

CHECK AGAINST DELIVERY

SPEECH TO **3RD ANNUAL VANCOUVER INTERNATIONAL SECURITY** **SUMMIT** **October 29, 2026**

Michael Harvey
Information and Privacy Commissioner for British Columbia

Good morning, everyone.

It's an honour to be here on the territories of the xʷməθkʷəy̓əm (Musqueam), Skwxwú7mesh (Squamish), and Səlilwətaʔ/Selilwitulh (Tsleil-Waututh) First Nations.

I am privileged to be able to live in this beautiful province with my family, surrounded by nature which reminds me to always reflect on how that comes with both privilege and responsibility, to the land itself, to the people that have lived here, and to the people that live here now.

As an Officer of the British Columbia Legislature, I also acknowledge that I am privileged to work with people across many traditional Indigenous territories, covering all regions of our province. This privilege comes with a responsibility to seek every opportunity to advance goals of truth and reconciliation as I conduct my legislative mandates and, as a Canadian, as I live my life.

I would like to thank Greg Spievak, Christine Barry and the rest of the Reboot team for inviting me to join you here today.

...

The themes of this year's summit are urgent given where we find ourselves at this moment – as a province, as a country, and as individuals trying to find our footing during a time of both massive upheaval in the international order, and generation-defining technological change.

We're contending with the promise of artificial intelligence and other emerging technologies and the significant threats these developments pose to our ability to protect our privacy and have control over our personal information.

I know many of you in this room deal with these threats every day.

Last June, the [Canadian Centre for Cyber Security](#) noted that AI is "already lowering the barrier for entry for malicious activity", making phishing, voice scams, and deepfake impersonation more convincing and scalable.

A [KPMG survey](#) from March likewise found that 81% of Canadian companies surveyed had experienced attempted or successful AI-powered fraud, and over the past 12 months, 72% had lost money to it – up to 5% of business profits.

The question becomes how we can emerge from this period stronger, more resilient, and in greater control of our destinies – both in terms of the collective, as British Columbians and Canadians, and as individuals.

That's a big question and I believe that to answer it we must look to the values that we cherish, here in British Columbia and throughout Canada.

Those values can gain clarity and definition when we look at what we don't want for our country, but our strength, resilience, and our sovereignty cannot be sustained by negative comparisons.

We need to act with intention to choose the future we want, not to settle for what seems inevitable.

Today, I'm going to talk about that future through the perspective of how we treat our personal information – how those choices have profound implications for all of us as individuals, and, collectively, for our sovereignty as a nation.

And how the foundation for that future is built on trust.

...

Personal information is no longer a side conversation when it comes to our sovereignty because of how central data is to the lives of so many of us in the Information Age.

Our personal information is not "about us" *it is us* – it's what we're thinking about and want to share with someone, it's the places we're going, the things we're buying, even our health.

Control over that data means control over an essential part of who we are – our stories – what gives us agency in the Information Age.

Too often, we feel that control slipping away.

Our personal information becomes fodder for complex systems that seem beyond our reach or even our comprehension.

Our data is scraped, processed, and monetized, often without our consent or even our knowledge.

We may not know the exact machinations of how this is happening, but we can feel that it is, and that there's nothing we can do about it – that this is the price of admission for innovation in the Information Age.

But think of what gets lost when we acquiesce to that.

We're not only surrendering our individual privacy, we're giving up our autonomy.

When you consider that on a wider scale, that has profound implications for our sovereignty as a nation.

Five years ago, conversations about data sovereignty were mostly about data residency – where the servers were physically located.

Then we began to talk about the data in transmission – where our data went as it was processed from one server to another, or to the end user.

Then we looked at implications of foreign laws on Canadian soil – such as the US Cloud Act under which even Canadian data stored on servers in Canada could be subject to US legal processes if the company holding it falls under US jurisdiction.

When we recognize that there is no longer any meaningful distinction between our online and offline selves, old demarcations fall away, and the conversation turns to more foundational issues.

How we treat our data is how we treat our people.

In the Information Age, data sovereignty *is* sovereignty.

Of course, sovereignty is not an absolute – states operate in the real world, are bound by agreed-upon rules, international law, and the context of our times.

Absolute data sovereignty, likewise, isn't realistic, and the focus shouldn't be on isolating ourselves or sealing our data behind our borders.

We need to think more broadly and take a life cycle approach to data sovereignty.

It's not only where data is stored or where it travels.

It's about equipping people with digital skills, nurturing homegrown talent, and building Canadian industries that can shape – not just navigate – the Information Age.

It's protecting the individual and collective capacity of Canadians to have agency over their data.

Seen this way, data sovereignty provides us with a lens that we can use to take a risk-based approach.

At each stage of the life cycle, we can ask: what is important to us? What do we value? What is sensitive enough that it demands tighter controls? What is off limits?

This approach can guide how we handle different types of information and how we deal with other companies and other countries.

That's important because the rules we set around the collection, use and disclosure of personal information – the norms we let take hold now – will help shape our future as a country.

I think we can do better than we are now in building that future, and that the work before us starts with repairing the fractured trust we're seeing across society.

