the profound human cost of these systems. It details the psychological impacts of pervasive surveillance, including the "chilling effect" on free expression and the emergence of "algorithmic anxiety" and "black box gaslighting," where the opacity of systems undermines individual agency and testimonial credibility. The report then quantifies the devastating financial, psychological, and familial trauma of wrongful conviction, using the personal accounts of Parsons and Druken to illustrate the inadequacy of Canada's outdated compensation framework. Finally, it analyzes how surveillance technologies can entrench and amplify systemic racism, particularly the overrepresentation of Indigenous peoples in the Newfoundland and Labrador justice system.

The report concludes with a series of concrete, multi-layered recommendations for a rights-respecting future. These recommendations are directed at legislators, law enforcement agencies, the judiciary, and civil society, and they call for urgent action in four key areas: enacting a moratorium on high-risk technologies until robust legal frameworks are in place; closing legal loopholes that permit warrantless data acquisition; modernizing the compensation system for the wrongfully convicted; and strengthening independent, transparent oversight of all surveillance technologies deployed in Canada.

Part I: The Architecture of Modern Surveillance

The contemporary surveillance landscape is defined by its scale, speed, and subtlety. What was once the domain of targeted, resource-intensive operations has become a system of passive, automated, and continuous data collection and analysis. This transformation has been driven by the convergence of commercial data-gathering practices and state security objectives, creating a powerful infrastructure for monitoring and profiling populations. Understanding this architecture—from the logic of the algorithms to the tools of law enforcement—is essential to grasping its legal and social implications.

1.1. Algorithmic Profiling and Behavioural Inference

At the heart of modern surveillance is the practice of profiling: the automated processing of personal data to evaluate, analyze, or predict aspects of an individual's personality, behaviour, interests, or habits.[1] This process has evolved significantly from early, rudimentary methods to highly sophisticated systems powered by artificial intelligence.

The Logic of Profiling

Historically, web user profiling involved creating simple lists of keywords based on a user's browsing history or entered information.[2] While useful for basic applications like targeted advertising, this method was insufficient for more complex analysis. The modern approach formalizes profiling into a series of subtasks: data extraction, integration of information from disparate sources, and the discovery of user interests and behavioural patterns.[2] The ultimate goal is to construct a dynamic user profile, a rich compilation of information that can be continuously updated to reflect changes in a user's interests and activities.[3] This profile is not merely a collection of raw data; it is itself a new form of personal data, an algorithmic interpretation of an individual's

identity.[1]

Data Collection Mechanisms

The fuel for these profiling engines is a vast and continuous stream of personal data, often collected invisibly and without the user's full comprehension. Every click on a website or swipe on a smartphone can trigger hidden data-sharing mechanisms.[3] Embedded in web pages and applications are invisible scripts known as "trackers," which record user interactions and transmit this information to hundreds of third-party companies.[3] When the same tracker is present across multiple websites, it can build a detailed history of a user's online activities.[3]

This digital dragnet extends far beyond traditional web browsing. It includes data from social media platforms, search engines, and e-commerce sites.[4] The proliferation of the Internet of Things (IoT) has introduced an array of interconnected devices—smart home systems, vehicles, wearable technology, and even appliances—all of which can yield data for an investigation or profile.[4] Cookies, which are small files stored on a user's device, and tracking pixels, tiny images embedded in web pages or emails, are fundamental tools for monitoring user behaviour across these platforms, allowing data brokers to build comprehensive profiles based on browsing history, preferences, and online activities.[4]

Profile Construction Techniques

Once collected, this raw data is processed using various techniques to construct a user profile. One method involves assigning weights to terms or tags; for instance, the frequent use of certain tags can signify a higher user interest in associated topics.[3] More advanced systems employ filtering mechanisms to retrieve pertinent information. A rule-based approach uses a predefined set of "if-then" rules to classify users into categories, such as offering different services based on age and gender.[3] Content-based filtering creates user profiles by comparing item profiles (e.g., of a product or article) with user data to identify preferences.[3]

The most powerful tools in profile construction are Artificial Intelligence (AI) and

Machine Learning (ML). These technologies can analyze vast datasets to identify subtle correlations between different behaviours and characteristics.[1] An algorithm—a sequence of instructions or rules—can be trained on this data to make predictions about an individual's behaviour or to control their access to a service.[1] For example, a system might analyze social media posts for words and phrases that suggest "safe" or "unsafe" driving habits to assign a risk level and set an insurance premium.[1]

From Commercial to State Use

While many of these techniques were developed for commercial purposes, such as delivering more targeted online advertising [2], their application has seamlessly transitioned into the realms of law enforcement and national security. The same logic used to predict a consumer's next purchase can be adapted to predict an individual's likelihood of engaging in criminal activity. Law enforcement agencies now routinely utilize AI technology, including biometric surveillance and predictive policing models, to forecast potential crime areas and identify individuals of interest.[6]

This transition dangerously blurs the line between observed fact and algorithmic inference. The profiling process creates *new* personal data about an individual based on statistical correlations and predictions.[1] When law enforcement relies on this digital evidence, an algorithmic inference—which is fundamentally a probability—is often treated as a factual predicate for suspicion. This creates a significant risk of "automation bias," a phenomenon where human agents place undue trust in the output of a machine, potentially overlooking exculpatory evidence or context. A person is no longer judged solely on their actions, but on what an opaque algorithm

predicts they might do. This represents a fundamental shift in the principles of justice, subtly eroding the presumption of innocence by introducing a pre-emptive, data-driven layer of suspicion.

1.2. Law Enforcement's Digital Toolkit

Building on the foundation of algorithmic profiling, law enforcement agencies in Canada and abroad have adopted a diverse and powerful array of digital surveillance

tools. The deployment of these technologies follows a strategic operational workflow, beginning with the identification of a purpose, gathering intelligence on a subject, selecting appropriate surveillance methods, and culminating in the analysis of collected data to support an investigation.[7]

Geolocation and Proximity Surveillance

One of the most potent and controversial tools is the geofence warrant. This legal instrument instructs a technology company, most notably Google, to search its vast location database—often called the "Sensorvault"—for a list of all devices present within a specified geographic area during a particular time frame.[9] This technology has been used to identify suspects in serious crimes but has also swept up innocent individuals, such as a man who was wrongly implicated in a burglary because his bike ride was tracked through the vicinity of the crime scene.[9] The use of these warrants has skyrocketed, with Google receiving over 11,500 in 2020 alone.[9]

A parallel and equally concerning practice is the circumvention of the warrant process altogether. Law enforcement and other government agencies have been found to simply purchase location data from private data brokers.[10] Companies like Fog Data Science repackage tracking information from smartphone apps and sell police the ability to create "geofences" and query the movement history of any cell phone in a given area, effectively allowing them to "rewind a person's movement through a city" without judicial oversight.[10]

Biometric and Visual Surveillance

Facial recognition technology (FRT) has become a cornerstone of modern visual surveillance. These systems use AI to extract a unique biometric template, or "faceprint," from an image and compare it against a database of known faces, such as a gallery of mug shots.[11] Law enforcement agencies use FRT to identify suspects from CCTV footage, social media images, or even doorbell camera videos.[6] While potentially useful, the technology is fraught with ethical concerns, particularly regarding algorithmic bias, as many systems have been shown to have higher error

rates for racialized individuals and women.[11]

Another pervasive form of visual surveillance is the use of Automatic License Plate Readers (ALPRs). These high-speed cameras, which can be mounted on police cars or stationary objects like traffic lights, capture thousands of license plates per minute, recording the location, date, and time.[14] This data can be stored and aggregated, allowing police to map a driver's typical travel patterns and infer sensitive information, such as where they live or work.[14] Despite their widespread adoption, evidence for their effectiveness in reducing crime is limited, and studies have found significant error rates.[14]

Communications and Online Monitoring

The interception of electronic communications, including text messages, emails, and faxes, remains a key investigative technique, governed by specific legal frameworks that require a high threshold of probable cause.[15] However, law enforcement's online monitoring has expanded far beyond targeted interception. Federal agencies like the RCMP now engage in large-scale "open-source intelligence" (OSINT) gathering.[16] Through programs like "Project Wide Awake," the RCMP has procured services from private sector companies like Babel Street. These services provide a platform to collect and analyze vast amounts of personal information from social media, online forums, location-based services, and even the dark web, all without a warrant.[16]

AI-Driven Behavioural Monitoring

The frontier of law enforcement surveillance is moving towards real-time, AI-driven behavioural monitoring and predictive policing. This involves using algorithms to analyze data and forecast potential crime areas or identify individuals at risk of offending.[6] A clear example of this trend is the RCMP's stated interest in acquiring an "Artificial Intelligence Behaviour Monitoring Solution" for its holding cells. This proposed system would use contactless sensors to monitor the behavioural movements and vital signs of individuals in custody, alerting personnel to "concerning and/or destructive behaviour" or life-threatening medical distress.[17] While framed as a safety measure, such a system represents a profound intrusion into an individual's

physical and psychological state, using AI to interpret and flag behaviour deemed abnormal.

