Canadian Chamber of Commerce
Chambre de Commerce du Canada

Canadian Chamber Future of Business Centre
Centre de l’avenir des affaires de la Chambre de Commerce du Canada

WHY STRONG ENCRYPTION

Is Essential for Canada’s Security, Economic Future and Digital Sovereignty

By Heather West and Eric Miller | June 2025

Why Strong Encryption Is Essential for Canada's Security, Economic Future and Digital Sovereignty by:

Heather West

Fellow,
Canadian Chamber Future of Business Centre
Fellow, Center for Cybersecurity Policy and Law

Eric Miller

Fellow,
Canadian Chamber Future of Business Centre
President, Rideau Potomac Strategy Group

The Canadian Chamber of Commerce is committed to enabling the future of business success. To advance progress on forward-looking public policy issues, the Canadian Chamber Future of Business Centre is our platform for placing these topics into the public debate.

The Centre's reports are produced by external fellows at arm's length, separately from the Canadian Chamber's consensus-based policy committee process. The views expressed in this paper are those of the fellows.

Acknowledgements

The authors extend their sincere appreciation to the following individuals who contributed to the production of this report.

Advisory Council

Charles Finlay
Founding Executive Director
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

Daina Proctor
Canadian Security Services Leader
IBM

Jennifer Quaid
Executive Director
Canadian Cyber Threat Exchange

John Verdi
Senior Vice President for Policy
Future of Privacy Forum

Special Mention

Grace M. O'Neill
Analyst
Center for Cybersecurity Policy and Law

Contents

“It is not overstating matters to say that strong encryption and effective cyber security have become strategic imperatives for Canada.”

Introduction: A New — and Old — World

Canada in 2025 is entering a period of profound change.

The post-World War II era of *Pax Americana* is largely over. U.S. global leadership has given way to America First. The Trump administration is rethinking who its allies are. On the economic front, America First means the broad imposition of tariffs and other commercial restrictions on traditional friends and foes alike. U.S. protectionism and the policy uncertainty coming out of Washington is undermining the investment climate in Canada that has long promoted secure access to the U.S. market as a cornerstone of its offering. Canada is now pursuing genuine trade diversification and new relationships with an urgency never seen before. In light of the evolving geopolitical context, Canada, like other traditional U.S. allies, is also preparing to spend more on its own security with a view to ensuring strategic autonomy.

While Canada needs to forge different pathways into its economic future, it must be conscious of the underlying dynamics around wealth creation in our contemporary world. Despite growing geopolitical tensions and talk of “deglobalization,” the digital infrastructure that interconnected the globe through its computers and devices over the past quarter century remains firmly in place and is as central as ever to the lives of Canadians.

All of this connectivity is generating vast quantities of data, which has become a valuable asset in its own right. Canadian economist Dan Ciuriak notes that precisely estimating its value is difficult because there are no associated receipts or invoices from which to establish a transaction value. As a proxy, he looks at the relative share of intangible to tangible capital[1] in the composition of corporate assets of S&P 500 firms. The share of intangibles rose from 17%

[1] Intangible assets include data, copyrights, patents, and trademarks. Tangible assets include land, buildings, natural resource deposits, and machinery.

in 1975 to 68% in 1995 to 90% in 2024. From this, Dr. Ciuriak separates sub-components of intangibles, ultimately estimating that the value of data is $6.3 trillion or 17% of all intangible assets.[2]

The digital economy has the potential to be a hugely powerful driver of Canadian economic growth in the years ahead. Too often, Canadians look at the digital economy as an American sector. There is no doubt that the United States enjoyed a first mover advantage from the 1990s through the 2010s which created a variety of world-leading tech firms. There is also no doubt that Silicon Valley remains a place of incredible economic dynamism. Yet, the U.S. tech sector is not fated to always be dominant. Moreover, its current policy upheavals in areas such as immigration may suppress future tech growth by pushing innovators elsewhere. Regardless, different regions of the world are steadily creating leading tech players of their own. Singapore-based Grab became so competitive that it pushed Uber out of the Southeast Asian ride-hailing business. Uruguay-based Mercado Libre is the largest e-commerce company in Latin America, crushing Amazon in the region. Sweden-based Spotify is the largest music streaming company in the world. The key policy question for Canadians should be: *What are the conditions necessary for growing more world-leading tech companies in Canada?*

[2] Dr. Dan Ciuriak. *Technological Conditions and the Rise and Fall of the Rules-Based System*. SSRN. April 23, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4762228.

An essential dimension is public policy. Canada's prosperity and national security are inextricably linked to the privacy and cyber security of its digital realm. Ensuring balanced policies that are permissive of innovation, effective in application and protective of privacy can be challenging. There is a wide array of approaches to these matters across the world. Mastering the right combination of approaches for Canada is fundamental to its success in the emerging global order.

As a baseline proposition, it is not overstating matters to say that strong encryption and effective cyber security have become strategic imperatives for Canada. This policy report, prepared for the Canadian Chamber of Commerce's Future of Business Centre, examines the critical role of encryption and cyber security in Canada, the evolving threat landscape, and the policy choices facing the country. It explores why maintaining robust encryption is vital for economic and personal security, the dangers posed by cybercrime and potential encryption weaknesses, and how Canada's approach is diverging from that of some allies like the United States. The report also reviews Canada's efforts to assert an independent stance and how these efforts align with growing a strong domestic tech sector. Comparisons are drawn with other jurisdictions (notably the European Union and Australia) to contextualize Canada's approach. Finally, the report provides actionable recommendations for policymakers and business stakeholders to reinforce Canada's cyber security, protect privacy and promote innovation.

