Cybersecurity needs faster, seamless public-private collaboration, say cyber experts

Continued on page 20

In the Communications Security Establishment annual report, Defence Minister Anita Anand said that increased activity by cyber threat actors, and the many warnings issued by the CSE to Canadian critical infrastructure providers, are “wake-up calls for us all.” The Hill Times photograph by Andrew Meade

Cyber security needs faster, seamless public-private collaboration, say cyber experts

Automatic defences protected the government from 2.3-trillion cyber attacks in the last year, or an average of 6.3 billion a day.

BY JESSE CNOCKAERT

Countering the threat to Canada from the growing frequency and complexity of cyberattacks will require an all-hands-on-deck approach with even greater collaboration between the public and private sectors, according to cybersecurity professionals.

“[Cyber threats are] not the same from one year to the next, and I think right now the whole world of threat surface for cyber is expanding exponentially,” said Angela Mondou, president and CEO of TECHNATION, the national association representing Canada’s information, communications, and technology industry. “I think one of my key messages to the government is that governments can’t do this alone. We have to leverage the support and resources that you have as a nation.”

Federal government IT networks were targeted in cyberattacks an estimated 2.3-trillion times during the fiscal year between April 1, 2022, and March 31, 2023, or an average of 6.3-billion times a day, according to the 2022-2023 annual report from the Communications Security Establishment (CSE), released on June 29. In that same time frame, CSE responded to 2,080 “cybersecurity incidents,” which included 957 involving federal government institutions, and 1,132 against critical infrastructure organizations.

Mondou told The Hill Times that a large focus for TECHNATION revolved around developing co-operation between the public and private sector when it comes to cybersecurity, which she called “collaboration by design.” She said dialogue between the public and private sectors so far shows there is a will to collaborate, but planning how to best carry it out is the next step.

“We would take more of a crisis-management approach, which is where you create a joint operations way of working together. You co-ordinate how you’re going to communicate, who’s going to be sharing what kinds of information, deeming what’s important,” she said. “How do we adopt the same kinds of practices that we’re doing … in the tech sector, with other government agencies within Canada? It really does come down to a protocol around the information, the intelligence sharing, [and] the communication.”

The topic of cybersecurity interconnection between different levels of government, Indigenous groups, and the private sector was also discussed June 27-28 during the Waterloo Security Dialogue, a conference hosted by the Centre for International Governance Innovation, held in Waterloo, Ont.

The nature of national security and cybersecurity threats have expanded over the years to threaten individual Canadians, not just the nation as a whole, according to Mondou. “It does come down to the ability to work together in a very co-ordinated way, and getting ahead of the crisis,” she said. “The war zone is now a technical theatre. The combat operations are being driven by intelligence gained from satellites where you can now have visibility into what’s going on right on the front lines, or right to a general cell phone.”

Defence Minister Anita Anand (Oakville, Ont.) said that increased activity by cyber threat actors, and the numerous warnings issued by the CSE to Canadian critical infrastructure providers, are “wake-up calls for us all” in her forward in the CSE annual report.

“As this report shows, CSE and its Canadian Centre for Cyber Security are working hard to defend Canada from a wide variety of threats to our national security, our economic security and even our democracy itself. We must be clear-eyed about the threats we face, and we must work with all stakeholders, including partners around the world to defend our common interests,” said Anand in the report.

To help address cyberattacks on critical infrastructure, the 2022 federal budget announced $185.5-million over five years, starting in 2022-2023, and $40.6-million ongoing in new CSE funding.

CSE includes the Canadian Centre for Cyber Security (Cyber Centre), the federal government’s operational lead for cybersecurity. According to the CSE annual report, this year the Cyber Centre’s partnerships team engaged with almost 1,400 critical infrastructure organizations, including partners in the energy, finance, transportation, water and manufacturing sectors, which is up from about 1,000 groups the year before.