The adoption of these mass surveillance tools represents a fundamental inversion of traditional investigative principles. Historically, policing began with a crime, and the investigation sought to identify a suspect through evidence. Tools like geofence warrants and city-wide FRT networks reverse this logic. They begin with a vast dataset of a population's movements and activities and search within it for a potential suspect, effectively treating everyone within the digital dragnet as a person of interest until proven otherwise.[18] This shift from a presumption of innocence to a presumption of data-driven suspicion has profound implications for civil liberties, transforming the very nature of the relationship between the citizen and the state in the digital age.

Table 1: Comparison of Surveillance Technologies Used by Law Enforcement

Technology	Primary Function	Data Source(s)	Key Legal/Ethical Concern	Relevant Canadian Context/Case Law
Geofence Warrant	Identifies all mobile devices within a specific geographic area during a set time period.	Technology company location databases (e.g., Google's Sensorvault).	Lack of particularized suspicion; treats innocent bystanders as suspects; digital "general warrant."	No direct SCC ruling; principles from *R. v. Spencer* on REOP in location data are highly relevant.
Facial Recognition Technology (FRT)	Identifies or verifies individuals by comparing their facial features to a database of known faces.	CCTV footage, social media, mugshot databases, driver's license photos.	Algorithmic bias (higher error rates for racialized groups and women); potential for mass surveillance; chilling effect on public assembly.	OPC investigation into RCMP's use of Clearview AI; RCMP National Technology Onboarding Program (NTOP) established in response.[20]
Automatic	Captures and	Mobile and	Mass collection	Governed by

License Plate Reader (ALPR)	logs license plates, creating a searchable database of vehicle locations and movements.	stationary cameras on public roads and infrastructure.	and long-term retention of location data of innocent individuals; potential for mapping personal patterns and associations.	provincial privacy acts (*ATIPPA* in NL) for police use; raises Section 8 *Charter* concerns.
OSINT Platforms (e.g., Babel X)	Aggregates and analyzes publicly accessible information from the internet for intelligence gathering.	Social media, forums, dark web, fee-for-access private databases.	Legality and ethics of scraping data; collection of information on individuals not suspected of a crime; lack of transparency and oversight.	OPC investigation into RCMP's "Project Wide Awake" found inadequate due diligence on data sources.[16]
AI Behavioural Monitoring	Uses AI to analyze behaviour and vital signs to detect concerning activity or medical distress in real-time.	Contactless sensors (video, thermal, etc.) in controlled environments (e.g., holding cells).	Highly invasive monitoring of physical and psychological states; potential for biased or inaccurate algorithmic interpretation of behaviour.	RCMP has issued a call for such a solution, which must comply with the *Privacy Act* and *Directive on Automated Decision-Making*.[17]

Part II: The Canadian Legal Landscape: Privacy and Policing in the Digital Age

The rapid evolution of surveillance technology has presented a profound challenge to Canada's legal frameworks, which were largely conceived in an analog era. The judiciary and legislature have been tasked with adapting long-standing principles of privacy and justice to a world of intangible data, borderless networks, and algorithmic

decision-making. This section analyzes the key constitutional and statutory instruments that form the Canadian legal landscape for digital surveillance, highlighting the ongoing struggle to maintain a balance between legitimate law enforcement needs and the fundamental rights of individuals.

Table 2: Key Canadian Privacy Legislation and Application

Legislation	Scope of Application	Key Principle/Requirement	Relevance to Surveillance
***Charter of Rights and Freedoms*, Section 8**	Constitutional right protecting individuals from unreasonable search and seizure by the state.	Establishes the "Reasonable Expectation of Privacy" (REOP) as the threshold for state intrusion. A search without a warrant is presumptively unreasonable.	Sets the fundamental constitutional standard that all police surveillance activities must meet. Defines the scope of privacy in digital data, communications, and location.
Privacy Act	Governs the collection, use, and disclosure of personal information by federal government institutions.	Collection must be directly related to an operating program. Use and disclosure are strictly limited, especially without consent.	Directly regulates the data handling practices of federal agencies like the RCMP and CSIS, including their use of surveillance technologies and OSINT programs.
PIPEDA	Governs how private-sector organizations collect, use, and disclose personal information in the course of commercial activities.	A consent-based model requiring knowledge and consent for data handling, with specific, limited exceptions.	Governs how police can access personal information held by private companies (e.g., ISPs, social media platforms, data brokers).
Artificial Intelligence and Data Act (AIDA) (Proposed)	Would regulate the design, development, and deployment of "high-impact" AI	A risk-management framework requiring accountability, transparency,	Intended to provide a future regulatory framework for the algorithmic profiling

	systems in the private and public sectors.	fairness, and human oversight for high-impact AI.	and predictive policing systems used in surveillance.

2.1. The Charter's Digital Shield: Section 8 and the "Reasonable Expectation of Privacy"

The cornerstone of privacy protection in Canada is Section 8 of the *Canadian Charter of Rights and Freedoms*, which guarantees that "[e]veryone has the right to be secure against unreasonable search or seizure".[21] The Supreme Court of Canada (SCC) has interpreted this provision as a safeguard for people, not places, protecting a sphere of individual autonomy within which citizens have the right "to be let alone".[22] Crucially, the purpose of Section 8 is preventative; it is designed to "intercept unjustified searches or seizures before they... take place," not merely to assess their validity after the fact.[22]

The application of Section 8 hinges on whether a state action constitutes a "search" or "seizure." This occurs whenever the state intrudes upon an individual's "reasonable expectation of privacy" (REOP).[21] To determine if a REOP exists, the SCC has established a contextual, substance-over-form analysis known as the "totality of the circumstances" test. This test is guided by four main lines of inquiry:

1. **The subject matter of the search:** What information was being sought, and what does it tend to reveal about an individual? [22]
2. **The claimant's direct interest:** Did the search implicate the claimant's personal privacy rights? [22]
3. **The claimant's subjective expectation of privacy:** Did the individual believe the information was private? [22]
4. **The objective reasonableness of that expectation:** Would a reasonable person in the same situation consider the expectation of privacy to be legitimate? [22]

In the digital age, the concept of "informational privacy" has become central to this analysis. The SCC has recognized that Section 8 protects a "biographical core of personal information," which includes details about an individual's lifestyle, personal choices, and intimate relationships that they would not want disseminated to the state.[22] This core concept has been further refined to include three overlapping ideas: privacy as secrecy (the right to keep information confidential), privacy as control (the

right to determine how one's information is used), and, critically for the online world, privacy as anonymity (the ability to engage in activities without being identified).[22]

2.2. Landmark Jurisprudence: Applying the Charter to New Technologies

The SCC has applied these principles to new technologies in a series of landmark cases that have progressively fortified Canadians' digital privacy rights.

