The Watch on the Rock: Mass Surveillance, Secrecy, and the Legacy of Mistrust in Newfoundland and Labrador

Executive Summary

This report investigates the evidence of systemic surveillance targeting the population of Newfoundland and Labrador. It concludes that while no single, explicit program of "mass surveillance" has been identified, the confluence of broad federal national security legislation, the deployment of advanced and opaque policing technologies, and pervasive private-sector data collection creates a *de facto* system of surveillance capability. This system operates within a profound vacuum of public transparency, which resonates dangerously with the province's unique history of mistreatment by external authorities and a legacy of institutional secrecy. This historical context does not merely provide background; it acts as an amplifier, transforming abstract concerns over privacy into tangible threats against civil liberties and the social contract.

The analysis begins by establishing this historical foundation, detailing the divisive 1949 Confederation debates, the perceived economic exploitation of the 1969 Upper Churchill contract, the catastrophic 1992 cod moratorium caused by federal mismanagement, and the institutional betrayal of the Mount Cashel Orphanage scandal. It then details the legal and technical architecture of the Canadian surveillance state, built upon post-9/11 legislation like the *Anti-terrorism Act* and Bill C-51, which empowered federal agencies such as the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) with broad, often secretive, powers that are exercised directly within the province.

The report identifies the specific vectors through which population-wide data is collected, including telecommunications providers, computer operating systems, physical and aerial surveillance platforms, and emerging monitoring capabilities within social housing. It documents the specific, highly intrusive tools deployed by law enforcement in the province, including cell-site simulators and on-device spyware, whose use has been shrouded in secrecy.

Ultimately, this report finds that the primary public allegation substantiated by the evidence is not against a specific individual but against a *system* that operates

without adequate transparency or accountability. This pattern of institutional secrecy echoes the darkest chapters of the province's history, creating a unique and acute risk to democracy and civil liberties in Newfoundland and Labrador. The report concludes with a series of actionable recommendations for legislative reform, independent provincial oversight, mandatory transparency reporting, and a public inquiry to address these systemic risks.

Introduction: A History of Grievance as Prologue to Surveillance

To understand the impact of surveillance in Newfoundland and Labrador, one must first understand that it is not perceived in a vacuum. The province's relationship with external authority—first Britain, then Canada—has cultivated a unique political culture defined by a deep-seated mistrust, a fierce sense of a separate identity, and a profound sensitivity to external control.[1] This history is not merely a colourful backdrop; it is the critical lens through which modern surveillance is viewed, amplifying abstract privacy concerns into a continuation of a long and painful narrative of mistreatment.

The foundational moment of this fractured relationship was the province's entry into Canada in 1949. The decision was not a moment of national unity but the result of two bitter and closely contested referendums that deeply divided the population. Proponents, led by Joey Smallwood, argued that joining Canada would bring economic security and social programs like the "baby bonus".[2] Opponents in the Responsible Government League, led by Peter Cashin, feared the loss of independence, identity, and control, warning that Confederation was a "Canadian mousetrap".[3] The final vote was razor-thin, with Confederation winning by just 52.3 percent, leaving a legacy of resentment and a feeling among many that their nationhood had been sold for economic promises.[4] This contentious beginning established a dynamic where actions by the federal government are often viewed with suspicion.

This sense of being outmaneuvered by more powerful outside interests was cemented by the 1969 Upper Churchill hydro-electric contract. The deal, signed between the provincially-owned Churchill Falls (Labrador) Corporation (CFLCo) and Hydro-Québec, locked the province into selling nearly all the power from one of the world's largest hydroelectric sites to Quebec for 65 years at extraordinarily low, fixed

prices.[6] When energy prices soared in the 1970s, Hydro-Québec reaped massive profits by reselling the power, while Newfoundland and Labrador received a fraction of its value. Despite numerous legal and political challenges, the contract has remained largely intact, becoming a potent symbol of economic exploitation and a constant reminder of how the province's vast natural resource wealth has been siphoned away to benefit others.[6]

The most catastrophic failure of federal stewardship came with the collapse of the Northern cod fishery. On July 2, 1992, the Canadian government imposed a moratorium, ending a 500-year-old way of life and triggering the single largest mass layoff in Canadian history.[9] The collapse was a direct result of decades of federal mismanagement by the Department of Fisheries and Oceans (DFO), which had consistently ignored scientific warnings and set unsustainable quotas to appease commercial interests.[10] The moratorium devastated rural Newfoundland and Labrador, putting an estimated 30,000 people out of work and leading to a decade of population decline.[9] It was a profound betrayal, demonstrating that the federal government, entrusted with the province's most vital resource, was not a reliable steward.

While these events cemented a narrative of external mistreatment, the Mount Cashel Orphanage scandal revealed a deep-seated rot of institutional secrecy and failure within the province itself. For decades, members of the Irish Christian Brothers who ran the St. John's orphanage subjected boys to horrific physical and sexual abuse.[12] Crucially, a 1975 investigation by the Royal Newfoundland Constabulary (RNC) was curtailed by the provincial Department of Justice, despite confessions from two of the Brothers. The truth was systematically covered up by the very institutions meant to protect the public, and only came to light through the bravery of victims and investigative journalism over a decade later.[12] Mount Cashel stands as the ultimate local example of institutional betrayal and the devastating human cost of official secrecy.