Dr. Gord Agnew, an associate professor in the electrical and computer engineering department at the University of Waterloo in southern Ontario, told The Hill Times that greater public and private sector co-ordination to repel cyber attacks is needed, because

Source: The changing landscape of cyber security following the COVID-19 pandemic, released July 11, 2023, by Statistics Canada

Cyber threats information

- State-sponsored cyber programs of China, Russia, Iran, and North Korea pose the greatest strategic cyber threats to Canada.
- State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these states. State actors can also exploit vulnerabilities in software and activities in Canada, Canadian organizations and their intellectual property for espionage, and even Canadian individuals and groups for financial gain.
- Cybercrime continues to be the cyber threat at large, affecting Canadians and Canadian groups. Due to its impact on an organization’s ability to function, consumers are almost certainly the most disruptive form of cybercrime facing Canadians.
- As Canada adopts smart systems and becomes more digitally transformed, more sectors and services will become vulnerable to cyber threats. This includes espionage, fraud, extortion and sabotage. Smart systems generate large amounts of data which, in certain applications, may include detailed personal information from users. As smart systems are incorporated into physical services and exposed to the internet, the potential for service disruption from cyber threat activity increases.
- Instead of targeting organizations directly, cyber threat actors are increasingly targeting the software tools and services used by groups via supply chain compromises. These threats increase when vendors have elevated access to their clients’ networks. This kind of relationship is becoming more common as cloud-based software infrastructure, and platform-as-a-service models proliferate.
- Large enterprises are almost certainly the most common form of cybercrime that Canadians will experience over the next few years as threat actors attempt to steal personal, financial, and corporate data via the internet, fraud and scams, including malicious cyber threat activity such as phishing, result in major financial losses. According to the Canadian Anti-Fraud Centre, there have been over 150,000 reports of fraud in Canada with over $600 million stolen since January 2021.

Source: The changing landscape of cyber security following the COVID-19 pandemic, released July 11, 2023, by Statistics Canada
Policy Briefing: Digital Security

How government can restore public confidence in our privacy rights

If the government truly wants to show Canadians that our privacy rights matter, it needs to pass strong data protection laws as soon as possible.

Laura Tribe
Opinion

Digital security doesn’t just mean using a different password for every account and avoiding suspicious links. It also means worrying that your sensitive, personal data has been stolen by hackers simply because you bought gas. Those affected by the recent Suncor breach are experiencing the increasingly accepted new normal for Canadians—data is a currency being exchanged, stolen, bought and sold with complete disregard for those impacted. And years of inaction and broken promises have undermined trust in the institutions meant to protect us.

Ninety-three per cent of Canadians are concerned about the protection of their privacy, according to a recent poll released by the Office of the Privacy Commissioner of Canada.

Promising change isn’t enough—Canadians need action. We need urgent, comprehensive measures to protect our privacy and restore trust in government. Here’s how Parliamentarians can do it:

First and foremost, we need corporate accountability. The federal government must deliver on its promise to overhaul Canada’s outdated privacy laws.

It’s been over four years since privacy reform was first promised. And even though the government has made Big Tech public enemy No. 1, its current privacy reform proposal, Bill C-27, The Digital Charter Implementation Act, is effectively written to let Big Tech off the hook. Not only has C-27 moved at a snail’s pace, but it’s riddled with loopholes and flaws that fail to provide the public with the confidence that the government is truly going to hold companies to account.

If the government truly wants to show Canadians that their privacy rights matter, it needs to pass strong data protection legislation as soon as possible. It needs to empower the privacy commissioner to issue binding orders and substantial fines for violations, establish a private right of action for individuals whose privacy has been violated, and remove all the new exceptions that will let the private sector dodge accountability for their data handling practices.

Second, we need new guardrails around how our information is protected within the government.

We’ve seen Bill C-59’s failed attempt to hold national security agencies to account for their re-peated overreach. Plans to update the pre-internet era federal Privacy Act abandoned, and now law enforcement can demand data for warrantless access to sensitive data held by internet companies. In short, we’ve watched continued expansions of surveillance and data collection powers without any meaningful efforts to safeguard how the government handles and shares our data.

If Canadians don’t know that government and intelligence officials are respecting our rights, how can we trust them?

Lastly, and most importantly of all, we need renewed trust in our democratic institutions.

The allegations of potential foreign election interference have rattled Canadians’ faith in our elections. To save it, we need to be able to trust those who are charged with upholding and protecting our democratic processes to correct any injustices, and strengthen our elections.

Unfortunately, our politicians’ most recent response has been to exempt themselves from accountability. Just last month, MPs used Bill C-47, the Budget Implementation Act, to carve political parties out of the privacy laws. If politicians don’t respect their own citizens in the face of an election, how can we trust them to hold others to account?