The Critical Importance of Strong Encryption and Cyber Security in Canada

Robust encryption and cyber security measures are cornerstones of Canada's economy, government operations and personal privacy in the digital age. They provide the trust and security to citizens, consumers, businesses and governments that allow digital transactions and communications to flourish.

Protecting the Economy and Commerce

Encryption secures the vast range of economic activities now conducted online — from banking and e-commerce to intellectual property exchange. It protects sensitive trade secrets, business strategies and customer data from industrial espionage or theft.[3] As most Canadian companies are small-or medium-sized enterprises (SMEs), their ability to compete and innovate often hinges on affordable access to strong encryption and secure networks. Deliberately weakening the encryption available to businesses or their customers would directly undermine their growth and erode customer trust.[4]

[3] https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cyber security-economic-growth-and-foreign-policy/#:~:text=Encryption%20is%20used%20to%20protect,the%20trust%20of%20their%20customers.

[4] Ibid.

Canadians now spend an estimated $100 billion CAD annually on retail e-commerce. These transactions are made possible only by encrypted payment systems that assure consumers their credit card and personal data remain confidential. Without encryption and cyber safeguards, the digital economy's remarkable growth would surely falter due to lack of trust.

Securing Government Operations and Critical Infrastructure

Federal, provincial and municipal governments rely on encryption to secure everything from classified communications and citizen records to critical infrastructure controls. Communications infrastructure — including telecommunications, transportation, energy, and financial systems — all use encryption to maintain integrity and prevent malicious intrusions. Public Safety Canada notes that encryption "protects the integrity of critical national infrastructure, individuals, and businesses, from malicious intrusion, including everything from telecommunications and transportation systems to financial services and the energy sector."[5] Government cyber security is national security: Encrypted networks safeguard military and intelligence communications, and cyber security defenses keep hostile actors from sabotaging Canada's critical infrastructure or stealing sensitive data. The Government of Canada has a dual interest: Using strong encryption internally to safeguard its operations and promoting high cyber security standards across Canadian society to make the country less vulnerable and more prosperous.

[5] https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/035/index-en.aspx?wbdisable=true#:~:text=Encryption%20has%20gained%20considerable%20traction,protect%20exchanges%20from%20being%20exploited.

Protecting Personal Privacy and Data

For individuals, encryption is often the last line of defense protecting the privacy of personal data and communications. In an era when Canadians entrust healthcare information, financial records and daily conversations to digital services, encryption ensures that this sensitive information remains confidential and only accessible to intended parties. End-to-end encryption in messaging apps, for instance, allows Canadians to communicate privately without fear of eavesdropping — a modern necessity for exercising the fundamental right to privacy. While the *Canadian Charter of Rights and Freedoms* does not include a specific right to privacy, courts have interpreted the right to be secure against unreasonable search and seizure (Article 8) as a strong privacy protection in the realm of communications. The Supreme Court of Canada has repeatedly affirmed that individuals have a reasonable expectation of privacy in their digital communications, rejecting the more "permissive" U.S. approach that denies privacy for data shared with third parties.[6] Encryption thus supports Charter rights by technically enabling privacy in the digital realm. It also underpins freedom of expression and association. In 2020, none other than the Five Eyes governments[7], including Canada, issued an *International Statement on End-to-End Encryption and Public Safety*. It states that "strong encryption...plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security," and is an "existential anchor of trust in the digital world."[8] In other words, strong encryption underpins Canada's existence as a free society and the status of Canadians as a free people.

Strong encryption and cyber security are not niche concerns for digital network engineers. Rather, they are the cornerstones of security, prosperity and privacy.

[6] https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/#:~:text=In%20contrast%2C%20that%20potential%20seedling,the%20same%20types%20of%20personal.

[7] The Five Eyes is the intelligence sharing network comprised of the government of Canada, the United States, the United Kingdom, Australia, and New Zealand.

[8] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-jnt-sttmnt-ncrptn-pblc-sfty/index-en.aspx#:~:text=We%2C%20the%20undersigned%2C%20support%20strong,weaken%20or%20limit%20security%20systems.

Growing Cyber Threats in a Digitized Global Economy and Society

Over the past 25 years, everything has become digitized. It is therefore of little surprise that criminals, propagandists and spies from hostile jurisdictions now spend much of their time in cyberspace. Online retail platforms allow Canadians to access goods from the far concerns of the world. Yet, this same connectivity pulls threats from across the globe into the lives of Canadians. Safety, security and trust have never been more important.

Growing Cybercrime

From the perspective of the bad guys, this is the "golden age" of cybercrime. These criminals have continued to proliferate because they can make large profits while facing low risk of arrest, especially when they operate on a cross-border basis. Some nation states even operate in a type of public-private partnership with criminal gangs. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023–24* (NCTA) identified ransomware as the cybercrime most likely to impact Canadian organizations and individuals.[9] In 2021 there were at least 235 known ransomware attacks on Canadian industry — an average of almost five per week — with each incident costing an average of $6.35 million in recovery and lost opportunities.[10]

[9] https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

[10] https://www.cigionline.org/articles/inadequate-cyber-defence-is-damaging-canadas-economy/#:~:text=Incidents%20such%20as%20these%20may,attacks%3B%20most%20were%20launched%20by.