These four historical traumas—political, economic, and social—are not disparate events. They form a coherent narrative of external exploitation and internal institutional failure that has profoundly shaped the province's collective psyche. Any system of surveillance, particularly one that is opaque, managed by federal agencies, or driven by powerful corporations, is inevitably interpreted through this historical lens. The legacy of mistrust acts as an amplifier, transforming abstract technological and legal issues into a tangible threat that resonates with lived experience. Surveillance is not just a matter of privacy; it is a matter of power, control, and trust in

a place where trust has been repeatedly and catastrophically broken.

Part I: The Architecture of the Canadian Surveillance State

The capacity for widespread surveillance in Newfoundland and Labrador is not born of province-specific policy, but is rather an extension of a national security architecture constructed primarily in Ottawa. This legal and institutional framework, built in the shadow of 9/11, grants federal agencies broad powers to monitor, investigate, and share information about Canadians. These powers are not confined to the national capital; they are exercised across the country, including through a direct and active presence in Newfoundland and Labrador.

The Post-9/11 Legislative Overhaul: The *Anti-terrorism Act* (2001)

In the immediate aftermath of the September 11, 2001 attacks, the Canadian Parliament passed the *Anti-terrorism Act* (ATA), a sweeping piece of legislation that fundamentally altered the country's legal landscape.[14] The Act amended numerous laws, including the

Criminal Code, to create a new slate of terrorism-specific offences and provide law enforcement and intelligence agencies with powerful new investigative tools.[14]

Key among these was the expansion of the state's surveillance powers. The ATA integrated terrorism offences into the *Criminal Code's* electronic surveillance scheme, notably removing the "last-resort" requirement for obtaining wiretap authorizations in these cases.[14] This lowered the bar for police to intercept private communications. The maximum duration for a wiretap authorization was extended from 60 days to one year, and the period for which police could delay notifying a target of surveillance was extended to three years.[14] The Act also expanded the National DNA Data Bank to include terrorism offences, allowing for the collection and storage of genetic material from a wider range of individuals.[14] These measures collectively provided the state with a more permissive and powerful toolkit for monitoring individuals.

The Expansion of Powers: Bill C-51, The *Anti-terrorism Act, 2015*

The powers of the Canadian security state were expanded even further with the passage of Bill C-51 in 2015.[17] This controversial legislation introduced a host of new measures, the most significant of which was the enactment of the

Security of Canada Information Sharing Act.[18] This new Act authorized 17 different federal government departments and agencies to share the personal information of Canadians with one another for the purpose of protecting against "activities that undermine the security of Canada".[18]

Civil liberties organizations, academics, and privacy experts heavily criticized the bill for its vague and overly broad language.[19] Critics argued that the definition of "undermining the security of Canada" was so expansive it could include legitimate protest and dissent, creating a chilling effect on free speech.[19] The legislation effectively dismantled the legal and bureaucratic silos that had previously prevented the wholesale sharing of personal data—from tax records to travel information—between government bodies. This created the legal foundation for an unprecedented level of data aggregation and analysis on ordinary Canadians, all conducted without their knowledge or consent and with minimal oversight.[17]

Canada's Intelligence Agencies and their Provincial Reach

The powers granted by this legislative framework are wielded by federal agencies that have a direct operational footprint in Newfoundland and Labrador, blurring the line between national security and local policing.

- **Canadian Security Intelligence Service (CSIS):** As Canada's primary human intelligence agency, CSIS is mandated to investigate threats to national security, including terrorism, espionage, and foreign interference.[21] While its headquarters are in Ottawa, CSIS's operations are national in scope. The agency's **Atlantic Region** encompasses all four Atlantic provinces and maintains a district office in **St. John's**.[23] This gives CSIS a direct physical and operational presence in Newfoundland and Labrador, allowing it to conduct investigations and intelligence-gathering activities on the ground. The agency also engages in

"Academic Outreach and Stakeholder Engagement" to build relationships with universities and other organizations, further embedding itself in the provincial landscape.[24]

- **Communications Security Establishment (CSE):** The CSE is Canada's signals intelligence (SIGINT) agency, responsible for collecting foreign intelligence by intercepting electronic communications and for providing cybersecurity and information assurance for critical domestic infrastructure.[26] Its mandate allows it to monitor the global information infrastructure, which is the technical backbone for all internet and telecommunications traffic entering and leaving Canada. While the CSE's primary collection activities are directed externally, its defensive mandate gives it purview over domestic networks, making it a key player in the national surveillance apparatus.[26]
- **Royal Canadian Mounted Police (RCMP):** The RCMP has a unique dual mandate in the province. It serves as Canada's federal police force, with responsibility for investigating national security offences, but it also acts as the provincial police force for most of Newfoundland and Labrador outside the Northeast Avalon Peninsula.[27] This creates a significant overlap of mandates, where the same organization and often the same officers are responsible for both local law enforcement and national security investigations.