As a basic starting point, politicians must hold themselves to the same standards to which they hold the rest of us, subjecting themselves to the same standards to which Canadians’ privacy and data protection laws apply to everyone else.

Canadians’ trust in the digital world has taken a tumble. The current digital security environment is complex and intimidating. Very few of us are privacy cyberspace experts, and yet the government’s lack of action means that we’re all increasingly made to feel individually responsible for our own privacy protections.

The only way to restore trust is by taking action. It’s one thing to say you’re serious about privacy; it’s another thing to show it. We need parliamentarians to pick from the list of ideas above and get on with it. Our data mobility means we’re all increasingly made to feel individually responsible for our own privacy protections.

Laura Tribe is the executive director at OpenMedia, a grass-roots organization which works to keep the internet open, affordable, and surveillance-free.

The Hill Times

Improving Bill C-27 and fighting cyber threats facing Canada

Addressing concerns about privacy rights and their impact on joining the digital economy needs an approach involving government, industry, and civil society.

Ali Delghanthana
Opinion

Bill C-27, the Digital Charter Implementation Act, has been recognized by Canada’s Privacy Commissioner Philippe Dufresne as a step in the right direction towards protecting Canadians’ fundamental privacy rights, and supporting public interest and innovation. The bill has several positive aspects that deserve acknowledgment.

Firstly, Bill C-27 introduces new rules and regulations to enhance transparency and accountability in the handling of personal information by organizations. It establishes clear obligations for organizations to inform individuals about the collection, use, and disclosure of their personal data. Additionally, the bill grants individuals greater control over their personal data by giving them the right to request access to their information held by organizations. It also introduces a right to data mobility, allowing individuals to transfer their personal data from one organization to another. These provisions contribute to strengthening individuals’ privacy rights, and empowering them to manage their digital identities more effectively.

Secondly, there are areas where Bill C-27 can be further improved to modernize this country’s privacy law.

One key aspect is the need for stronger enforcement powers and penalties for non-compliance. Strengthening the enforcement regime would act as a deterrent and ensure that firms take privacy obligations seriously. Additionally, the privacy commissioner could be given enhanced powers to proactively audit organizations’ privacy practices, investigate complaints, and impose penalties for privacy breaches.

Another area of improvement involves incorporating more robust consent mechanisms. Consent is a cornerstone of privacy protection, and it is important to ensure that individuals can provide informed consent in a meaningful way. The bill could include provisions to enhance consent mechanisms, such as standardized consent forms, clear language, and the ability for individuals to easily withdraw consent.

Canada faces a range of cyber threats that pose significant risks to its citizens, businesses, and critical infrastructure. These threats include state-sponsored cyber espionage, cybercrime, hacktivism, and malicious cyber activities targeting government institutions, businesses, and individuals. To address these threats and mitigate the damage of cyber-attacks, the federal government has been actively working on bolstering its cybersecurity measures. Some of the key government initiatives include:

• Introducing and updating legislation to address cyber threats and strengthen the legal framework for cybersecurity.
• Establishing a comprehensive cybersecurity strategy to protect the country from cyber threats.
• Investing in cybersecurity infrastructure, including investments in critical infrastructure protection, training for cybersecurity professionals, and the establishment of cybersecurity centres of excellence across the country.
• Actively participating in international collaborations and partnerships to combat cyber threats.

Cyber threats are not limited to the country. Public campaigns, workshops, and educational resources can empower individuals to understand their rights, adopt good privacy practices, and be more discerning about the information they share online.

Addressing concerns about privacy rights and their impact on participation in the digital economy requires a comprehensive approach involving government, industry, and civil society. Collaboration among these stakeholders can foster a digital environment that prioritizes privacy, while encouraging innovation and economic growth.

Ali Delghanthana is an academic-entrepreneur in cybersecurity, a Canada Research Chair in Cybersecurity and Threat Intelligence, and an associate professor in Cybersecurity at the University of Guelph. He is also the director of a research lab dedicated to advance research and training in cybersecurity. He is the director and founder of the Master of Cybersecurity and Threat Intelligence Program at the University of Guelph.

The Hill Times
The ground rules for the industrial adoption of AI

The government is co-ordinating programs and policies to ensure that AI is developed safely and responsibly in Canada for Canadians.