R. v. Spencer **(2014):** This unanimous decision is arguably the most important digital privacy ruling in Canadian history. The case involved police asking an Internet Service Provider (ISP) for the subscriber information (name and address) associated with an IP address used to download child pornography.[26] The Court found that individuals have a REOP in this information. Justice Cromwell, writing for the Court, rejected the narrow view that the search was merely for a name and address. Instead, he adopted a "broad and functional approach," defining the subject matter as the identity of an internet user linked to their online activity.[26] The Court held that this information touches the "biographical core" because it can reveal intensely private information about a user's lifestyle and personal choices.[25] The decision's most significant contribution was its robust recognition of "privacy as anonymity." The Court affirmed that internet users expect their online activities to be anonymous, and this expectation is reasonable even when those activities occur in a public or semi-public digital space. The act of linking an anonymous online persona to a real-world identity was deemed a significant intrusion that engages Section 8 protection, thus requiring prior judicial authorization (a warrant).[25]

R. v. Marakah **(2017):** In this case, the SCC addressed whether an individual retains a REOP in text messages after they have been sent and are stored on the recipient's device.[28] The police had searched the accomplice's phone and found incriminating messages sent by Marakah. The majority of the Court found that Marakah did have a REOP. Chief Justice McLachlin emphasized that the true subject matter of the search was not the physical device, but the "electronic conversation" itself.[24] The Court acknowledged that by sending a message, the sender loses some control and accepts the risk that the recipient might share it. However, it drew a crucial distinction: accepting the risk of disclosure by a private individual is not the same as accepting the risk of warrantless state intrusion.[24] By choosing a private medium to communicate with a specific person, the sender maintains a reasonable expectation that the state

will not be listening in without lawful authority.[24]

These decisions reveal a proactive judicial philosophy. The SCC in *Hunter v. Southam* established Section 8's preventative purpose.[22] The rulings in

Spencer and *Marakah* apply this principle by anticipating and closing off potential loopholes for warrantless state access to digital information. Rather than waiting for the harms of a new surveillance technique to become widespread, the Court has tended to define privacy rights robustly at the outset. This proactive stance suggests that indiscriminate, mass surveillance tools like geofence warrants would face significant constitutional hurdles in Canada. Such a tool, which searches the data of everyone in a given area without individualized suspicion, appears fundamentally incompatible with the preventative, targeted nature of a reasonable search as envisioned by the SCC. This contrasts sharply with the situation in the United States, where a circuit court split highlights a more reactive struggle to fit these new technologies into existing legal doctrines.[9]

2.3. Statutory Guardrails: The *Privacy Act* and *PIPEDA*

Beyond the constitutional framework of the *Charter*, federal statutes provide additional layers of protection for personal information.

The ***Privacy Act*** governs how federal government institutions, including the RCMP and the Canadian Security Intelligence Service (CSIS), handle personal information.[30] It stipulates that an institution may only collect personal information that is "directly related to an operating program or activity of the institution".[31] Disclosure of this information without the individual's consent is strictly limited. For law enforcement purposes, disclosure is permitted to another government institution that has identified its lawful authority and has requested the information for the purpose of enforcing a law or gathering intelligence.[31] However, this does not grant police a blanket authority to collect information.

The ***Personal Information Protection and Electronic Documents Act (PIPEDA)*** applies to private-sector organizations engaged in commercial activities.[31] It is built on a consent-based model, meaning organizations must generally obtain an individual's knowledge and consent for the collection, use, or disclosure of their personal information.[32]

PIPEDA contains several specific exemptions that allow disclosure to law enforcement without consent. For instance, an organization *may* disclose information if a government institution requests it for law enforcement purposes and identifies its lawful authority, or if the organization itself has reasonable grounds to believe the information relates to the contravention of a law.[25]

The interaction between these statutes and the *Charter* was a central issue in *R. v. Spencer*. The Crown argued that the police request for subscriber data was authorized by the law enforcement disclosure provision in *PIPEDA*. The SCC decisively rejected this argument, ruling that *PIPEDA*'s permissive disclosure clause does not create a "lawful authority" for police to obtain information where a REOP exists.[25] In essence, the Court affirmed that a statute cannot authorize what the Constitution forbids. The existence of a REOP under the

Charter is the determinative factor, and if one exists, police must obtain a warrant.

2.4. Regulating the Algorithm: Canada's Proposed *Artificial Intelligence and Data Act (AIDA)*

Recognizing the unique challenges posed by AI, the Government of Canada tabled the *Artificial Intelligence and Data Act (AIDA)* as part of Bill C-27 in 2022.[34] AIDA represents Canada's first attempt at a comprehensive, risk-based regulatory framework for AI. The Act is intended to protect Canadians from harms and discriminatory outcomes while encouraging responsible innovation.[34]

AIDA's core provisions would apply to what it defines as "high-impact" AI systems. While the exact definition is left to future regulations, these are generally understood to be systems that could have significant effects on health, safety, or human rights, such as those used in law enforcement, employment, or access to services. For these systems, AIDA would impose several key requirements on the organizations that design or deploy them [34]:

- **Accountability:** Organizations must establish governance mechanisms and document their compliance with legal obligations.
- **Transparency:** The public must be provided with plain-language information about how high-impact systems are being used, including their capabilities and limitations.
- **Fairness and Equity:** Systems must be built with an awareness of potential

discriminatory outcomes, and measures must be taken to mitigate such biases.
- **Human Oversight and Monitoring:** Systems must be designed to enable meaningful human oversight and monitoring of their outputs.
- **Safety:** Systems must be proactively assessed to identify and mitigate risks of harm, including from foreseeable misuse.

The Act proposes the creation of an AI and Data Commissioner to support the Minister of Innovation, Science and Industry in overseeing the regime. The Minister would have the power to order the cessation of a system's use or to publicly disclose information about contraventions to prevent harm.[34]

However, the progress of AIDA has been slow. As of early 2025, Bill C-27 had died on the order paper due to the prorogation of Parliament, meaning the legislative process must restart.[36] In the interim, the Office of the Privacy Commissioner of Canada (OPC) has issued guidance on the responsible use of generative AI, providing principles on legal authority, consent, accountability, and transparency that serve as a temporary framework for organizations navigating this new technological landscape.[38]

Part III: A Provincial Case Study: Surveillance and Justice in Newfoundland and Labrador

While the constitutional and federal statutory frameworks set the national stage, the practical application of surveillance technologies and the administration of justice occur at the provincial and local levels. Newfoundland and Labrador provides a compelling case study, with its unique policing structure, a history of profound miscarriages of justice that have shaped its legal culture, and an active provincial oversight body.

3.1. Provincial Oversight: *ATIPPA* and the Role of the OIPC

The primary legislative instrument governing privacy at the provincial level is the *Access to Information and Protection of Privacy Act, 2015 (ATIPPA)*.[41] This Act serves a dual purpose: it grants the public a right of access to records held by public bodies

while simultaneously protecting the privacy of individuals by regulating how their personal information is collected, used, and disclosed.[41] Public bodies covered by the Act, which include provincial government departments and law enforcement agencies like the Royal Newfoundland Constabulary (RNC), may only collect personal information if it is expressly authorized by an Act, collected for law enforcement purposes, or is directly related to and necessary for an operating program.[41]

Oversight and enforcement of *ATIPPA* are the responsibility of the Office of the Information and Privacy Commissioner (OIPC) of Newfoundland and Labrador, an independent office of the House of Assembly.[41] The OIPC's mandate includes investigating complaints from the public regarding access to information requests and potential privacy breaches, receiving mandatory privacy breach notifications from public bodies, and conducting "own motion" investigations where it deems necessary.[41]

The OIPC's oversight of the RNC is documented in its public investigation reports. For example, in Report A-2024-011, the Commissioner reviewed the RNC's decision to redact portions of an investigation file requested under *ATIPPA*. While the OIPC found that the RNC had properly withheld some information under exceptions for legal advice and harm to law enforcement, it disagreed with other redactions and recommended the disclosure of the remaining information.[44] In another case, Report A-2025-001, the OIPC recommended the RNC disclose records to a complainant who had created and provided the records themselves, concluding the RNC had improperly withheld them.[45] These reports demonstrate the OIPC's role as a mechanism for public accountability. However, a review of publicly available reports reveals a notable absence of investigations specifically focused on the RNC's use of surveillance technologies, representing a potential gap in transparency and oversight in this critical area.[47]

3.2. Policing on the Rock: RNC and RCMP Capabilities

Policing in Newfoundland and Labrador is divided between the provincial RNC, which serves major urban areas like the St. John's metropolitan region and Corner Brook, and the Royal Canadian Mounted Police (RCMP), which polices the remainder of the province under a contract agreement.