This structure results in the federalization of local surveillance. The most powerful and secretive surveillance mandates in the country are not abstract legal concepts for the province; they are embodied by federal agencies with a permanent and active presence. National security priorities defined in Ottawa can be enacted at a local level using tools and authorities that are not subject to provincial or municipal oversight. The legal architecture is national, but its implementation is deeply local, bringing the full weight of the Canadian surveillance state to bear on communities across Newfoundland and Labrador.

Part II: The Digital Dragnet: Vectors of Mass Data Collection in Newfoundland and Labrador

The legal framework of the Canadian surveillance state is brought to life through a technical architecture that enables the collection of vast amounts of data from the population. This digital dragnet operates across multiple vectors, from the foundational infrastructure of the internet to the operating systems on personal

computers and the management systems in social housing. While each vector serves a distinct commercial or administrative purpose, their combined effect is the creation of a rich, multi-layered repository of personal information, accessible to both corporate and state actors.

Telecommunications as the First Line of Surveillance

As the gatekeepers of all internet traffic, Internet Service Providers (ISPs) represent the primary chokepoint for data collection. In Newfoundland and Labrador, the dominant provider is Bell Aliant. The company's privacy policy states that it collects a wide range of personal information, including call records and internet service usage data, to "establish and maintain a responsible commercial relationship" and "understand [customer] needs and preferences".[29] This data is retained for as long as needed to meet legal or business requirements.[32]

ISPs possess the technical capability to perform Deep Packet Inspection (DPI), a process that allows them to examine the content of unencrypted internet traffic passing through their networks.[33] While the Canadian Radio-television and Telecommunications Commission (CRTC) has established a framework to govern these practices, it does not ban them, instead requiring ISPs to be transparent about their use.[34] Even when traffic is encrypted (e.g., using HTTPS), the underlying DNS requests that translate a domain name like

www.example.com into an IP address are typically sent in the clear. This means the ISP can log every website a user visits, regardless of whether the user opts for a third-party DNS service like Google's. While Virtual Private Networks (VPNs) are a common countermeasure, ISPs can employ techniques to detect and block VPN traffic, limiting their effectiveness as a tool for ensuring privacy.[35]

The Ubiquitous Operating System: Baseline Data Collection

A second, pervasive layer of data collection occurs at the level of the computer's operating system. Microsoft Windows, the dominant OS on desktop and laptop computers, incorporates an extensive telemetry system that constantly sends data

back to the company's servers.[38] This data collection is divided into two tiers: "Required" and "Optional."

"Required" diagnostic data, which cannot be disabled by a home user, includes detailed device configuration information (hardware, OS version), system stability reports, error logs, and records of software updates and installations.[38] "Optional" data, if enabled by the user, is far more intrusive, capturing detailed browsing history from Microsoft browsers, granular logs on application usage, and even full crash dumps—complete snapshots of the computer's active memory at the time of a system failure.[38] This creates a baseline of constant, low-level surveillance on a significant portion of the province's population, with the resulting data being transmitted to and stored by a foreign multinational corporation.

The Watchful Eye: Physical and Aerial Surveillance

Physical surveillance is an increasingly common feature of public life. Newfoundland and Labrador's Information and Privacy Commissioner has noted the growing use of video surveillance by public bodies across the province, raising concerns about the erosion of privacy in public spaces.[39] The RNC has historically expressed interest in expanding its network of closed-circuit television (CCTV) cameras, particularly in the downtown core of St. John's, to deter crime and gather evidence.[41]

Beyond ground-level cameras, a significant high-technology surveillance capability operates from the province's skies. The federal government awarded a five-to-ten-year contract worth $128 million to PAL Aerospace, a St. John's-based company, for aerial surveillance of Canada's inland, coastal, and offshore waters.[42] While the stated purpose of this contract is to support Fisheries and Oceans Canada in combating illegal fishing and enhancing maritime security, it equips a local company with advanced intelligence, surveillance, and reconnaissance (ISR) aircraft and technology, representing a powerful surveillance asset operating from within the province.[42]

A New Frontier: Surveillance in Social Housing

A particularly concerning vector for surveillance is emerging within the province's social housing sector. Public Housing Authorities (PHAs) are increasingly adopting comprehensive software suites to manage their operations. One such system is Yardi's Voyager PHA, which centralizes a vast amount of highly sensitive information about low-income households.[44] The platform is used to manage everything from applicant screening—including criminal and credit checks—to income and asset verification, waitlist management, maintenance requests, and rent payment processing.[45]

This centralization of data creates a detailed digital profile of some of the province's most vulnerable citizens. The potential for mission creep is significant, especially with the integration of Internet of Things (IoT) or "smart home" technologies. Yardi actively markets a product called RentCafe Home IQ, which allows property managers to remotely control and monitor smart devices in rental units, including smart locks and leak sensors.[47] While the available documentation does not explicitly mention the deployment of audio, motion, or CO2 sensors in Newfoundland and Labrador public housing, the underlying software platform is designed for precisely this kind of integrated device management.[48] This creates a clear technological pathway for the future expansion of surveillance directly inside the homes of public housing tenants.