Artificial Intelligence is one of the greatest technological transformations of our age, impacting citizens and businesses alike. Around the world, billions of dollars are being spent yearly on AI research and development. As more and more AI applications come online in virtually every field of business and industry, Canada is well-positioned to be a leader in AI commercialization. We rank third among Group of Seven nations on the Stanford Global AI Vibrancy Index, and fourth in the world for the impact of our AI publications. Montreal has the highest concentration of researchers and students of deep learning in the world, and Toronto-Waterloo has the highest concentration of AI startups.

All this has not come about by chance: Canada was the first in the world to launch a funded national AI strategy. The Pan-Canadian Artificial Intelligence Strategy is helping Canada maintain a globally competitive position in AI research, and supporting commercialization and adoption. The Government of Canada also supports basic and applied research in AI, and has made targeted investments in both large and smaller companies—including major investments through our five Global Innovation Clusters.

The government encourages firms interested in exploring AI to educate themselves on the technology, from the executive to the implementation teams. They should begin with small experiments, such as pilots and proof-of-concept projects that allow lessons to be learned without jeopardizing company business activities. It is critical to ensure the fundamentals are present; indeed, without skilled personnel, robust infrastructure and well-managed data, adopting AI will be impossible.

Companies should also ensure suitable processes for privacy and consent; assess data sources and models from the perspective of diversity, non-discrimination and fairness; prioritize societal and environmental well-being; and take accountability for system outputs and outcomes. As we have done at the federal level, it’s a good idea for companies to develop an overall corporate strategy for AI, including goals for the use of the technology, a plan to implement it, and a definition of success.

For example, AI is being used throughout the insurance industry to deliver operating efficiencies and improved services to customers and brokers. As in other industries, Robotic Process Automation and data extraction are being used to perform tasks previously handled by human agents, such as submission intake. More complex actions such as underwriting, inspections and damage analysis are often now either informed or carried out by trained AI models. Automation of processes can reduce completion time, human error and costs. For example, Intact Insurance recently announced a partnership with the Université de Laval to leverage AI in the underwriting process, including to optimize the way they assess risks.

Scale AI, one of Canada’s five Global Innovation Clusters, is supporting our AI ecosystem by encouraging and funding AI projects with hundreds of organizations collaborating to invest in innovation. Scale AI aims to establish Canada as a global hub for AI dedicated to business productivity and intelligent supply chains. From working with Canadian ports to optimize their operations to incorporating AI into large food processors to AI-based demand forecasting for grocers, projects funded through Scale AI are already revolutionizing the way our nation’s companies do business.

As this transformative technology continues to affect more and more aspects of modern life, the Government of Canada is committed to working with industry and other stakeholders to guide commercialization. We will continue to ensure that the development and use of AI is governed by clear rules in a manner that aligns with Canadian values like respect for human rights, inclusion, diversity, innovation and economic growth.

Liberal MP Andy Fillmore, who represents Halifax, N.S., is parliamentary secretary to the minister of innovation, science, and industry. First elected in 2015, he has held numerous roles in government including parliamentary secretary for Canadian heritage, for democratic institutions, and for infrastructure and communities. He also served as chair of the House Indigenous Affairs Committee. Before politics, Fillmore spent 20 years as a city planner and community builder in the private, public, and academic sectors, including Halifax’s first-ever manager of urban design. He attended Acadia University and holds graduate degrees from Harvard University and Dalhousie University. He lives in Halifax with his family.
Necessary but not enough: Canada’s proposed new private-sector privacy law

Teresa Scassa
Opinion

Bill C-27, currently before Parliament, promises to modernize Canada’s private sector data protection law with a new Consumer Privacy Protection Act (CPPA). Yet even this title relies on an outdated privacy paradigm. Individuals will be treated as “consumers,” when, through the ceaseless and inevitable collection of their data, they are the co-producers.

Canada’s current law—the Personal Information Protection and Electronic Documents Act (PIPEDA)—dates back to the early 2000s when individual control over personal data dovetailed nicely with a concept of privacy as a right to assume sovereignty over one’s data. Over time, companies collected personal data primarily to provide goods or services, and data protection obligations sought to ensure that individuals understood why their data was being collected, and how it would be used. The law required organizations to limit collection to what was necessary, obliged them to ensure the information they used was accurate, and required them to protect the personal data they collected.