The RNC's Criminal Investigation Division includes specialized units equipped to

handle digital evidence. The Technical Investigation Unit focuses on supporting investigations through the use of "electronic investigative techniques," while the Computer Forensics Unit is responsible for the seizure, extraction, and forensic examination of data from computers, cell phones, and other digital devices.[49] The RNC has also adopted modern technology for crime scene analysis, such as a new 3D laser scanner that can create detailed models of a scene for visualization in court.[50] Despite these capabilities, there is a notable lack of publicly accessible strategic plans or recent annual reports from the RNC, limiting public insight into its long-term technological and operational priorities.[51]

The RCMP, operating as the provincial police force in many areas, brings with it the full technological capacity of a national law enforcement agency. Its national Technical Investigation Services provides leadership in surveillance technology and techniques.[58] This includes controversial programs like "Project Wide Awake," which leverages private-sector OSINT tools like Babel X to conduct mass data collection from online sources.[16] The use of such powerful, privacy-invasive technologies by the RCMP is subject to federal oversight. The Treasury Board of Canada Secretariat requires federal institutions to conduct a Privacy Impact Assessment (PIA) for any new or substantially modified program that involves personal information, to identify and mitigate privacy risks.[59]

This dual-policing structure creates a potential "oversight paradox." The RNC, as a provincial public body, is directly and primarily accountable to the provincial OIPC under *ATIPPA*. However, the most advanced and potentially intrusive surveillance systems deployed within the province are often those procured and managed by the RCMP at a national level. The primary investigation and oversight of these national RCMP programs fall to the federal Privacy Commissioner under the *Privacy Act*, as seen in the investigation into Project Wide Awake.[16] This fragmentation means that residents of Newfoundland and Labrador are subject to surveillance from technologies vetted and scrutinized by a federal body, potentially creating a disconnect in local accountability and a challenge for the provincial OIPC, which may lack the jurisdiction or technical capacity to fully assess the national-level systems operating within its borders.

3.3. The Lamer Inquiry: A Legacy of Wrongful Conviction and Systemic Reform

The contemporary justice system in Newfoundland and Labrador cannot be

understood without acknowledging the profound impact of the Commission of Inquiry into the proceedings pertaining to Gregory Parsons, Randy Druken, and Ronald Dalton, led by former Supreme Court Chief Justice Antonio Lamer. The inquiry, which released its report in 2006, investigated three separate and devastating miscarriages of justice that exposed deep systemic flaws in the province's policing and prosecution services.[61]

Gregory Parsons was wrongfully convicted in 1994 for the 1991 murder of his mother, Catherine Carroll.[64] Randy Druken was wrongfully convicted in 1995 for the 1993 murder of his girlfriend, Brenda Young.[65] Both convictions were the result of flawed investigations and prosecutions that ultimately collapsed under the weight of new evidence, including DNA testing that exonerated both men.[64]

The Lamer Report's central finding was that the investigations and prosecutions were plagued by "tunnel vision," a mindset where police and Crown attorneys become so focused on a single suspect that they fail to properly investigate other leads and interpret all evidence, whether inculpatory or exculpatory, through a lens of presumed guilt.[62] In the Parsons case, Lamer described the investigation as a "'runaway train,' fuelled by tunnel vision".[63] In the Druken case, the inquiry found there was "no reliable evidence" for the prosecution, which relied heavily on the testimony of a jailhouse informant who later recanted.[66] The report also identified a problematic "Crown culture" that contributed to the wrongful convictions.[62]

The inquiry produced 45 recommendations for comprehensive reform of the justice system, targeting police, prosecutors, and the judiciary.[62] One of the most direct and tangible outcomes of the inquiry was the RNC's decision to overhaul its investigative interviewing techniques. In response to Lamer's critique of confrontational and accusatory methods that reinforce tunnel vision, the RNC became the first police force in North America to adopt the PEACE model of interviewing.[70] This method emphasizes

Preparation and planning, **E**ngage and explain, obtaining an **A**ccount, **C**losure, and **E**valuation, promoting a more open-minded, information-gathering approach over a confession-driven one.[70] The legacy of the Lamer Inquiry serves as a stark warning of the catastrophic human cost of systemic failures in the justice system—a warning that resonates powerfully in an era where biased algorithms and indiscriminate digital surveillance threaten to create new, technologically-driven forms of tunnel vision.

Part IV: The Human Cost: Social and Psychological Impacts of Surveillance and Misidentification

Beyond the abstract realms of technology and law lies the tangible human impact of digital surveillance and wrongful profiling. The knowledge of being constantly watched alters behaviour and strains mental well-being, while the consequences of a system that errs—producing a wrongful accusation or conviction—are catastrophic and life-altering. This section examines these profound costs, from the subtle psychological pressures of the observer effect to the devastating, multi-generational trauma of a miscarriage of justice.

4.1. The Psychology of Being Watched: The Observer Effect and the Chilling Effect

The very act of observation changes the behaviour of the observed. This phenomenon, known in social sciences as the Hawthorne Effect or the Observer Effect, posits that individuals modify their behaviour in response to their awareness of being watched.[71] While first identified in industrial productivity studies, this effect is a fundamental outcome of pervasive surveillance.[75] In a society saturated with CCTV, location tracking, and online monitoring, this awareness can lead to "surveillance-induced conformity," where people alter their actions—from what they post on social media to how they behave in public spaces—out of a desire to conform to social expectations or a fear of judgment.[76]

This conformity has a corrosive impact on democratic freedoms, creating a "chilling effect" on expression and association.[77] When citizens know that facial recognition cameras may be present at a public protest, or that their online discussions are being monitored, they may be deterred from exercising their fundamental rights to assembly and free speech.[77] This self-censorship erodes the open discourse essential to a functioning democracy.

The psychological harms are not limited to behavioural changes. The constant awareness of being monitored increases an individual's "cognitive load"—the mental effort required to process information—leading to mental fatigue, stress, and impaired decision-making over time.[76] Studies have shown a direct correlation between electronic monitoring in the workplace and poor mental health, with monitored

employees reporting higher levels of stress, anxiety, and burnout.[78] This surveillance-related stress can escalate to paranoia and a diminished sense of autonomy and privacy, fundamentally altering how individuals experience the world.[76]

As surveillance systems become more complex and opaque, new forms of psychological harm are emerging. The concept of "algorithmic anxiety" describes the stress associated with being subject to the decisions of inscrutable algorithms. This is compounded by what researcher Kelley Cotter terms "black box gaslighting".[80] This phenomenon occurs when individuals experience what they believe to be algorithmic bias or suppression (such as the "shadowbanning" of their social media content), only to have the platform deny their reality, citing the technical complexity of their "black box" systems.[80] This dynamic, where an individual's lived experience is invalidated by an unaccountable technological authority, creates profound self-doubt and undermines the ability to hold powerful systems accountable.[80]

This erosion of testimonial credibility represents a significant threat to social justice advocacy. Historically, movements for social change, from the American Civil Rights Movement to anti-colonial struggles, have been fueled by the power of "prophetic testimony"—the clear, morally charged articulation of lived experience to expose and challenge systemic injustice.[81] Figures like Fannie Lou Hamer and Mamie Till-Bradley used their personal stories of suffering to confront the conscience of a nation and demand change.[81] This form of advocacy depends on the perceived credibility of the witness. Today, however, the architecture of digital surveillance and algorithmic opacity creates a powerful tool for invalidating such testimony. When marginalized individuals report experiences of algorithmic bias or disproportionate surveillance, their claims can be dismissed by the opaque authority of the "black box." This is a modern, technological form of gaslighting that does not just silence dissent but actively works to dismantle the speaker's reality, striking at the very foundation of testimony-based social justice work.[80]

4.2. The Trauma of Wrongful Conviction: Costs and Consequences

When surveillance and profiling systems fail, the result can be a wrongful accusation and, in the most extreme cases, a wrongful conviction. The consequences of such a miscarriage of justice are devastating, inflicting deep and lasting harm on the individual, their family, and society at large.