Threats to Critical Infrastructure

In a digitized economy, critical infrastructure is a prime target for both cybercriminals and state-sponsored hackers. The constant attacks on Ukraine's power grid serves as a reminder of the vast scope of destruction that cyber weapons can cause to the key operating systems of society. Canada is certainly not immune. Sectors such as finance, energy, transportation and healthcare have suffered major cyber incidents. Cybercriminal groups target critical infrastructure operators knowing that disruptions can be more harmful and force quicker ransom payouts. For example, an attack on a pipeline or a power utility can interrupt services to millions. Hostile nations target critical infrastructure both for espionage purposes and because of its vast potential to cause destruction in the event of a war. The Communications Security Establishment (CSE) — Canada's signals intelligence and cyber defense agency — reports blocking billions of malicious cyber actions targeting government systems annually. The overall picture is one of "complex and sophisticated" threats, requiring constant vigilance.[11]

The cyber threat environment facing Canada and Canadians is daunting. Cyberattacks are a clear and present danger to Canada's economic prosperity, public safety and individual wellbeing. This justifies the strong emphasis Canada places on cyber security. It also forms a crucial backdrop to debates about encryption and lawful access — the rise in crime and difficult-to-trace attacks is often cited by law enforcement as a reason to seek more powers, including access to encrypted data.

[11] https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

Weakening Encryption Poses Material Risks to Canadian Interests

In response to rising cybercrime and national security concerns, some voices — often law enforcement or intelligence agencies — have proposed weakening encryption protections to allow easier access to data.

This is typically termed “exceptional access” or “lawful access.” Specifically, this would involve requiring technology companies to build backdoors into encrypted services or mandating that users’ encryption keys be escrowed so government can obtain them when needed. While the motive is to help police catch criminals or prevent terrorist attacks, such measures would introduce grave risks to Canada’s economic, security and civil liberties interests. Placing “backdoors” into systems offers an open invitation to malicious actors to exploit it. Virtually every cyber security expert and major tech company agrees that deliberate weaknesses in encryption undermine security for all and are not worth the supposed trade-off in public safety. In addition, backdoors would undermine the trust of users of and customers for Canadian products and services. This is a hardly a good way to build a globally competitive digital sector.

What Canada's Laws Say about Cybercrime and Legal Access

Canadian criminal law addresses encryption indirectly, mainly in the context of lawful access to information.

Part VI of the *Criminal Code* governs the interception of private communications (wiretaps) and generally requires police to obtain a judge's authorization (warrant) to intercept communications. These interception provisions apply to any communications, encrypted or not.

There is no exception in the law that changes the warrant requirement due to the communication being encrypted. In other words, police are not given any additional authority to intercept, and they must still meet the high threshold for a wiretap warrant under Part VI. If a communication is lawfully intercepted but encrypted. For example, if investigators wiretap an End-to-End Encrypted (E2EE) messaging stream, the law allows the interception but does not compel the service provider to decrypt the content. Unlike some jurisdictions, Canada has no law that forces tech companies to ensure their systems are decryptable; thus, end-to-end encrypted messages caught in transit remain gibberish to authorities unless they can break the encryption on their own.

One important exception pertains to regulations on licensed telecommunications providers. Since 1995, the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) has imposed technical requirements on wireless carriers as a condition of license. Standard 12 of the SGES requires telecom providers to provide encrypted communications on its network to law enforcement "in clear" (unencrypted) form upon lawful request. This effectively discourages them from using any encryption on voice/data traffic that they cannot later decrypt for law enforcement. For Internet-based services (messaging apps, VoIP, etc.), there is no equivalent Canadian regulation mandating encryption design. Internet and tech companies generally fall outside traditional telecom licensing, so E2EE services (e.g., WhatsApp, iMessage, BlackBerry Messaging) are not bound by SGES and can deploy strong encryption freely.

Beyond real-time interception, the *Criminal Code* provides for search warrants and production orders to obtain stored data. These can reach encrypted information. For example, police can seize an encrypted device or compel an internet provider to hand over encrypted records. However, Canadian law does not force the recipient of such an order to decrypt the data or reveal an encryption key if they are not already in possession of the plaintext. The *Protecting Canadians from Online Crime Act* (2014) expanded these investigative powers (adding preservation demands/orders and updated production order powers), but it did not create any new obligation to assist with decryption.

Canadian law does criminalize certain cyber activities related to encryption in specific contexts. For instance, it is illegal to willfully intercept private communications without lawful authority, so hacking into someone's encrypted communications stream is a crime. It is also an offense to possess or use a device to obtain computer services fraudulently; theoretically this could include using encryption-cracking tools maliciously, though the law targets hacking devices more broadly. Notably, using encryption to conceal evidence of a crime is not a crime in itself. While obstruction of justice charges could apply if someone destroyed evidence, simply encrypting one's files or communications is a legal act even if it frustrates investigators.