The historical narrative of Newfoundland and Labrador is one of exploitation of its physical resources, from the hydroelectric power of Churchill Falls to the cod stocks of the Grand Banks. The modern vectors of data collection present a direct parallel to this history. Personal data has become the new resource. The browsing habits, computer usage patterns, and financial details of the provincial population are being systematically extracted. The value generated from this data—whether for targeted advertising, software improvement, or risk management—primarily benefits large, external entities like Bell, Microsoft, and Yardi, as well as the federal state. In this context, the people of Newfoundland and Labrador are once again positioned as a resource to be mined, their data extracted and processed for the benefit of outside powers, echoing the historical grievances that have defined the province's identity.

Part III: Policing the Periphery: Law Enforcement Technology on the Ground

Beyond the broad, passive collection of data, law enforcement agencies operating in Newfoundland and Labrador deploy a range of sophisticated and highly intrusive

technologies to actively surveil and investigate individuals. The capabilities of these tools, often acquired and used with little to no public consultation or transparency, represent a direct and significant threat to the civil liberties of the province's residents.

The Royal Newfoundland Constabulary's Modern Toolkit

The Royal Newfoundland Constabulary (RNC), which polices the province's major urban centres, has developed a modern technological capacity for investigation and surveillance. Its organizational structure includes several specialized units dedicated to technical operations. The Mobile Support Unit conducts physical surveillance, while the Technical Investigation Unit employs "electronic investigative techniques".[50] The Computer Forensics Unit is tasked with the seizure and examination of digital evidence from computers, cell phones, and other devices, and a dedicated Video Services Unit performs forensic analysis of surveillance footage.[50]

Recent acquisitions demonstrate a commitment to adopting advanced technology. In 2025, the RNC acquired a 3D laser scanner for crime scene reconstruction and a portable spectrometer for identifying unknown chemical substances, including illicit drugs.[51] While these tools have clear applications in evidence gathering, their acquisition highlights a broader trend of technological modernization within the force. This modernization must be contextualized against the RNC's historical role in the Mount Cashel cover-up, an institutional failure rooted in secrecy.[12] This history raises critical questions about whether the force's commitment to transparency and accountability has kept pace with its growing technological power.

The Federal Footprint: RCMP Intrusive Capabilities in NL

The RCMP, which provides provincial policing for most of Newfoundland and Labrador, has access to the full suite of investigative technologies available to Canada's national police force. Several of these tools are exceptionally intrusive and have been used in a manner that deliberately obscured their existence from the Canadian public.

- **Cell-Site Simulators (IMSI Catchers):** The RCMP has owned and operated these devices since at least 2005.[52] Commonly known as IMSI Catchers, these devices

mimic a legitimate cell phone tower, compelling all mobile phones within a given radius—potentially up to two kilometers—to connect to it.[52] In doing so, the device captures the unique IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) numbers of every phone in the area.[54] This is an indiscriminate, dragnet surveillance tool that gathers data from hundreds or thousands of innocent people in order to identify a single device of interest. For more than a decade, the RCMP refused to confirm or deny its use of this technology, with its existence only being officially acknowledged in 2017 following media investigations and a formal inquiry by the Privacy Commissioner of Canada.[52]

- **On-Device Investigative Tools (ODITs):** The RCMP also employs what it terms On-Device Investigative Tools, which are functionally equivalent to government-deployed spyware.[55] With judicial authorization, these tools can be covertly installed on a target's computer or smartphone. Once installed, an ODIT can provide police with access to a vast trove of private information, including intercepting private communications, capturing screenshots and keyboard strokes, and remotely and secretly activating the device's camera and microphone.[53] The RCMP's use of this technology was also conducted for years without public knowledge or consultation with the Privacy Commissioner.[58]
- **Body-Worn Cameras (BWCs):** In a move presented as a step toward transparency, the RCMP began a national rollout of body-worn cameras in November 2024, with the first deployments in Newfoundland and Labrador occurring at the Holyrood and Ferryland detachments.[59] According to RCMP policy, the cameras are intended to record interactions with the public during calls for service but are not to be used for general surveillance and are to be deactivated in locations with a high expectation of privacy, such as private homes or hospitals, except in exigent circumstances.[60] The video evidence is uploaded to a secure, cloud-based "digital evidence management system".[60] While framed as an accountability measure, the control over the data—when to record, when to stop, and who can access the footage—remains entirely with the police force.[62]
- **Facial Recognition Technology (FRT):** The RCMP has acknowledged its use of facial recognition technology, which involves using software to compare images of unknown individuals against lawfully obtained photo databases to generate investigative leads.[57] This capability is part of a broader, and highly controversial, trend among Canadian police services, some of which were found to have used Clearview AI, a company that built its database by scraping billions of images from social media without consent.[64]

The deployment of these technologies by the two primary police forces in the

province creates a powerful and multi-layered surveillance capacity. The following table synthesizes the known capabilities, the legal threshold for their use, and the degree to which their existence and operation have been transparent to the public. This summary highlights a recurring theme: the most potent surveillance tools are also the most secretive.