However, advances in technology and changes in business models have dramatically altered the importance of data and how value is extracted from it. Data analytics derive insights from personal data that drive targeted advertising and profiling. Data now also fuel the burgeoning artificial intelligence (AI) industry; personal data are used in the development of technologies that can employ predictive systems, and so much more. Personal data has become a valuable commodity: it is mined, extracted, traded, sold, and repurposed in ways that we—the data sources—struggle to comprehend.

PIPEDA was not designed for this context. Limiting collection will no longer suffice when more data means more innovation. Consent is a grim fiction when data collection is ubiquitous and continuous. We often have no choice but to use data-hungry digital technologies to work, to be educated, to transact, to drive our cars, to listen to music, read, or watch television. Worse, some companies consider that what people post on the internet is fair game. Clearview AI scraped photographs from social media sites to build its powerful facial recognition service.

Transparency and documentation obligations—though required for a secure and better functioning democracy and to limit collection to what was necessary, obliged them to ensure the information they used was accurate, and required them to protect the personal data they collected.

But in our question for digital security, our toolkit needs more. We must empower workers who are familiar with the technical reality and design choices, and those at the decision table. We also need to provide worker protection, and instituting effective policies would facilitate investigations and collaboration between public and private sectors.

Bill C-27 should be redrafted and budget to lead such investigations and collaboration between public and private sectors. When whistleblowers have unraveled numerous technological scandals, asserting the essential role of disclosing security breaches, surveillance, and backdoors in protecting our digital security. Whistleblowers have preempted or exposed a range of social wrongdoings, encompassing political, social, financial, technological, and health fields. Extensive research demonstrates that whistleblowers are carriers of the foremost means of detecting misconduct in both public and private sectors.

Canada demonstrates a marked deficiency in robust whistleblower protection—both in its public and private sectors. Even existing frameworks tend to be exceedingly restrictive in determining who gets protected, what type of disclosure is safeguarded, and to whom. It leaves those who risk a lot to alert authorities and the public largely vulnerable.

Our lives are now governed by algorithms. While AI promises considerable benefits, recent developments and obscure algorithms have raised multiple legal, political, and ethical issues, including data sovereignty, fundamental rights, and the protection of those brave enough to disclose these issues. Canadians are in the dark about algorithm-led decision-making, and very concerned by how their data is used, shared, and beyond their wildest expectations—including by their governments.

Bill C-27’s proposed implementation is currently plagued by a troubling lack of transparency, oversight, and accountability. Years of regulatory inaction have fostered a sociotechnical environment where algorithms are shaped by technologists’ choices instead of society’s collective will and needs. Meanwhile, the digitalization of our culture and deployment of private AI systems across society have shifted power to new structures that lie beyond existing governance and accountability frameworks. These new “governors” bring concerns for democracy and its future transparency.

The failure of their internal governance models, infrastructural vulnerabilities, and critical information systems, and inaction with respect to anti-competitive behaviours that created a digital ecosystem governed by a handful of major players.

Whistleblowers and former employees unveled massive evidence of state and corporate surveillance, and of deliberate malice and harmful choices that have negatively impacted society. These shortcomings have amplified risks to priority marginalized communities.

After years of inaction, Canada is finally considering updating its legal framework, notably with Bill C-27, recasting the private sector data protection framework. Yet, those legislative developments focus on transparency and documentation obligations. This may help with the ongoing opacity and foster some sort of oversight.

In our question for digital security, our toolkit needs more. We must empower workers who are familiar with the technical reality and design choices, and those at the decision table. We also need to provide worker protection, and instituting effective policies would facilitate investigations and collaboration between public and private sectors.

But in our question for digital security, our toolkit needs more. We must empower workers who are familiar with the technical reality and design choices, and those at the decision table. We also need to provide worker protection, and instituting effective policies would facilitate investigations and collaboration between public and private sectors.

Canada demonstrates a marked deficiency in robust whistleblower protection—both in its public and private sectors. Even existing frameworks tend to be exceedingly restrictive in determining who gets protected, what type of disclosure is safeguarded, and to whom. It leaves those who risk a lot to alert authorities and the public largely vulnerable.

Certainly, striking a fair balance between public disclosures and the safeguarding of trade and state secrets is essential. Yet, the public interest should trump the financial or political interests of the privileged few.