The *Criminal Code* allows a judge who issues a warrant or wiretap authorization to order third parties to assist police in executing it through a "lawful access" assistance order. Prosecutors have attempted to use this to compel decryption assistance (e.g., ordering a suspect or a tech company to help unlock a device). To date, no Canadian law explicitly compels an individual to disclose their password or encryption key, and such efforts run into constitutional barriers. In a 2010 Quebec Court of Appeal case, the court stated

that forcing someone to reveal a password is inadmissible and any data obtained as a result would be an “unreasonable” seizure — the law will not permit an order that effectively compels a person to self-incriminate. Similarly, in R. v. Shergill (2019), an Ontario court refused to enforce an assistance order against an accused to make him unlock his phone, concluding that compelling a password would violate the Charter right against self-incrimination. These cases underscore that under the *Canadian Charter of Rights and Freedoms*, an accused person has the right not to be conscripted into aiding their own prosecution (sections 7 and 11(c) of the Charter protect against self-incrimination and being forced to testify against oneself).

For third parties like companies, the law is less settled. An assistance order could potentially require a tech company to assist (for example, attempting a decryption if feasible), but since most E2EE providers do not hold the keys, they have no ability to comply. As of now, there is no statute that clearly requires a tech company to build a decryption tool or backdoor for investigators. Any such demand would likely be challenged under the Charter as well, engaging privacy rights under section 8 and freedom of expression if it compels writing new code. In practice, Canadian police have sometimes found creative workarounds. In one case, the RCMP obtained a BlackBerry master encryption key through undisclosed means and used it to decrypt over one million messages during a criminal investigation. But such instances are rare and often shrouded in secrecy. The bottom line in criminal law is that encryption is recognized as a barrier that police must overcome with existing powers. The fact that a tech company’s encrypted data could constitute a barrier to law enforcement is not regulated by a special anti-encryption law.

In the broader critical infrastructure and government sector, encryption is largely seen as a positive security measure. Canada’s cyber security policies encourage the use of robust encryption to protect critical systems from cyber threats, such as banking, energy, and transportation networks. For example, the Government of Canada’s *National Cyber Security Strategy* and the guidance of the Canadian Centre for Cyber Security promote strong cryptographic standards for securing sensitive data and communications in critical systems. In regulated industries, authorities often recommend or require encryption through standards. For instance, financial institutions under the Office of the Superintendent of Financial Institutions (OSFI) are expected to encrypt customer data and transactions as part of meeting OSFI’s cyber risk management guidelines. In healthcare, as discussed, regulators insist on encryption for patient information.

Geopolitical Factors and a Fracturing Five Eyes Alliance

The Five Eyes alliance has been a pillar of the democratic world's security architecture for the past eight decades. It is built on trust and shared values — that now appear to be fracturing.

The origins of the Five Eyes can be found on the security cooperation among allies in World War II. Canada, having effectively been granted full autonomy from Britain under the 1931 Statute of Westminster, asserted its foreign policy independence by separately declaring war on Germany in September 1939. Throughout the conflict, Canada built and delivered distinct capabilities in support of the Allied Cause. In June 1941, Canada established the Examination Unit (XU) — its first civilian cryptographic bureau — under the auspices of the National Research Council (NRC).[12]

The XU played a key role in supporting Allied efforts to crack enemy codes and ciphers used in communication signals from 1941 to 1945. The XU achieved significant successes, such as deciphering codes and cracking the transposition cipher of the Vichy fleet.[13]

At war's end, Canada's leaders decided to maintain a civilian cryptographic bureau. They understood the value of a specialized government agency dedicated to a growing need for protecting sensitive information. The NRC's Communications Branch began operations in 1946, staffing it with XU veterans. XU's wartime work had proven pivotal to establishing the groundwork for Canada's peacetime signals intelligence (SIGINT) capabilities, securing Canada's position in post-war intelligence negotiations, and helping to establish cryptography as a key function of the federal government.[14] In 1975, the Communications Branch was renamed

[12] See text at: https://www.canada.ca/en/parks-canada/news/2021/08/the-examination-unit-19411945.html.

[13] See text at: https://parks.canada.ca/culture/designation/evenement-event/examen-examination.

[14] See text at: https://www.canada.ca/en/parks-canada/news/2021/08/government-of-canada-recognizes-second-world-war-civilian-cryptographic-bureau-as-a-national-historic-event.html.

the Communications Security Establishment (CSE)[15], which would henceforth report to the Minister of National Defence.

The Five Eyes intelligence-sharing alliance was established through a series of agreements. This partnership grew from the successful wartime intelligence collaboration between the United States and Great Britain. In 1949, Ottawa and Washington signed the CANUSA agreement.[16] The alliance was expanded to include Australia and New Zealand in 1956.[17] Throughout the Cold War, this strong network of trust proved incredibly effective and durable.

Following the Cold War, Canada's SIGINT activities, like those of its allies, changed with the times. With the onset of the Afghanistan war in 2001, CSE was called upon to support troops in a combat situation for the first time since the Korean War. By its own admission, CSE provided half the intelligence on Taliban militants, leaders, and their strategies used by the Canadian Army in the war. Much of the rest came from its intelligence partners, especially the Five Eyes. Canada, of course, provided lots of actionable intelligence to its allies with troops on the ground. By 2016, CSE was playing a critical role, including through the hacking of computer systems in Operation Impact — the Canadian Armed Forces' mission against ISIS.[18]

In addition, CSE followed technology changes. With the rise of the internet, less SIGINT was moving through phone calls and more was moving online. In 2000, CSE set a new mission for itself: "to be the agency that masters the global information network to enhance Canada's safety and prosperity."[19] In 2001, following the 9/11 attacks, the Government of Canada passed the *Anti-Terrorism Act*, which effectively helped to realize this vision. It empowered CSE to significantly expand its digital surveillance activities and to organize a robust cyber defense.[20] By the mid-2010s, it often came to be said that the digital intelligence and cyber security capabilities of CSE punched well above its weight relative to its budget. In 2018, the Government of Canada created the Canadian Centre for Cyber Security, both to deal with threats to government networks and those across the country.[21]

[15] See text at: https://www.cse-cst.gc.ca/en/culture-and-community/history.