Table 1: Known Surveillance and Investigative Technologies of NL Police Forces

Technology	Agency (RNC/RCMP)	Function	Legal Requirement for Use	Public Transparency Level
Cell-Site Simulator	RCMP	Identifies/locates all mobile devices in an area (indiscriminate)	Judicial Authorization	Very Low; use confirmed only after media/OPC investigation [52]
On-Device Investigative Tool (ODIT)	RCMP	Covertly collects data from a target device (spyware), including activating mic/camera	Judicial Authorization	Very Low; use confirmed only after media reports [53]
Aerial Surveillance	Federal (via PAL Aerospace)	Broad-area monitoring for fisheries/maritime security	Contractual Mandate	High (Public Contract) [42]
Facial Recognition Technology (FRT)	RCMP (capability)	Compares images against lawfully obtained photo databases	Policy-dependent; requires lawful photo database	Very Low [57]
Video Forensics	RNC/RCMP	Analysis of	Standard	Low [41]

& Surveillance		collected video surveillance; Mobile surveillance support	investigative procedure	
Computer & Digital Forensics	RNC/RCMP	Extraction/analysis of data from seized digital devices	Search Warrant	Low [50]
Body-Worn Cameras	RCMP	Records interactions between police and public	Operational Policy	Medium (Policy is public, but footage is not) [59]

Part IV: Echoes of History: Accountability, Secrecy, and Systemic Risk

This investigation finds no evidence of a single, codified program of "mass surveillance" explicitly targeting the population of Newfoundland and Labrador. However, the analysis reveals the existence of a *de facto* system of mass surveillance *capability*. This system is the emergent property of three interconnected forces: national security laws that permit expansive, cross-governmental information sharing; the local presence of federal agencies with powerful and secretive mandates; the indiscriminate data collection practices of private corporations that control essential infrastructure; and the deployment of intrusive, clandestine technologies by police. The sum of these parts is a surveillance apparatus whose potential reach is far greater than is publicly acknowledged.

Addressing Allegations Through the Lens of Secrecy

The user query asked for an investigation into public allegations made against individuals within this system. The evidence, however, points not to individual malfeasance but to a pervasive and deeply concerning culture of institutional secrecy.

The most significant allegation substantiated by this report is against the system itself—a system that operates by default in the shadows, resisting transparency and accountability.

This pattern of institutional behaviour is not new to the province; it is a direct echo of the institutional failures that enabled the horrors at the Mount Cashel Orphanage. The 1975 police investigation into abuse was deliberately curtailed by the Department of Justice, and the truth was actively suppressed for years by the very institutions sworn to uphold the law and protect the vulnerable.[12] This was a catastrophic failure of accountability, born of a culture of secrecy.

A chilling parallel can be drawn to the modern-day conduct of the RCMP regarding its most powerful surveillance tools. For over a decade, the force used cell-site simulators to conduct dragnet surveillance on Canadians while refusing to confirm or deny their existence, even in response to formal access to information requests.[52] Similarly, its use of spyware (ODITs) was undertaken without public consultation or the knowledge of the Privacy Commissioner of Canada.[58] The mechanism in both cases is identical: a powerful public institution deploys a highly intrusive capability without public knowledge or consent and actively resists transparency. While the nature of the harm differs—physical and sexual abuse versus the violation of privacy—the institutional

modus operandi of secrecy is a direct and disturbing historical parallel.

The Resonant Threat: Surveillance as a Modern Form of Disenfranchisement

This modern surveillance apparatus, when viewed through the province's historical lens, becomes more than a threat to privacy; it becomes a modern form of disenfranchisement. A system where a remote federal power, acting through the RCMP and CSIS, can deploy invisible, indiscriminate monitoring technologies against the population is a 21st-century iteration of the same power dynamics that led to the Upper Churchill contract and the cod moratorium. It reinforces the deeply ingrained sense of being a powerless periphery, subject to the decisions of a remote and unaccountable center. It transforms citizens from active participants in a democracy, whose consent is required, into data points to be managed, monitored, and controlled. This dynamic undermines the very foundation of the social contract and validates the historical skepticism toward external authority that defines the province's political

culture.

The Oversight Gap

This systemic risk is compounded by a significant accountability vacuum. While Newfoundland and Labrador has an Office of the Information and Privacy Commissioner (OIPC) responsible for overseeing provincial privacy laws like *ATIPPA* and investigating privacy breaches by public bodies, its mandate is strictly limited.[66] The OIPC has no jurisdiction over federal agencies. This means that the activities of CSIS in its St. John's office and the national security operations of the RCMP within the province fall completely outside the purview of any local or provincial oversight body.

Federal oversight bodies, such as the National Security and Intelligence Review Agency (NSIRA), operate largely behind a veil of secrecy, and their findings are often heavily redacted.[70] Furthermore, the Privacy Commissioner of Canada has repeatedly lamented the office's lack of enforcement powers, rendering it a watchdog with no teeth.[73] This creates a critical oversight gap where the most powerful and intrusive surveillance tools are subject to the least effective and least transparent forms of accountability, leaving the citizens of Newfoundland and Labrador with little recourse or visibility into how they are being monitored.