Legal frameworks must evolve to protect public safety over perpetuating power imbalances. This also requires intersectionality and to whom. It leaves those who risk a lot to alert authorities and the public largely vulnerable.

As digital systems increasingly shape our collective existence, influencing vital aspects of our lives and the very essence of our democracy, the protection of whistleblowers and security researchers becomes imperative and increasingly needed. It is required for a secure and better digital future.

Florian Martin-Bartheau is a fellow of the Bakhim Klein Center for Internet and Society at the University of Ottawa and an associate professor of law and the University Research Chair in Technology and Society at the University of Ottawa.

Teresa Scassa is the University Research Chair in Artificial Intelligence and Data Act and the Canada Research Chair in Privacy and Public Policy, and Professor of Law at the University of Ottawa. Her research is in the area of privacy law, data governance, and artificial intelligence.

The Hill Times

Policy Briefing Digital Security

Canadians digital safety cars for strong whistleblower and security researcher protection

Florian Martin-Bartheau
Opinion

Bill C-27, currently before Parliament, promises to modernize Canada’s private sector data protection law with a new Consumer Privacy Protection Act (CPPA). Yet even this title relies on an outdated privacy paradigm. Individuals will be treated as “consumers,” when, through the ceaseless and inevitable collection of their data, they are the co-producers.

Canada’s current law—the Personal Information Protection and Electronic Documents Act (PIPEDA)—dates back to the early 2000s when individual control over personal data dovetailed nicely with a concept of privacy as a right to assume sovereignty over one’s data. Over time, companies collected personal data primarily to provide goods or services, and data protection obligations sought to ensure that individuals understood why their data was being collected, and how it would be used. The law required organizations to limit collection to what was necessary, obliged them to ensure the information they used was accurate, and required them to protect the personal data they collected.

However, advances in technology and changes in business models have dramatically altered the importance of data and how value is extracted from it. Data analytics derive insights from personal data that drive targeted advertising and profiling. Data now also fuel the burgeoning artificial intelligence (AI) industry; personal data are used in the development of technologies that can employ predictive systems, and so much more. Personal data has become a valuable commodity: it is mined, extracted, traded, sold, and repurposed in ways that we—the data sources—struggle to comprehend.

PIPEDA was not designed for this context. Limiting collection will no longer suffice when more data means more innovation. Consent is a grim fiction when data collection is ubiquitous and continuous. We often have no choice but to use data-hungry digital technologies to work, to be educated, to transact, to drive our cars, to listen to music, read, or watch television. Worse, some companies consider that what people post on the internet is fair game. Clearview AI scraped photographs from social media sites to build its powerful facial recognition service.

Transparency and documentation obligations—though required for a secure and better functioning democracy and to limit collection to what was necessary, obliged them to ensure the information they used was accurate, and required them to protect the personal data they collected. The failure of their internal governance models, infrastructural vulnerabilities, and critical information systems, and inaction with respect to anti-competitive behaviours that created a digital ecosystem governed by a handful of major players.

Whistleblowers and former employees unveled massive evidence of state and corporate surveillance, and of deliberate malice and harmful choices that have negatively impacted society. These shortcomings have amplified risks to priority marginalized communities.

After years of inaction, Canada is finally considering updating its legal framework, notably with Bill C-27, recasting the private sector data protection framework. Yet, those legislative developments focus on transparency and documentation obligations. This may help with the ongoing opacity and foster some sort of oversight.

But in our question for digital security, our toolkit needs more. We must empower workers who are familiar with the technical reality and design choices, and those at the decision table. We also need to provide worker protection, and instituting effective policies would facilitate investigations and collaboration between public and private sectors.

Canada demonstrates a marked deficiency in robust whistleblower protection—both in its public and private sectors. Even existing frameworks tend to be exceedingly restrictive in determining who gets protected, what type of disclosure is safeguarded, and to whom. It leaves those who risk a lot to alert authorities and the public largely vulnerable.

Certainly, striking a fair balance between public disclosures and the safeguarding of trade and state secrets is essential. Yet, the public interest should trump the financial or political interests of the privileged few.

Legal frameworks must evolve to protect public safety over perpetuating power imbalances. This also requires intersectionality and to whom. It leaves those who risk a lot to alert authorities and the public largely vulnerable.