[16] See text at: https://www.cips-cepi.ca/2020/10/21/the-changing-scope-of-the-five-eyes-implications-for-canada/.

[17] See text at: https://direct.mit.edu/jcws/article/25/1/101/115125/Why-the-Five-Eyes-Power-and-Identity-in-the.

[18] Murray Brewster. *Canada's electronic spy service to take more prominent role in ISIS fight*. CBC News. February 18, 2016. https://www.cbc.ca/news/politics/canada-spy-agency-isis-fight-1.3454617.

[19] Bill Robinson. *Marking 70 years of eavesdropping in Canada*. OpenCanada. September 1, 2016. https://opencanada.org/marking-70-years-eavesdropping-canada/.

[20] *Part II: Evolution of the Government's Framework for Cyber Defence*. National Security and Intelligence Committee of Parliamentarians. February 14, 2022. https://nsicop-cpsnr.ca/reports/rp-2022-02-14/04-en-part-2.html.

[21] Ibid

The fracturing of the Five Eyes alliance is a tragedy for all involved, but a restoration in the current political climate seems challenging. The Trump administration typically presents its closest traditional allies as “freeloaders” who are “ripping off” the United States. President Trump’s tariffs and near constant statements about his desire to annex Canada have poisoned the relationship with the United States. In February 2025, the *Financial Times* reported that Peter Navarro, an influential Trump trade advisor, was pushing to remove Canada from the Five Eyes as a way of putting pressure on Canada’s economy.[22] While Navarro denied the report, it is consistent with the Trump approach to foreign policy: To throw away eight decades of trust and partnership for short term leverage.

The bottom line is that Canada will need to reduce its dependence on intelligence sharing with the United States and pursue different partnerships consistent with the realities of this era while significantly investing in building its own capabilities.

[22] https://www.ft.com/content/2dfa3c11-64a7-49f6-83df-939b8d1cfb8e.

In addition to the “Trump factor,” the Five Eyes countries have also been diverging on certain key policy issues including lawful access and surveillance/privacy.

Lawful access: The U.S., UK, and Australia have tended to form a more hardline cohort pushing for “lawful access” to encrypted communications. New Zealand and Canada, while generally supportive, have been quieter and somewhat more moderate in their rhetoric. In 2016, the UK passed the sweeping *Investigatory Powers Act* that includes provisions to remove electronic protections (encryption) under warrant. In 2018, Australia passed a far-reaching anti-encryption law which compels companies to assist authorities in accessing encrypted data. By contrast, while Canada signed on to language urging tech companies to find solutions for government access to encrypted data, it has not translated this into domestic law.

Surveillance: As noted above, U.S. courts adhere to the “third-party doctrine,” whereby information voluntarily given to third parties like banks, telecom companies, or online service providers receives no privacy protection under the Fourth Amendment. According to Citizen Lab, this has enabled extensive warrantless data collection by U.S. authorities since the 1970s.[23] In contrast, Canadian jurisprudence has rejected this doctrine. The Supreme Court of Canada warned that unrestricted electronic surveillance “would annihilate any expectation that our communications will remain private,” and thus requires strict oversight.[24] The result is that Canadian law imposes more constraints on law enforcement access to data (warrants, court orders, etc.) and views privacy as a quasi-constitutional right even in digital contexts. This divergence means that certain U.S. practices like broad subpoenas for internet metadata or the Patriot Act’s provisions would likely be deemed unconstitutional in Canada. More generally, the United States has no national privacy regime. Canada does have such a regime, built around federal and provincial laws and institutions such as the Privacy Commissioner (see Annex A for a more detailed overview of Canada’s regime). This difference in philosophy regularly creates tensions around cross-border data flows and cooperation.

[23] https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/#:~:text=are%20more%20incompatible%20when%20it,law%20enforcement.

[24] Ibid.

Aligning Privacy and Security Efforts with Tech Sector Growth and Strong Encryption Standards

Canada's approaches to privacy, encryption and cyber security policy are not unfolding in a vacuum. Rather, they directly intersect — and shape — the country's economic ambition to foster a world-class domestic tech sector. Rather than seeing security and privacy as burdens on industry, Canada increasingly views them as differentiators that can spur innovation and growth.

Trust as a Competitive Advantage

In the digital marketplace, trust is currency. Companies that can assure users and clients that their data is secure and handled responsibly stand to gain a significant competitive edge. With strong privacy laws and a reputation for security, Canada is positioning itself as a jurisdiction of high trust. For example, this can attract businesses to set up AI research in Canada, knowing the regulatory environment respects privacy and avoids the "complexities inherent" in jurisdictions such as the U.S. or China. It can also be a selling point for Canadian tech firms expanding globally as they can say their products are built and tested under one of the world's strictest privacy regimes, which is appealing to privacy-conscious consumers and enterprise customers, especially in Europe or Asia. For example, a Canadian software company that complies with Europe's General Data Protection Regulation (GDPR) by design can more easily market in international markets than a U.S. competitor that might have to retrofit compliance. If Canada continues to champion encryption (ensuring that business communications, cloud storage, etc. are secure), it creates an environment where digital entrepreneurs can build services without constantly worrying about breaches undermining their business model. High encryption standards also mean fewer devastating cyber incidents, which in turn makes Canada a stable place to do business. In short, Canada's refusal to weaken encryption can actually attract companies that want to promise security to their customers.