Recommendations

The convergence of historical mistrust, secretive surveillance technologies, and a fractured oversight landscape creates an unacceptable risk to the civil liberties and democratic health of Newfoundland and Labrador. Addressing this requires decisive action at both the federal and provincial levels.

1. **Federal Legislative Reform:** The Government of Canada should repeal the *Security of Canada Information Sharing Act*, enacted as part of Bill C-51, to restore the legal barriers to indiscriminate, cross-departmental sharing of Canadians' personal information. Furthermore, the *CSIS Act* should be amended to narrow the agency's threat reduction powers and to explicitly prohibit any

action that would violate the *Canadian Charter of Rights and Freedoms*.

2. **Provincial Policing Technology Oversight:** The Government of Newfoundland and Labrador should establish an independent, civilian oversight body with the mandate and technical expertise to review and approve—or deny—the acquisition and deployment of new surveillance technologies by any police force operating within the province, including both the RNC and the provincial policing operations of the RCMP. No new surveillance technology should be deployed without this body's prior approval.
3. **Mandatory Transparency Reporting:** The *Royal Newfoundland Constabulary Act* and the provincial policing services agreement with the RCMP should be amended to require both forces to publish annual, public reports on their use of surveillance technologies. These reports must include, at a minimum, aggregate statistics on the number of warrants sought and granted for tools such as Cell-Site Simulators and On-Device Investigative Tools, as well as a description of the types of investigations in which they were used.
4. **Commission of Public Inquiry:** The Government of Newfoundland and Labrador should launch a full Commission of Public Inquiry, modeled on the Hughes Inquiry into the Mount Cashel abuse scandal. This inquiry should be granted full subpoena power to investigate the historical and current use of surveillance technologies by state and corporate actors in the province, assess their impact on the civil liberties of its citizens, and provide binding recommendations for a new, transparent framework for accountability.
5. **Strengthening Provincial Privacy Law:** The provincial *Access to Information and Protection of Privacy Act, 2015 (ATIPPA)* should be amended to require all public bodies, including municipalities and police forces, to conduct and publicly release a comprehensive Privacy Impact Assessment *before* the procurement or deployment of any new surveillance program or technology. This would ensure that privacy implications are considered at the outset, not after the fact.

Works cited

1. Revolution Rejected? - Newfoundland and Labrador Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/exploration/revolution-rejected.php
2. Politics of Newfoundland and Labrador - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Politics_of_Newfoundland_and_Labrador
3. Newfoundland and Canada: 1864-1949 - Newfoundland Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/politics/confederation-1864-1949.php
4. Newfoundland and Labrador and Confederation | The Canadian Encyclopedia, accessed July 19, 2025, https://www.thecanadianencyclopedia.ca/en/article/newfoundland-and-labrador-and-confederation

5. The Confederation Debate Transcript - Canada's History, accessed July 19, 2025, https://www.canadashistory.ca/explore/politics-law/newfoundland-s-big-choice/newfoundland-s-big-choice-part-2-transcript
6. The Churchill Falls contract and why Newfoundlanders can't get over it, accessed July 19, 2025, https://policyoptions.irpp.org/magazines/making-parliament-work/the-churchill-falls-contract-and-why-newfoundlanders-cant-get-over-it/
7. Keynote Address: The Canadian Supreme Court's decision in Churchill Falls (Labrador) Corporation Limited v. Hydro-Québec | Global law firm | Norton Rose Fulbright, accessed July 19, 2025, https://www.nortonrosefulbright.com/en/knowledge/publications/b4d49dea/keynote-address-the-canadian-supreme-courts
8. The 1969 Contract: Churchill Falls - Newfoundland Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/politics/churchill-falls.php
9. Economic Impacts of the Cod Moratorium - Newfoundland Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/economy/moratorium-impacts.php
10. Collapse of the Atlantic northwest cod fishery - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Collapse_of_the_Atlantic_northwest_cod_fishery
11. A Tragedy with No End | Science History Institute, accessed July 19, 2025, https://www.sciencehistory.org/stories/magazine/a-tragedy-with-no-end/
12. Mount Cashel Orphanage - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Mount_Cashel_Orphanage
13. Mount Cashel Orphanage Abuse Scandal - Newfoundland and Labrador Heritage, accessed July 19, 2025, https://www.heritage.nf.ca/articles/politics/wells-government-mt-cashel.php
14. About the Anti-terrorism Act - Department of Justice Canada, accessed July 19, 2025, https://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html
15. Anti-terrorism Act - Laws.justice.gc.ca, accessed July 19, 2025, https://laws-lois.justice.gc.ca/eng/acts/a-11.7/page-1.html
16. The Anti-Terrorism Act - BC Civil Liberties Association, accessed July 19, 2025, https://bccla.org/privacy-handbook/main-menu/privacy7contents/privacy7-17.html
17. Anti-terrorism Act, 2015 - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Anti-terrorism_Act,_2015
18. Legislative Summary for Bill C-51 - Library of Parliament, accessed July 19, 2025, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C51E
19. Understanding Bill C-51 in Canada: The Anti-Terrorism Act, 2015 ..., accessed July 19, 2025, https://ccla.org/get-informed/talk-rights/understanding-bill-c-51-in-canada-the-anti-terrorism-act-2015/
20. SUMMARY The provisions of Bill C-51 modifying the law in relation to sexual assault offences are unnecessary, overbroad, and sev, accessed July 19, 2025,