The financial toll is staggering. The average cost of a single wrongful conviction in the United States has been estimated at $6.1 million, a figure that includes not only direct compensation but also state costs for incarceration and legal proceedings.[84] For the exonerated individual, the economic impact is catastrophic, encompassing years of lost wages, depleted family savings on legal fees, and severely diminished career prospects due to the stigma of incarceration.[86] The cost to the state is also immense. The average cost of a year in a Canadian federal prison is over $159,000 ($436 per day), meaning a decade of wrongful incarceration represents well over $1.5 million in direct costs alone, not including policing and court expenses.[85]

These financial figures, however, pale in comparison to the psychological scars. Research on the mental health of exonerees reveals a public health crisis. Studies have found that wrongfully convicted individuals experience rates of depression four times higher, anxiety seven times higher, and Post-Traumatic Stress Disorder (PTSD) eleven times higher than the general population.[88] A UK-based study found that a majority of exonerees met the diagnostic criteria for "enduring personality change following catastrophic experience," a condition with symptoms similar to those observed in war veterans.[89] These traumas are compounded by the unique injustice of their situation, leading to chronic sleep problems, paranoia, and a profound sense of mistrust.[90]

The trauma extends beyond the individual, inflicting what has been described as a "collective trauma" upon their families.[92] Wrongful conviction destabilizes families emotionally and financially. Children of the wrongfully convicted suffer the trauma of separation and stigma, which are strong risk factors for adverse life outcomes.[85] The relationships that survive the initial shock often deteriorate over the long years of imprisonment, as family members grow weary or are forced to move on with their lives, leaving the incarcerated individual in a state of profound isolation.[92] Upon release, rebuilding these fractured ties is immensely difficult, as exonerees grapple with their own trauma and a sense of social displacement, often feeling like strangers to their own families.[92]

The experiences of Gregory Parsons and Randy Druken in Newfoundland and Labrador provide a stark, localized illustration of this devastation. Parsons, convicted of murdering his mother, spent years under a cloud of suspicion in his community, a trauma compounded by the fact that his supposed friend was the real killer.[64] He has described his decades-long fight for justice as a "never-ending nightmare".[93] Druken, who spent over six years in prison for a murder he did not commit, described his life as an "absolute nightmare" and told the Lamer Inquiry that the process "tore my family apart".[94] His wrongful conviction was a catalyst for a series of family tragedies,

including the death of one brother and the murder of another by a third brother.[66]

For the few who receive it, financial compensation is often an inadequate and fraught remedy. Canada's federal-provincial compensation guidelines, established in 1988, are widely seen as outdated and overly restrictive. They provide for minimal compensation, have not been adjusted for economic realities, and impose a difficult-to-meet requirement for a declaration of factual innocence.[97] This has led to an inconsistent system where many exonerees receive no compensation at all, a failure that the United Nations Human Rights Committee has found to be in breach of Canada's treaty obligations.[97] Even when compensation is awarded, as in the cases of Parsons ($1.3 million) and Druken ($2 million), exonerees have stated that no amount of money can make up for the lost years and the enduring trauma.[65]

Table 3: The Costs of Wrongful Conviction in Newfoundland and Labrador

Exoneree	Years Imprisoned	Key Cause of Wrongful Conviction	Total Financial Compensation	Documented Psychological/Social Impact	Key Lamer Inquiry Finding
Gregory Parsons	68 days (plus 7 years under suspicion)	Police and Crown "tunnel vision"; reliance on flimsy, circumstantial evidence (e.g., a song lyric).	$1.3 million	Enduring public suspicion; prolonged battle for justice; profound personal trauma from discovering his mother's body and being accused of her murder.	The investigation and prosecution became a "'runaway train,' fuelled by tunnel vision".[63]
Randy Druken	Over 6 years	Reliance on testimony from a jailhouse informant who later	$2.0 million	Described his life as an "absolute nightmare"; the process "tore my	There was "no reliable evidence" for the prosecution, and he

		recanted; failure to disclose exculpatory DNA evidence.		family apart," leading to further violence and tragedy within his family.	should never have been charged.[63]

4.3. Systemic Bias and Disproportionate Harms

The harms of surveillance and wrongful profiling are not distributed equally across society. Instead, they disproportionately impact already marginalized communities, amplifying existing patterns of discrimination within the justice system.

In Canada, the most glaring example of this is the staggering overrepresentation of Indigenous peoples in the correctional system. While Indigenous people make up approximately 5% of the Canadian population, they account for over 32% of the federal prison population.[100] The situation is even more acute for Indigenous women, who represent 43% of female custody admissions, and Indigenous youth.[102] These statistics are the result of complex, intersecting factors, including the intergenerational trauma of colonialism, residential schools, socio-economic marginalization, and systemic racism within the justice system.[102]

In Newfoundland and Labrador, this national crisis is reflected locally. The province has a long and complicated history of relations with its Indigenous peoples—including the Mi'kmaq, Innu, and Inuit—who were largely omitted from the Terms of Union when the province joined Canada in 1949, denying them access to federal programs and recognition for decades.[107] This legacy of neglect has contributed to the challenges faced by Indigenous communities within the provincial justice system. In response, community-led initiatives and government funding are beginning to address these issues. The federal government has provided over $1.16 million to the Nunatsiavut Government to support community-based justice services and an Inuit Cultural Awareness Educator to train justice professionals.[101] In St. John's, organizations like First Light provide culturally grounded support for Indigenous people navigating the justice system, while Community Justice Connect offers restorative justice services to address conflicts involving racism.[111]

The danger is that new surveillance technologies, rather than being neutral tools, will

serve to amplify these existing biases. Facial recognition systems trained on datasets that are imbalanced and disproportionately feature white individuals have been shown to have higher false positive rates for racialized people, particularly Black women.[11] When law enforcement uses these flawed tools, they risk reinforcing patterns of elevated scrutiny on marginalized communities.[11] Similarly, predictive policing algorithms, which are trained on historical crime data, can create a feedback loop. If a neighborhood has been historically over-policed, the data will reflect higher arrest rates, leading the algorithm to recommend even more patrols in that area, which in turn generates more arrests, "justifying" the initial bias.[77] This process can entrench and provide a veneer of technological objectivity to discriminatory policing practices.

Recognizing these dangers, the 2021 House of Commons report, *Systemic Racism in Policing in Canada*, issued a series of recommendations aimed at fundamental reform. Crucially, the report called for the development of an Indigenous Police Services Framework to promote self-determination and self-governance over policing, and for the transition of the RCMP to a police service model with robust civilian oversight to ensure its policies and operations are free from systemic bias.[114] These recommendations underscore the reality that addressing the harms of surveillance cannot be separated from the broader project of confronting systemic racism in the justice system.

Part V: Synthesis and Recommendations for a Rights-Respecting Future

The preceding analysis reveals a critical juncture in the evolution of surveillance and justice in Canada. The rapid deployment of powerful, low-cost technologies has created a significant imbalance, where the state's capacity for monitoring has far outpaced the legal and social structures designed to protect fundamental rights. The legacy of wrongful convictions in Newfoundland and Labrador serves as a potent reminder of the catastrophic human cost when these structures fail. To restore balance and ensure a rights-respecting future, a concerted and multi-faceted response is required from all actors within the justice system.

5.1. Bridging the Gaps: A Synthesis of Key Challenges

Four key challenges emerge from this report that must be addressed to mitigate the risks of digital surveillance and wrongful profiling.

- **The Technology-Law Lag:** There is a persistent and widening gap between the pace of technological innovation and the ability of legislatures and courts to develop adequate safeguards. While the Supreme Court of Canada has established strong foundational principles for digital privacy, these principles are being tested by novel tools like geofence warrants and AI-driven predictive systems for which specific legal rules do not yet exist.
- **The Transparency Deficit:** The effectiveness of many surveillance systems relies on their complexity and opacity. "Black box" algorithms and secretive procurement of private-sector surveillance services create a significant transparency deficit, making it nearly impossible for the public, oversight bodies, and even the courts to meaningfully assess their legality, accuracy, and potential for bias. This undermines public trust and cripples accountability.
- **The Oversight Mismatch:** In provinces like Newfoundland and Labrador with a dual-policing structure, there is a jurisdictional mismatch in oversight. The most technologically advanced and privacy-invasive systems are often deployed by the RCMP, a national force whose programs are primarily reviewed by the federal Privacy Commissioner. This can leave provincial oversight bodies without the jurisdiction or technical capacity to scrutinize technologies being used on their own citizens, fragmenting accountability.
- **The Human Cost Imperative:** The discourse around surveillance technology often focuses on its efficiency and effectiveness in fighting crime. This analysis has demonstrated that the human costs of error—wrongful profiling, psychological trauma, and the complete devastation of a wrongful conviction—are profound and often irreparable. Any cost-benefit analysis of these technologies must prioritize these human costs, recognizing that financial compensation is an inadequate remedy for a life derailed by a miscarriage of justice.

5.2. Policy Recommendations

Based on this synthesis, the following recommendations are proposed to guide reform

at the legislative, operational, judicial, and community levels.