As digital systems increasingly shape our collective existence, influencing vital aspects of our lives and the very essence of our democracy, the protection of whistleblowers and security researchers becomes imperative and increasingly needed. It is required for a secure and better digital future.

Florian Martin-Bartheau is a fellow of the Bakhim Klein Center for Internet and Society at the University of Ottawa and an associate professor of law and the University Research Chair in Technology and Society at the University of Ottawa.

Teresa Scassa is the Canada Research Chair in Privacy and Public Policy, and Professor of Law at the University of Ottawa. Her research is in the area of privacy law, data governance, and artificial intelligence.

The Hill Times
Digital Security Policy Briefing

Canada's AI bill needs to catch up to get ahead of the curve

Daniel Konikoff

Cybersecurity needs faster, seamless public-private collaboration, say cyber experts

Canada's Digital Charter Implementation Act—necessary first step to regulating AI, but ahead of the curve it is not: it is empty legislation in search of substance. What little substance it does have relegates fundamental human rights as secondary to corporate and commercial interests, when it should be doing the opposite.

Regulating AI is a pressing policy issue, and jurisdictions around the world are rising to meet the moment. Last month, after two years in development, the European Union passed a draft of the AI Act. Late in 2022, the United States published a Blueprint for an AI Bill of Rights that while not legislation, provides guidance and a roadmap for America's responsible use of AI. What the EU's AI Act and the White House's Blueprint have in common is their focus on civil and human rights, and the consequences that unregulated AI can have on people. If Canada is to get ahead of anything, its AI bill first needs to catch up, finding a way to prioritize the public over the private.

One of the ways AIDA downplays civil and human rights in the AI Act by characterizing the harms it characterizes as "harm." AIDA defines harm as "(a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual." This neglects group- or society-based harms, like AI's role in violating Canadians' privacy. Privacy is important to Canadians: according to a June poll by the Office of the Privacy Commissioner of Canada, 93 per cent of Canadians expressed some level of concern about the protection of their privacy. Without codifying privacy as a constitutional right worthy of respect and priority, there is little in AIDA to protect people from AI-driven privacy harms like data breaches or mass surveillance.

AIDA's definition of harm also fails to capture the serious concerns experts have about AI being discriminatory. AI often expresses social biases, as we have seen through automated decision-making that discriminates based on race, gender, or socioeconomic status. AIDA's definition of bias even includes an exception that asks whether an AI-driven decision "systematically and adversely differentiates, directly or indirectly" towards a person based on prohibited grounds of discrimination has adequate "justification." This is inexusable; not only does AIDA not define what type of bias they regard as justified, but the government shouldn't be giving private enterprises that use AI a "Get Out of Discrimination Free" card.

Parliament needs to understand that privacy violations and biased decisions are harmful to rights and freedoms, even if they don't fit within AIDA's idea of harm as something that "publicly" hurts your body, mind, or wallet. Bill C-27 acknowledges the importance of human rights and fundamental freedoms in its preamble, but does little to turn that acknowledgment into responsible legislation.

With Bill C-27 going to the House of Commons, the Privacy, Immigration and Official Languages Committee in the fall, MPs and committee members have the summer to think about how they can better modernize our approach to governing AI. They should start by recognizing the risks AI poses for civil and human rights—something that the Canadian Civil Liberties Association has expressed in our open petition for a more rights-based AI legislation, and as part of our work with the Right2Your Face coalition on regulating facial recognition technology.

In the meantime, Canada can take some leadership from our neighbours to the south, whose Blueprint for an AI Bill of Rights lays out, in strong terms, that AI innovation "must not come at the price of civil rights or democratic values." Canada can also look across the Atlantic to the EU's AI Act, which outright bans intrusive and discriminatory AI systems like real-time biometric identification systems, on grounds that they violate human rights and the right to privacy. It's no surprise that the innovation minister thinks Canada's AI regime is ahead of the curve on innovation and industry, but is Canada's behind the curve where it really counts.

Daniel Konikoff is the interim director of the Canadian Civil Liberties Association's Privacy, Technology and Surveillance Program. He is also a PhD candidate at the University of Toronto's Centre for Criminology and Sociolegal Studies, where he is completing his dissertation on the governance of police technology.

The Hill Times