Aligning with Global Strong Standards — A Trade Diversification Strategy

Canada's alignment with strong privacy/encryption also smooths the path for its companies to operate and grow internationally. Adopting standards akin to GDPR, for instance, means Canadian companies are already compliant or close to it when entering the European market. Similarly, championing encryption means Canadian communications apps or devices would not be viewed with suspicion in regions with strict privacy laws. As other jurisdictions raise their standards (even the U.S. tech industry is moving toward more privacy due to consumer demand and state-level regulation), Canadian firms that grew under high privacy and high security expectations will be ahead of the curve.

Developing Talent and Skills

Both cyber security and the broader tech sector growth in Canada face a huge skills shortage.[25] Aligning efforts here means training the next generation of skilled workers who can drive both security and innovation. The government and private sector are collaborating on initiatives to address the cyber security talent gap — funding more university programs, creating cyber ranges for training and supporting initiatives to bring underrepresented groups into tech, thus broadening the talent pool. Growing a strong domestic tech sector requires a robust pipeline of engineers, developers and researchers. By making cyber security "cool" and a priority, which is helped by public emphasis on national security and big-picture importance, more students may go into these fields. The Canadian Chamber of Commerce and businesses can partner with academia to offer internships and co-ops in security and privacy, aligning educational output with industry needs. Additionally, if Canada is seen as a pro-privacy, pro-security environment, it may retain talent that might otherwise move to Silicon Valley — some tech workers choose employers and countries based on ethical alignment. For instance, a skilled cryptographer or AI ethicist might prefer to work in Canada where the legal framework aligns with their values, rather than somewhere they feel their work might be used for mass surveillance.

Cyber Security as an Export Sector

With Canada's policy regime being broadly supportive of robust cyber security, Canada should begin to imagine a future in which cyber security services and cybersecure goods become export sectors. The government has been broadly supportive of building out Canada's cyber security knowledge base and commercial sector. With its high standards, it should pursue partnerships with companies and governments abroad interested in this orientation.

[25] https://ictc-ctic.ca/reports/accelerating-canadas-workforce#section-report.

A Short Diversion into Canada's Quantum Future

In the history of technology, there are occasionally transformational leaps that change everything. While AI is getting most of the headlines, the rise of quantum technologies, especially quantum computing, will be transformational.

Quantum technologies are based on quantum mechanics, a fundamental theory in physics that describes the physical properties of nature at the scale of atoms and sub-atomic particles. The ideas that gave rise to quantum mechanics arose gradually over the first three decades of the 20th century. Quantum mechanics is one of the strangest, most magnificent and least intuitive theories ever to be developed in the history of science. While studying atoms and sub-atomic particles sounds esoteric, in the decades after it was proposed, knowledge of quantum mechanics would facilitate the development of technologies as diverse as the atomic bomb, the semi-conductor, life-saving Magnetic Resonance Imaging (MRI) machines and Global Positioning Systems (GPS).

The great dream of many quantum scientists is to build a functional quantum computer. As this technology progresses, the impact of quantum tools and techniques on our communications systems and methodologies will only grow. Traditional encryption methods rely on the difficulty of factoring large numbers or solving discrete logarithm problems — two tasks that quantum computers would solve exponentially faster. That means that once quantum computing reaches a sufficient level of maturity, many existing encryption protocols will no longer be secure, potentially exposing sensitive communications, financial transactions and state secrets.

Canadian companies and policymakers must prepare for the transition to post-quantum cryptography (PQC) — new cryptographic methods resistant to quantum attacks. Organizations such as the U.S. National Institute of Standards and Technology (NIST) are currently standardizing quantum-resistant encryption algorithms. Canada is actively involved in these technical efforts. Additionally, the Canadian Centre for Cyber Security and government initiatives like Quantum-Safe Canada are investing in quantum-safe encryption solutions. These efforts include transitioning Canadian government IT systems to post-quantum algorithms.[26]

Canada's *National Quantum Strategy* (NQS), launched with a $360 million investment over seven years in Budget 2021, explicitly prioritizes quantum-safe cyber security. The NQS report[27] highlights the "significant risk" quantum computing poses to current cryptography and urges the government to "raise awareness of quantum security issues" and foster a sense of urgency in responding.[28]

Canada is a leader in quantum research, with institutions like the University of Waterloo's Institute for Quantum Computing (IQC) and companies like Xanadu Quantum Technologies developing quantum-resistant security measures. Canadian companies are combining traditional cryptography with quantum-resistant techniques to ensure long-term data protection. As Canadian quantum hardware firms like Xanadu and D-Wave Systems continue to advance, they serve as a double-edged sword — bolstering the economy while also bringing closer the day when quantum machines could break classical encryption. This dynamic has spurred local cyber security companies to create solutions today for tomorrow's threat, with innovations in hybrid certificates, tools for quantum risk assessment and aids for PQC deployment.[29] Companies such as Quantum Bridge Technologies specialize in quantum-safe communications.[30]