For Federal and Provincial Legislatures:

1. **Enact a Moratorium on High-Risk Technologies:** Implement a national and provincial moratorium on the use of live, real-time facial recognition technology in public spaces by law enforcement. This moratorium should remain in effect until a clear, robust, and publicly debated legislative framework is established that defines its permissible uses, establishes strict necessity and proportionality requirements, and ensures compliance with the *Charter of Rights and Freedoms*.
2. **Legislate Against the Data Broker Loophole:** Introduce federal legislation, modeled on the principles of the proposed U.S. "Fourth Amendment Is Not For Sale Act" [10], to explicitly prohibit law enforcement and intelligence agencies from purchasing personal information from data brokers when a warrant would otherwise be required to obtain that information directly. This would close a critical loophole that allows for the circumvention of judicial oversight.
3. **Modernize Wrongful Conviction Compensation:** Repeal the outdated 1988 federal-provincial compensation guidelines and enact comprehensive legislation to create a fair, consistent, and accessible compensation system for the wrongfully convicted. This new system should include provisions for automatic, immediate financial and social service assistance upon release, remove restrictive eligibility criteria that demand a formal declaration of innocence, and ensure that compensation awards are not capped and truly reflect the profound economic, psychological, and social harms endured.[115]
4. **Expedite and Strengthen AIDA:** Prioritize the reintroduction and passage of a strengthened *Artificial Intelligence and Data Act*. The Act should be amended to include a specific, high-risk category for AI systems used for law enforcement, predictive policing, and justice system applications. This category should trigger mandatory, independent, and public audits for accuracy, discriminatory impact, and human rights compliance before any such system can be deployed.

For Law Enforcement Agencies (RNC, RCMP):

5. **Mandatory and Transparent Privacy Impact Assessments (PIAs):** Mandate

the completion of a comprehensive PIA for *all* new surveillance technologies *before* procurement or deployment. These PIAs must be submitted to the relevant federal or provincial privacy commissioner for binding review and comment, and a public summary of the PIA and the commissioner's response must be released to ensure transparency.

6. **Adopt the Lamer Inquiry's Spirit:** Move beyond the letter of the Lamer Inquiry's recommendations to embrace its core spirit. This involves establishing internal "red team" protocols, where a separate team of investigators is tasked with actively challenging the primary investigative theory in any major case. This institutionalizes a mechanism to combat the "tunnel vision" that the inquiry identified as a key contributor to wrongful convictions.[63]
7. **Enhance Data Governance and Public Reporting:** Develop and publish clear, public-facing policies for each surveillance technology in use (e.g., ALPRs, drones, body-worn cameras). These policies must specify the purpose of the technology, strict data retention limits, criteria for data sharing, and procedures for data deletion to prevent the creation of indefinite, de facto population databases. An annual public report should be issued detailing the use of these technologies and the data collected.

For the Judiciary and Crown Prosecutors:

8. **Develop Judicial Guidance for New Warrants:** In the absence of legislative reform, judicial bodies should develop specific guidance or practice directives for assessing warrant applications involving novel surveillance techniques. For geofence or similar "digital dragnet" warrants, this guidance should require police to demonstrate not only probable cause that a crime was committed but also that the proposed search is the least intrusive means available, is narrowly tailored in time and geography to a high degree of specificity, and includes a multi-step process with ongoing judicial supervision to minimize the impact on innocent third parties.
9. **Scrutinize Algorithmic Evidence:** The judiciary and Crown should approach evidence derived from AI and algorithmic profiling with extreme caution. This requires promoting judicial education on the functioning and limitations of these technologies. A higher threshold for the admissibility of such evidence should be established, requiring the Crown to provide full disclosure of the algorithm's methodology, known error rates, training data, and potential for demographic

bias, allowing the defence to meaningfully challenge its reliability.

For Civil Society and Oversight Bodies:

10. **Strengthen Inter-Jurisdictional Oversight Cooperation:** Establish a formal working group or memorandum of understanding between the Office of the Privacy Commissioner of Canada and all provincial and territorial privacy commissioners. The purpose of this group would be to share technical expertise, develop joint investigative protocols, and create a unified oversight framework for national surveillance technologies (like those used by the RCMP and CSIS) that are deployed at the local level, thereby closing the "oversight paradox."
11. **Support Community-Based Justice Initiatives:** Federal and provincial governments must provide increased, stable, and long-term core funding to community-based organizations that support individuals navigating the justice system and work to mitigate the harms of over-policing and wrongful conviction. This includes organizations like the John Howard and Elizabeth Fry Societies, and Indigenous-led organizations such as First Light in St. John's, whose culturally grounded programs are essential to addressing the systemic overrepresentation of Indigenous peoples in the justice system.

Works cited

1. What is automated individual decision-making and profiling? | ICO, accessed July 19, 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/
2. A Combination Approach to Web User Profiling - Jing Zhang, accessed July 19, 2025, https://xiaojingzi.github.io/publications/TKDD11-Tang-et-al-web-user-profiling.pdf
3. Guarding Digital Privacy: Exploring User Profiling and Security Enhancements - arXiv, accessed July 19, 2025, http://www.arxiv.org/pdf/2504.07107
4. The Ultimate Guide to Online Surveillance - Number Analytics, accessed July 19, 2025, https://www.numberanalytics.com/blog/ultimate-guide-online-surveillance
5. Digital Evidence - Major Cities Chiefs Association, accessed July 19, 2025, https://majorcitieschiefs.com/wp-content/uploads/2024/10/MCCA-Digital-Evidence-White-Paper-_-Oct-2024.pdf
6. The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent - PubMed Central,

accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12116099/
7. The Art of Surveillance: Tips and Techniques for Private Investigators, accessed July 19, 2025, https://www.investigators.net.au/blog/the-art-of-surveillance-tips-and-techniques-for-private-investigators/
8. Successful Surveillance Operations | Covert Results, accessed July 19, 2025, https://covertresults.com/blog/successful-surveillance-operations/
9. Much Ado About Geofence Warrants - Harvard Law Review, accessed July 19, 2025, https://harvardlawreview.org/blog/2025/02/much-ado-about-geofence-warrants/
10. Police Quietly Obtain Private Location Data with a Checkbook and not a Warrant, accessed July 19, 2025, https://www.pogo.org/analysis/police-quietly-obtain-private-location-data-with-a-checkbook-and-not-a-warrant
11. Advances in Facial Recognition Technology Have Outpaced Laws, Regulations - New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns | National Academies, accessed July 19, 2025, https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns
12. Facial Recognition Technologies | The Regulatory Review, accessed July 19, 2025, https://www.theregreview.org/2024/12/28/seminar-facial-recognition-technologies/
13. The Civil Rights Implications of the Federal Use of Facial Recognition Technology, accessed July 19, 2025, https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf
14. Surveillance Technologies and Constitutional Law - PMC - PubMed Central, accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10704392/
15. 28. Electronic Surveillance—Title III Applications | United States Department of Justice, accessed July 19, 2025, https://www.justice.gov/archives/jm/criminal-resource-manual-28-electronic-surveillance-title-iii-applications
16. Special report to Parliament: Investigation of the RCMP's collection ..., accessed July 19, 2025, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/
17. Artificial Intelligence Behaviour Monitoring Solution - Innovation, Science and Economic Development Canada, accessed July 19, 2025, https://ised-isde.canada.ca/site/innovative-solutions-canada/en/artificial-intelligence-behaviour-monitoring-solution
18. Bloomberg Law, "Counsel Have Toolbox to Fight Geofence Warrants as Split Widens", accessed July 19, 2025, https://www.barclaydamon.com/news/bloomberg-law-counsel-have-toolbox-to-fight-geofence-warrants-as-split-widens
19. En banc Fourth Circuit panel uses bank robbery to debate geofence warrants,