https://www.ourcommons.ca/Content/Committee/421/JUST/Brief/BR9204682/br-external/AcumenLawCorporation-e.pdf
21. Canadian Security Intelligence Service (CSIS) (pdf) - Foreign Interference Commission, accessed July 19, 2025, https://foreigninterferencecommission.ca/fileadmin/foreign_interference_commission/Documents/Exhibits_and_Presentations/Overview_Institutional_Reports/CAN.DOC.000017.pdf
22. Mandate - Canada.ca, accessed July 19, 2025, https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html
23. Canadian Security Intelligence Service - Wikipedia, accessed July 19, 2025, https://en.wikipedia.org/wiki/Canadian_Security_Intelligence_Service
24. Canadian Security Intelligence Service - Canada.ca, accessed July 19, 2025, https://www.canada.ca/en/security-intelligence-service.html
25. Protect your research - Newfoundland & Labrador - Canada.ca, accessed July 19, 2025, https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/protect-your-research/AOSE_Regional_Factsheet_NEWFOUNDLAND_LABRADOR_DIGITAL_ISBN_A.pdf
26. Communications Security Establishment Canada Annual Report ..., accessed July 19, 2025, https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2024-2025
27. Justice Department survey shows Newfoundlanders and Labradorians feeling less safe | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/justice-department-safety-survey-1.7544569
28. Newfoundland and Labrador RCMP news | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/nl/news
29. Privacy Policy - Bell Aliant, accessed July 19, 2025, https://bellaliant.bell.ca/privacy-security/privacy
30. Personal information and your privacy - Bell, accessed July 19, 2025, https://www.bell.ca/Security_and_privacy/How_we_collect_and_use_data
31. How does Bell collect, use, store and protect your personal information, accessed July 19, 2025, https://support.bell.ca/billing-and-accounts/policies/how_does_bell_collect_and_protect_your_personal_information?step=8
32. 2022- Data privacy and information security - BCE Inc., accessed July 19, 2025, https://bce.ca/responsibility/key-documents/2022-data-privacy-information-security.pdf
33. Deep Packet Inspection: Its Nature and Implications, accessed July 19, 2025, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2009/clarke_200903/
34. Telecom Regulatory Policy CRTC 2009-657 | CRTC, accessed July 19, 2025, https://crtc.gc.ca/eng/archive/2009/2009-657.htm
35. How to Bypass VPN Blockers Effectively - Cybernews, accessed July 19, 2025,

https://cybernews.com/how-to-use-vpn/bypass-vpn-blocks/
36. Detecting and Bypassing VPN Blocking by Your ISP in 2024 | by Migziteno - Medium, accessed July 19, 2025, https://medium.com/@migzite1no/detecting-and-bypassing-vpn-blocking-by-your-isp-in-2024-68aa74125822
37. How to bypass ISP throttling [2 of the best VPN solutions] - SaaS Genius, accessed July 19, 2025, https://www.saasgenius.com/blog/how-to-bypass-isp-throttling-2-of-the-best-vpn-solutions/
38. Windows 10 & 11 Telemetry Explained: Privacy, Data Collection ..., accessed July 19, 2025, https://windowsforum.com/threads/windows-10-11-telemetry-explained-privacy-data-collection-user-control.373361/latest
39. How much video surveillance is too much, asks privacy commissioner | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/how-much-video-surveillance-is-too-much-asks-privacy-commissioner-1.3147014
40. OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador June 26, 2015, accessed July 19, 2025, https://www.oipc.nl.ca/files/GuidelinesForVideoSurveillance.pdf
41. Eyes in sky could help cut crime: RNC chief | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/canada/newfoundland-labrador/eyes-in-sky-could-help-cut-crime-rnc-chief-1.704101
42. Government of Canada awards aerial surveillance contract in St John's to improve conservation and protection of our oceans, accessed July 19, 2025, https://www.canada.ca/en/fisheries-oceans/news/2019/03/government-of-canada-awards-aerial-surveillance-contract-in-st-johns-to-improve-conservation-and-protection-of-our-oceans.html
43. PAL Aerospace Awarded Aerial Surveillance Contract by the Government of Canada, accessed July 19, 2025, https://palaerospace.com/pal-aerospace-awarded-aerial-surveillance-contract-government-canada/
44. Social housing - Yardi, accessed July 19, 2025, https://www.yardi.com/market/social-housing/
45. PHA - Yardi, accessed July 19, 2025, https://www.yardi.com/market/pha/
46. RightSource - Yardi, accessed July 19, 2025, https://www.yardi.com/product/rightsource/
47. RentCafe Home IQ - Yardi, accessed July 19, 2025, https://www.yardi.com/product/rentcafe-home-iq/
48. AI, IOT and Real Estate - The Balance Sheet - Yardi Corporate Blog, accessed July 19, 2025, https://www.yardi.com/blog/global/ai-iot-and-real-estate/23229.html
49. The Role of Internet of Things (IoT) in Facility Management - Yardi Corom, accessed July 19, 2025, https://www.yardicorom.com/blog/the-role-of-internet-of-things-iot-in-facility-management/