Canadian financial regulators and security agencies are also gearing up for the PQC transition. Canada is part of the G7 Cyber Expert Group, which, in 2022, warned that financial institutions must start adopting PQC to safeguard sensitive data.[31] Sectors like energy and healthcare that handle long-lived sensitive data are being advised by the Canadian Centre for Cyber Security to consider the "Harvest Now, Decrypt Later" threat — where adversaries steal encrypted data now to decrypt once a sufficiently powerful and accurate quantum computer is available.[32]

As quantum computing advances, Canadian companies and policymakers must take proactive steps to ensure encryption remains robust against future threats. The Canadian government should encourage the adoption of quantum-safe E2EE solutions in critical infrastructure, finance, healthcare, and national security. By transitioning to post-quantum encryption and maintaining strong E2EE protections, Canada can safeguard its digital infrastructure, protect citizen privacy and remain a leader in the global cyber security landscape.

[26] Preparing your organization for the quantum threat to cryptography (ITSAP.00.017) - Canadian Centre for Cyber Security

[27] https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy.

[28] Demystifying Canada's Quantum Strategy | InfoSec Global)

[29] ISARA Dedicates Four Hybrid Certificate Patents to the Public ...

[30] Quantum Bridge Gains Fast-Track Approval in Canada for Quantum-Safe Encryption with DSKE and Post-Quantum Cryptography Quantum Bridge Gains Fast-Track Approval in Canada for Quantum-Safe Encryption with DSKE and Post-Quantum Cryptography

[31] G7 Cyber Expert Group Warns of Quantum Computing Risks in

[32] Preparing your organization for the quantum threat to cryptography (ITSAP.00.017) - Canadian Centre for Cyber Security

Policy Recommendations

Drawing on the analysis above, this report offers the following actionable policy recommendations for the Canadian government and stakeholders to bolster privacy, encryption and cyber security in a manner that supports both security and economic prosperity. The recommendations are aimed at ensuring Canada remains a leader in digital trust, protects its interests against cyber threats and fosters a thriving tech ecosystem.

Encryption Policy and National Security

1. Publicly commit to preserving strong encryption and rejecting backdoors: The Government of Canada should issue a clear, high-profile policy statement affirming that strong, uncompromised encryption will remain legal and accessible in Canada. It will not require technology companies to embed weaknesses or backdoors into their products. There will be no mandatory decryption or "exceptional access." Canada's commitment to strong encryption would send a strong signal to businesses and the Canadian public, solidifying the country's stance that security and privacy will not be sacrificed. This public commitment would also reject the narratives around finding a "balance" in encryption policy. Rather, it would make clear that strong encryption is the precondition for secure governance, privacy and innovation.

2. **Affirm encryption as essential infrastructure:** Treat robust encryption as non-negotiable for Canada's national security, digital sovereignty and global economic competitiveness. Ensure that strong encryption is supported throughout the country.

Law Enforcement and Investigative Capabilities

3. Invest in investigative alternatives: There are many ways law enforcement can undertake effective investigations without mandating the engineering of vulnerabilities into the technologies used by Canadians. For example, government could, either directly or through the support of innovative Canadian firms, fund robust work programs on advanced analytics and targeted forensics that do not undermine encryption. They could also further explore the contribution of lawful hacking. This would be part of a bigger work program supporting lawful access innovation. It would focus specifically on funding research and development of investigative methods that operate within encryption constraints.

4. Foster voluntary cooperation: Encourage collaborative frameworks between tech providers and law enforcement that protect user privacy and system integrity. Such programs can build trust and yield innovative results without "breaking the engineering."

Cyber Security and Critical Infrastructure

5. Standardize strong encryption requirements: Standardizing strong encryption standards is an essential step. The federal government should work with the provinces to require E2EE and advanced cryptographic safeguards across regulated sectors, including finance, healthcare and energy.

6. Enhance institutional capacity: The Government of Canada should increase resources for the Canadian Centre for Cyber Security to lead encryption implementation and secure infrastructure adoption. It should also look at how it can better collaborate with the Canadian Cyber Threat Exchange in pushing out sound cyber practices to Canadian businesses and non-governmental institutions.

7. Promote encryption in national security policy: The Government of Canada should embed encryption standards in its government procurement and digital resilience strategies. This way, it's employing directly or aiding in the dissemination of secure robustly engineered technologies.

8. Support Businesses — especially SMEs — in improving cyber security defenses: Many breaches and ransomware incidents exploit the fact that smaller organizations have fewer resources and less expertise to deploy strong defenses. The government should expand programs that provide financial incentives and expertise for cyber security upgrades. This could include tax credits for certified cyber security investments (e.g., adopting multi-factor authentication, encryption of data at rest, security training for staff), or grants/ vouchers for SMEs to obtain cyber security assessments and improvements. Scaling up the CyberSecure Canada certification program is one practical step: Make it widely known and perhaps offer a modest subsidy for the cost of certification for first-time participants. The government can also consider a "cyber security marketplace" where vetted Canadian vendors offer discounts or special packages for small business needs (antivirus, managed backups, etc.). By raising the baseline security of all businesses, Canada reduces the overall attack surface.