accessed July 19, 2025, https://www.courthousenews.com/en-banc-fourth-circuit-panel-uses-bank-robbery-to-debate-geofence-warrants/
20. RCMP National Technology Onboarding Program – Transparency Blueprint: Snapshot of operational technologies, accessed July 19, 2025, https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint
21. "Normative Foundations for Reasonable Expectations of Privacy" by Hamish Stewart, accessed July 19, 2025, https://digitalcommons.osgoode.yorku.ca/sclr/vol54/iss1/12/
22. Charterpedia - Section 8 – Search and seizure, accessed July 19, 2025, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html
23. Can You Hear Me Now? Conceptions of Privacy in Section 8 - Schulich Law Scholars, accessed July 19, 2025, https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1169&context=cjlt
24. R. v. Marakah: Outgoing text messages, privacy expectations and the “electronic conversation” - Hicks Adams, accessed July 19, 2025, https://hicksadams.ca/r-v-marakah-outgoing-text-messages-privacy-expectations-and-the-electronic-conversation/
25. There is a Reasonable Expectation in Subscriber Records, says Canada's Highest Court, accessed July 19, 2025, https://iapp.org/news/a/there-is-a-reasonable-expectation-in-subscriber-records-says-canadas-highes
26. R v Spencer - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/R_v_Spencer
27. R. v. Spencer: Anonymity, the Rule of Law, and the Shrivelling of the Biographical Core, accessed July 19, 2025, https://lawjournal.mcgill.ca/article/r-v-spencer-anonymity-the-rule-of-law-and-the-shrivelling-of-the-biographical-core/
28. R. vs. Marakah - Privacy Law Library, accessed July 19, 2025, https://privacylibrary.ccgnlud.org/case/r-vs-marakah
29. R v Marakah: SCC Defends Reasonable Expectation of Privacy in Text Messages, accessed July 19, 2025, https://www.dww.com/articles/r-v-marakah-scc-defends-reasonable-expectation-of-privacy-text-messages
30. Privacy Act requests | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/corporate-information/access-information-and-privacy/privacy-act-requests
31. Canada's Privacy Act - Department of Justice Canada, accessed July 19, 2025, https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/pa-lprp.html
32. Responding to access to information requests under PIPEDA - Office of the Privacy Commissioner of Canada, accessed July 19, 2025, https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

33. Personal Information Protection and Electronic Documents Act, accessed July 19, 2025, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html
34. The Artificial Intelligence and Data Act (AIDA) – Companion document, accessed July 19, 2025, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document
35. Artificial Intelligence, Profiling and Automated Decision Making | Canada | Global Data and Cyber Handbook | Baker McKenzie Resource Hub, accessed July 19, 2025, https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/north-america/canada/topics/artificial-intelligence-profiling-and-automated-decision-making
36. AI's Double-Edged Sword: Balancing Innovation and Privacy of Information | IPC, accessed July 19, 2025, https://oipc.sk.ca/ais-double-edged-sword-balancing-innovation-and-privacy-of-information/
37. Canadian privacy and AI horizon shifts again - DLA Piper, accessed July 19, 2025, https://www.dlapiper.com/insights/publications/2025/01/canadian-privacy-and-ai-horizon-shifts-again
38. Privacy and artificial intelligence (AI) - Office of the Privacy Commissioner of Canada, accessed July 19, 2025, https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/
39. Principles for responsible, trustworthy and privacy-protective ..., accessed July 19, 2025, https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/
40. Guide on the use of generative artificial intelligence - Canada.ca, accessed July 19, 2025, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html
41. Access to Information and Protection of Privacy Act, accessed July 19, 2025, https://www.oipc.nl.ca/files/LegislativeOverviewPrivacyProvisions.pdf
42. Access to Information and Protection of Privacy Act (Newfoundland and Labrador), accessed July 19, 2025, https://en.wikipedia.org/wiki/Access_to_Information_and_Protection_of_Privacy_Act_(Newfoundland_and_Labrador)
43. Investigations - Office of the Information and Privacy Commissioner, accessed July 19, 2025, https://www.oipc.nl.ca/about-us/investigations/
44. Office of the Information and Privacy Commissioner – Report A-2024 ..., accessed July 19, 2025, https://www.gov.nl.ca/releases/2024/oipc/0320n02/
45. Office of the Information and Privacy Commissioner – Report A-2025-001 Released | GovtMonitor, accessed July 19, 2025, https://www.govtmonitor.com/page.php?type=document&id=11056274
46. Office of the Information and Privacy Commissioner – Report A-2025-001 Released, accessed July 19, 2025,

https://www.gov.nl.ca/releases/2025/oipc/0120n01/
47. Investigation and Audit Reports – Office of the Information and Privacy Commissioner for BC, accessed July 19, 2025, https://www.oipc.bc.ca/reports/investigation-and-audit-reports/
48. Civilian Director's Report SIRT-NL File No. 2025-0006, accessed July 19, 2025, https://www.sirtnl.ca/files/SIRT-NL-2025-0006-Investigation-Summary-Directors-Report.pdf
49. Criminal Investigation Division – Royal Newfoundland Constabulary, accessed July 19, 2025, https://www.rnc.gov.nl.ca/what-we-do/criminal-investigation-division/
50. New 3D scanner is a 'game changer' for investigations, says RNC - Yahoo, accessed July 19, 2025, https://ca.news.yahoo.com/3d-scanner-game-changer-investigations-133353558.html
51. 2022-Juristat-Annual-Report - Royal Newfoundland Constabulary, accessed July 19, 2025, https://www.rnc.gov.nl.ca/transparency-and-accountability/publications/2022-juristat-annual-report/
52. Sexual Misconduct Support and Resource Centre Annual Report 2023–2024 - Canada.ca, accessed July 19, 2025, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/smsrc-annual-report-2023-2024.html
53. RCMP's 2023-24 Departmental results report | Royal Canadian ..., accessed July 19, 2025, https://rcmp.ca/en/corporate-information/publications-and-manuals/departmental-results-reports/2023-2024/full-report
54. 2022-2023 ANNUAL REPORT TO PARLIAMENT, accessed July 19, 2025, https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-42-2023-eng.pdf
55. Strategic Plan 2024-26 - NL Health Services, accessed July 19, 2025, https://nlhealthservices.ca/wp-content/uploads/2025/02/NLHS_Strategic-Plan-2024-26_FINAL.pdf
56. Departmental Plan - 2024 to 2025, accessed July 19, 2025, https://publications.gc.ca/collections/collection_2024/sp-ps/PS1-12-2024-eng.pdf
57. 2025-2027 Corporate Plan - Royal Newfoundland Constabulary, accessed July 19, 2025, https://www.rnc.gov.nl.ca/files/2025-27-Corporate-Report-Online.pdf
58. Technical Investigation Services | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/specialized-policing-services/technical-operations/technical-investigation-services
59. Privacy Impact Assessments | Royal Canadian Mounted Police, accessed July 19, 2025, https://www.rcmp-grc.gc.ca/en/privacy-impact-assessments
60. Privacy Impact Assessments, accessed July 19, 2025, https://www.oipc.nl.ca/about-us/advocacy-compliance/privacy-impact-assessments/

61. Untitled - Taman Inquiry, accessed July 19, 2025, http://www.tamaninquiry.ca/pdf/exhibits/exhibit-231_part8.pdf
62. Government releases Lamer Inquiry report - News Releases, accessed July 19, 2025, https://www.releases.gov.nl.ca/releases//2006/just/0621n03.htm
63. Lamer assails 'tunnel vision' in justice system | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/lamer-assails-tunnel-vision-in-justice-system-1.578256
64. Murder of Catherine Carroll - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Murder_of_Catherine_Carroll
65. N.L. man awarded $2M for wrongful conviction | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/n-l-man-awarded-2m-for-wrongful-conviction-1.580738
66. Does $2.1-million make up for lost time? - Oregon Advocate Online Resources, accessed July 19, 2025, https://www.oregonadvocates.org/geo/search/item.125114
67. THE LAMER COMMISSION OF INQUIRY PERTAINING TOTHE CASESOF:, accessed July 19, 2025, http://driskellinquiry.ca/pdf/lamerinquiry.pdf
68. Chapter 3 – Canadian Commissions of Inquiry, accessed July 19, 2025, https://www.ppsc-sppc.gc.ca/eng/pub/ptj-spj/ch3.html?wbdisable=true
69. Chapter 9 - Crown Advocacy - Public Prosecution Service of Canada, accessed July 19, 2025, https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/ch9.html
70. N.L. police revise interviewing style | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/n-l-police-revise-interviewing-style-1.966400
71. thedecisionlab.com, accessed July 19, 2025, https://thedecisionlab.com/reference-guide/psychology/the-hawthorne-effect#:~:text=The%20Hawthorne%20effect%20describes%20how,in%20social%20and%20clinical%20research.
72. What Is the Hawthorne Effect? | Definition & Examples - Scribbr, accessed July 19, 2025, https://www.scribbr.com/research-bias/hawthorne-effect/
73. pmc.ncbi.nlm.nih.gov, accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC3032358/#:~:text=The%20observer%20effect%20is%20the,changing%20the%20phenomena%20being%20studied.
74. Hawthorne effect - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Hawthorne_effect
75. The Observer Effect Unveiled - The Manufacturing Academy, accessed July 19, 2025, https://themanufacturingacademy.com/the-observer-effect-unveiled/
76. How surveillance technology is changing our behaviour and our ..., accessed July 19, 2025, https://studyonline.uts.edu.au/blog/how-surveillance-technology-changing-our-behaviour-and-our-brains
77. What are the ethical dilemmas of using AI for surveillance and ..., accessed July 19, 2025, https://fbisupport.com/ethical-dilemmas-using-ai-surveillance-behavioral-monito