50. Criminal Investigation Division - Royal Newfoundland Constabulary, accessed July 19, 2025, https://www.rnc.gov.nl.ca/what-we-do/criminal-investigation-division/
51. 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
52. The RCMP has been tracking our phones for years. What can we do about it? - OpenMedia, accessed July 19, 2025, https://openmedia.org/article/item/the-rcmp-tracking-our-phones
53. 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
54. Cell site simulators used by RCMP not capable of intercepting private communication, accessed July 19, 2025, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/
55. Q&A with an expert in electronic surveillance on the challenges and opportunities of collecting evidence | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/gazette/qa-expert-electronic-surveillance-challenges-and-opportunities-collecting-evidence
56. Covert Access and Intercept Team privacy impact assessment | Royal Canadian Mounted Police, accessed July 19, 2025, https://www.rcmp-grc.gc.ca/en/covert-access-and-intercept-team-privacy-impact-assessment
57. RCMP lifts veil on use of emerging technologies to fight crime - CityNews Halifax, accessed July 19, 2025, https://halifax.citynews.ca/2024/09/10/rcmp-lifts-veil-on-use-of-emerging-technologies-to-fight-crime/
58. Ontario police may have secretly used controversial Israeli spyware, report finds - CBC, accessed July 19, 2025, https://www.cbc.ca/news/canada/opp-paragon-solutions-spyware-1.7488027
59. RCMP NL announces use of body worn cameras by its police officers in Newfoundland and Labrador, accessed July 19, 2025, https://www.rcmp-grc.gc.ca/en/news/2024/rcmp-nl-announces-use-body-worn-cameras-police-officers-newfoundland-and-labrador
60. Body-worn cameras | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/body-worn-cameras
61. RCMP begins national deployment of body-worn cameras | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/news/2024/11/rcmp-begins-national-deployment-body-worn-cameras
62. Body Worn Camera (BWC) and Digital Evidence Management Service (DEMS) | Royal Canadian Mounted Police, accessed July 19, 2025, https://www.rcmp-grc.gc.ca/en/body-word-camera-bwc-and-digital-evidence-

management-service-dems
63. National Technology Onboarding Program | Royal Canadian Mounted Police, accessed July 19, 2025, https://rcmp.ca/en/specialized-policing-services/technical-operations/national-technology-onboarding-program
64. Use of controversial surveillance technology demonstrates the need to limit police power | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/opinion/opinion-police-facial-recognition-technology-clearview-ai-1.6306357
65. The Shocking Far-Right Agenda Behind the Facial Recognition Tech Used by ICE and the FBI - Mother Jones, accessed July 19, 2025, https://www.motherjones.com/politics/2025/04/clearview-ai-immigration-ice-fbi-surveillance-facial-recognition-hoan-ton-that-hal-lambert-trump/
66. Privacy Commissioner Recommends City of Corner Brook Release Withheld Files in ATIPP Review | VOCM, accessed July 19, 2025, https://vocm.com/2024/08/27/249665/
67. Data Privacy Week 2024 - News Releases - Government of Newfoundland and Labrador, accessed July 19, 2025, https://www.gov.nl.ca/releases/2024/oipc/0122n01/
68. NL - Request a Review or Make a Privacy Complaint - House of Assembly, accessed July 19, 2025, https://www.assembly.nl.ca/About/ATIPP/ATIPP_Dispute.aspx
69. How to Complete the Reporting a Privacy Breach Form, accessed July 19, 2025, https://www.oipc.nl.ca/files/ATIPPA2015HowtoCompletetheReportingaPrivacyBreachFormGuidelines.pdf
70. Public Safety and Canadian Security Intelligence Service Accountability Mechanisms: Backgrounder, accessed July 19, 2025, https://nsira-ossnr.gc.ca/en/reviews/our-reviews/ps-and-csis-accountability-mechanisms/backgrounder/
71. Halting spy operation placed CSIS team in unnecessary danger, watchdog report says, accessed July 19, 2025, https://www.ctvnews.ca/politics/article/halting-spy-operation-placed-csis-team-in-unnecessary-danger-watchdog-report-says/
72. Halting spy operation placed CSIS team in unnecessary danger, watchdog report says | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/politics/csis-operation-nsira-1.7547940
73. Federal privacy watchdog warns of growing dangers of 'surveillance capitalism' | CBC News, accessed July 19, 2025, https://www.cbc.ca/news/politics/privacy-commissioner-report-daniel-therrien-1.6279665