9. Enhance cyber literacy and workforce development: Long-term strength in cyber security and privacy requires a knowledgeable public and a skilled workforce. The government should expand digital literacy programs to include basic cyber security and privacy education for citizens. For example, this could include modules on subjects such as how to use encryption tools and how to avoid phishing. At the same time, the government should scale up initiatives to address the cyber talent gap. Actions could include providing scholarships for students in cyber security, incentivizing mid-career professionals to get cyber training and fast-tracking immigration for cyber security experts from abroad.

Post-Quantum Cryptography (PQC)

10. Lead the PQC transition: Building on its sizeable quantum science investments over the years, Canada should broadly mandate early adoption of post-quantum cryptographic standards and align federal systems with NIST recommendations. It should also integrate PQC into tech modernization programs. It must ensure that digital transformation efforts across government include quantum-resistant encryption upgrades. Finally, on workforce, Canada should co-invest with universities and companies in training for professionals in quantum cryptography, risk modeling and secure communications.

Trade Diversification

11. Integrate cyber security and privacy into economic strategy: Canada needs to fully embrace a commercial strategy based on being a high privacy, high security and high trust jurisdiction. The quality of its standards and practices should be the core of the Canadian brand in the digital realm. Operationally, the Government of Canada could launch an initiative that provides funding and incentives to tech companies building security and privacy-enhancing products, such as encryption software, privacy-respecting AI, secure messaging platforms and other digital innovations that support these objectives.

12. Carefully manage digital issues in the new North American trade agreement: As Canada and the United States pursue the negotiation of some type of new trade arrangement, core digital policy issues may well be on the agenda. Canada will need to stand firm to ensure that privacy and other fundamental rights are not put at risk.

International Engagement

13. Advance strong global encryption standards: By carving out a strong encryption policy, Canada has an incentive to shape encryption policy internationally. One way to do that is to bolster Canadian leadership in IETF, ISO, and multilateral cyber security forums to shape resilient encryption norms. It should also prioritize its encryption efforts diplomatically. This includes opposing international efforts to weaken encryption in digital trade agreements or cross-border surveillance compacts.

14. Foster international alliances on strong privacy and cyber norms beyond Five Eyes: Canada should leverage its unique position to build broader coalitions on digital policy — for instance, working with the European Union, Japan and other democracies on a joint statement or framework that endorses strong secure-by-design encryption ecosystems. In doing so, Canada is making the argument that it is a “strong link” in the cybersecure train. In so doing, it can effectively reject the criticisms of its Five Eyes partners.

Ongoing Consultations and Analysis

15. Continuously review and update policies with stakeholder input: Technology and threats evolve quickly. The government should establish a regular review cycle every three years for major policies such as on cyber security and privacy. By institutionalizing review processes, Canada can remain agile and avoid policy stagnation.

A Final Note

Canada is in a moment of great change and is worried about its future. The new government needs to act boldly and with great clarity.

By implementing these recommendations, Canada can strengthen its economy and security simultaneously. The guiding principle is that privacy, encryption and cyber security are not obstacles to overcome, but rather foundations to build upon. Ensuring our laws and programs reflect that will keep Canada safe, competitive and free in the digital era.

Annex One: A Short Overview of Privacy in Canada

For much of the first 100 years of Confederation, privacy was a concept which played out among individuals in the local towns and villages.

By the 1960s, privacy began to be a concern of governments. In a debate over decriminalizing homosexuality, then Justice Minister Pierre Trudeau famously declared in 1967 that "the state has no place in the bedrooms of the nation." This was, in essence, a statement of what the government would not include in the Criminal Code. By the 1970s, federal and provincial governments began to enact laws designed to specifically protect the privacy of citizens and ensure access to government information. By the 1990s, the rise of the internet and digital technologies created wholly new challenges.

Canada's privacy and data protection laws strongly influence the use of encryption as a safeguard for personal information, making encryption a best practice for protecting data privacy. The *Personal Information Protection and Electronic Documents Act* (2000) (PIPEDA), the federal law governing the private sector, requires organizations to protect personal data with appropriate security measures. Principle 4.7 explicitly states that security safeguards should include technological measures such as passwords and encryption. This creates a legal expectation that companies will use encryption, among other controls, to prevent unauthorized access to personal information. The Office of the Privacy Commissioner of Canada (OPC) has reinforced this in guidance, encouraging businesses to encrypt sensitive data on laptops and portable media as part of breach prevention.

Provincial private-sector privacy laws (such as Alberta's PIPA, British Columbia's PIPA, and Quebec's privacy law) mirror the federal requirements, requiring organizations to use reasonable security measures — often met by employing strong encryption for sensitive data.

In the public sector, the federal *Privacy Act* (1985) and similar provincial laws require government institutions to safeguard the personal information they hold. While these laws do not list specific technologies, in practice, encryption is a cornerstone of government IT security policy for protecting sensitive and personal data. For example, federal government directives, aligned with Communications Security Establishment standards, mandate encryption for transmitting and storing protected information. In the health sector, some laws and guidelines go further in specifying encryption: Ontario's *Personal Health Information Protection Act* (PHIPA) requires health custodians to take reasonable steps to secure patient data. The Ontario Privacy Commissioner has made clear that this means health information stored on mobile devices must be encrypted to prevent breaches. Canada's privacy framework doesn't merely allow encryption, it effectively encourages or even necessitates encryption as a best practice to comply with legal duties to safeguard confidentiality.

Canadian Chamber of Commerce

Chambre de Commerce du Canada

Canadian Chamber Future of Business Centre

Centre de l’avenir des affaires de la Chambre de Commerce du Canada