ring-security/
78. Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review, accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10918303/
79. Electronically monitoring your employees? It's impacting their mental health, accessed July 19, 2025, https://www.apa.org/topics/healthy-workplaces/employee-electronic-monitoring
80. 'Black box gaslighting' challenges social-media algorithm ..., accessed July 19, 2025, https://www.psu.edu/news/information-sciences-and-technology/story/black-box-gaslighting-challenges-social-media-algorithm-0
81. Prophecy in the Streets: Prophetic Politics, Rhetoric ... - Encompass, accessed July 19, 2025, https://encompass.eku.edu/cgi/viewcontent.cgi?filename=8&article=1000&context=ekuopen&type=additional
82. “Chapter 9: Prophecy in the Streets: Prophetic Politics, Rhetoric, and Practices during the Civil Rights Movement” in “Slavery to Liberation” | OEN Manifold, accessed July 19, 2025, https://manifold.open.umn.edu/read/slavery-to-liberation-2nd-ed-3-ch1-ua/section/a13a5ec1-e7bd-414d-afc5-2c12ba2ef37d
83. "It's Just a Trend": The Gaslighting of Digital Activists | Psychology Today, accessed July 19, 2025, https://www.psychologytoday.com/us/blog/power-in-relationships/202504/its-just-a-trend-the-gaslighting-of-digital-activists
84. True Cost of a Criminal Conviction - Bader Law Injury Lawyers, accessed July 19, 2025, https://baderlaw.com/research/cost-of-being-convicted-of-a-crime/
85. Pain, suffering, and jury awards: A study of the cost of ... - - ProHIC, accessed July 19, 2025, https://prohic.nl/wp-content/uploads/2022/01/315-WrongfulConvictionCosts.pdf
86. The Consequences of False Accusations: The Role of a Criminal Defense Attorney, accessed July 19, 2025, https://thedefensefirm.com/the-consequences-of-false-accusations-the-role-of-a-criminal-defense-attorney/
87. Prison Cost Now $436 Daily - Blacklock's Reporter, accessed July 19, 2025, https://www.blacklocks.ca/prison-cost-now-436-daily/
88. The psychological impact of wrongful convictions: The role of meaning making in recovery from trauma - ResearchGate, accessed July 19, 2025, https://www.researchgate.net/publication/359357434_The_psychological_impact_of_wrongful_convictions_The_role_of_meaning_making_in_recovery_from_trauma
89. Psychological Consequences of Wrongful Conviction and Imprisonment | Canadian Journal of Criminology and Criminal Justice - University of Toronto Press, accessed July 19, 2025, https://utppublishing.com/doi/abs/10.3138/cjccj.46.2.165
90. Psychological impact of being wrongfully accused of criminal offences: A

systematic literature review - PMC, accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7838333/
91. 1. Miscarriages of Justice: The Impact of Wrongful Imprisonment - JustResearch Edition no.13, accessed July 19, 2025, https://www.justice.gc.ca/eng/rp-pr/jr/jr13/p5a.html
92. The Relational Costs of Wrongful Convictions - PMC, accessed July 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9900528/
93. 'I fear for the world': Wrongfully-convicted Newfoundland man speaks out against his mother's killer - CTV News, accessed July 19, 2025, https://www.ctvnews.ca/canada/article/i-fear-for-the-world-wrongfully-convicted-newfoundland-man-speaks-out-against-his-mothers-killer/
94. 'I am an innocent man,' Druken tells Lamer - CBC, accessed July 19, 2025, https://www.cbc.ca/lite/story/1.537851
95. 'I am an innocent man,' Druken tells Lamer | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/i-am-an-innocent-man-druken-tells-lamer-1.537851
96. Randy Druken, wrongfully convicted of murder in 1990s, dead at 57 | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/randy-druken-dies-1.6700716
97. Compensation - Canadian Registry of Wrongful Convictions, accessed July 19, 2025, https://www.wrongfulconvictions.ca/issues/compensation
98. Guidelines compensation for wrongfully convicted and imprisoned persons, accessed July 19, 2025, https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/justice/programmes/indemnisation-erreurs-judiciaires/ej_lignes_directrices-a.pdf
99. Government to provide additional compensation to Greg Parsons, accessed July 19, 2025, https://www.releases.gov.nl.ca/releases//2005/just/0901n07.htm
100. Full Report and Analysis – A Miscarriages of Justice Commission, accessed July 19, 2025, https://www.justice.gc.ca/eng/rp-pr/cj-jp/ccr-rc/mjc-cej/report-rapport.html
101. Addressing the overrepresentation of Indigenous people in the ..., accessed July 19, 2025, https://nunatsiavut.com/addressing-the-overrepresentation-of-indigenous-people-in-the-justice-system-in-nunatsiavut/
102. Injustices and Miscarriages of Justice Experienced by 12 Indigenous Women, accessed July 19, 2025, https://sencanada.ca/media/joph5la2/en_report_injustices-and-miscarriages-of-justice-experienced-by-12-indigenous-women_may-16-2022.pdf
103. Indigenous overrepresentation in provincial/territorial corrections, accessed July 19, 2025, https://www.justice.gc.ca/eng/rp-pr/jr/jf-pf/2018/docs/nov01.pdf
104. Wrongful Convictions in Canada - Library of Parliament, accessed July 19, 2025, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/202077E

105. Examining Aboriginal Corrections in Canada, accessed July 19, 2025, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/xmnng-brgnl-crrctns/index-en.aspx
106. Over-representation of Indigenous persons in adult provincial custody, 2019/2020 and 2020/2021 - Statistique Canada, accessed July 19, 2025, https://www150.statcan.gc.ca/n1/pub/85-002-x/2023001/article/00004-eng.htm
107. Indigenous peoples of Newfoundland and Labrador | EBSCO Research Starters, accessed July 19, 2025, https://www.ebsco.com/research-starters/social-sciences-and-humanities/indigenous-peoples-newfoundland-and-labrador
108. The Aboriginal Peoples of Newfoundland and Labrador and Confederation, accessed July 19, 2025, https://journals.lib.unb.ca/index.php/NFLDS/article/download/789/1143/
109. Indigenous Peoples and Confederation - Newfoundland and Labrador Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/politics/indigenous-confederation.php
110. Nunatsiavut Government v. Newfoundland and Labrador – Sept. 24 2020, accessed July 19, 2025, https://nunatsiavut.com/wp-content/uploads/2020/09/Nunatsiavut-Government-v.-Newfoundland-and-Labrador-Sept.-24-2020.pdf
111. Community Justice Connect - Human Rights Commission, accessed July 19, 2025, https://thinkhumanrights.ca/community-justice-connect/
112. Justice Supports | First Light, accessed July 19, 2025, https://firstlightnl.ca/community-supports/justice-supports/
113. First Light - St. John's Friendship Centre - Bridge the gapp, accessed July 19, 2025, https://nl.bridgethegapp.ca/adult/service-directory/first-light-st-johns-friendship-centre/
114. Systemic Racism In Policing In Canada - House of Commons, accessed July 19, 2025, https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-e.pdf
115. Wrongful Conviction Compensation Fact Sheet, accessed July 19, 2025, https://www.massbar.org/docs/default-source/advocacy/innocence-initiative/innocence-resources/wrongful-conviction-compensation-fact-sheet.pdf