...

Last year, the Edelman Trust Barometer, one of the world's largest annual surveys on trust – found a deepening crisis of trust in Canada, with 67% of people saying they believed their leaders were deliberately misleading them.

This year's Edelman survey found that we're not just distrusting our institutions, but each other: 73% of Canadians say they're hesitant or unwilling to trust someone who holds different values, relies on different sources of information or comes from a different background.

In this environment, it's not surprising that people are also wary of sharing their personal information.

A recent survey commissioned by the Office of the Privacy Commissioner for Canada found that three-quarters of people are now less willing to share their personal information with organizations than they were five years ago:

- 78% have outright refused to hand over their information.
- 52% have deleted an account entirely because of privacy concerns
- 41% have walked away from a company after it suffered a breach.

An Angus Reid poll in July found that two-thirds of Canadians view AI negatively or critically.

Almost nobody surveyed – 1% – called it “very” trustworthy.

...

How do we rebuild trust?

That's the focus of much of the work my office does every day.

Our strategic plan, released last year, was titled “Trust in the Age of Information” and building trust is the throughline for our strategic priorities: Trust and transparency, trusted innovation, and enhancing rights equity.

These priorities were shaped by what people across British Columbia told us mattered to them in provincewide consultations.

They speak to the trust crisis we're facing today and the urgency of addressing it.

It's urgent because of what's at stake if we don't address it: who we are as a province, as a country, and the strength of our sovereignty.

I mentioned before the importance of defining our values, of what matters to us, and holding those close.

In Canada, our sovereignty is not achieved by coercion, force or fear of the state.

Instead, we have a form of democratic sovereignty that is strong and resilient because it's rooted in fundamentally different values.

The core of that foundation is trust.

Our democracy survives – it thrives – based on how much trust people have in the organizations and institutions that are part of their everyday lives.

Right now, we have work to do to repair that fractured trust.

We can start by modernizing our privacy laws to today's challenges.

...

Our private sector privacy law, the *Personal Information Protection Act*, or PIPA, is based on the premise that an individual must consent to an organization's collection, use or disclosure of their personal information.

Consent is a cornerstone of privacy laws around the world and a principle that we should uphold.

But in the Information Age, it's been warped beyond recognition.

Navigating consent today is like being dropped into a jetliner's cockpit with a thick technical manual and a control stick that may or may not be connected to anything.

These trappings of control create a false legitimacy for the use of our personal information.

When the controls are handed over, so too is the liability if something goes wrong, and any incentive a corporation may have to make things safer.

Our joint investigation into OpenAI, the makers of ChatGPT, with our federal and provincial counterparts, laid bare this fundamental disconnect between what our privacy laws demand, and how the world's most popular and widely used AI application works.

It highlighted how far we need to go to create an environment where trustworthy innovation in AI can thrive and it shows the extent of changes we need, both from innovators, and from our laws, to make that happen.

We assessed OpenAI's collection, use, and disclosure of personal information with ChatGPT against the privacy protections our legislation provides the people of our province.

What we found was that OpenAI contravened PIPA in all but one of the 13 issues we investigated.

To initially train ChatGPT, OpenAI scraped vast amounts of personal information from publicly accessible websites. This was widespread and indiscriminate, from social media, discussion forums, blog posts, news outlets, and more, whether from a child or an adult.

All of this publicly sourced information was obtained without any type of consent recognized under PIPA.

The OIPC is not anti-innovation. We recognize AI applications have potentially transformative benefits.

Our emerging information and privacy technologies team is exploring the potential for their use in our own work.

But in certain cases, such as this one, applications are developed without adequate privacy considerations.

Cases such as this also make it starkly apparent that our privacy laws were written for a different era and are strained to the breaking point.

Both companies *and* the law have to change.

After the release of the OpenAI report, I wrote to the Minister of Citizens' Services urging the government to act without delay to modernize our legislation to respond to today's challenges.

This doesn't mean removing guardrails as this powerful technology races ahead.

Instead, it means putting the onus on organizations to earn the trust of the people whose data they use.

We need to start with consent, but where that is neither feasible nor appropriate, we need other legal authorizations in PIPA that come with strong guardrails, robust independent oversight, and the burden for compliance on the people profiting from the use of peoples' data.

We need to have data governance requirements that scale with risk and, where the risk is high enough, outright limits on what can be done at all.

The goal is a British Columbia where companies innovate and compete on how to empower people with control over their own information, not on how to deprive them of their autonomy over their data and extract value from it.

The principal beneficiaries of the use of personal information must be the people to whom it belongs.

We need to make sure that AI works for us, not the other way around.

This is how we can lay the groundwork for trustworthy innovation, and how we repair trust – by looking to our values, and building from there.

...

At the federal level, Bill C-36, the Protecting Privacy and Consumer Data Act (PPCDA), contains many proposals to reform and modernize the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

While this is outside of my jurisdiction, it has significant implications here in British Columbia, that my team and I are monitoring.

Its introduction has started a long overdue conversation on how we can elevate the standard of privacy protection across Canada.

The Bill contains changes that a succession of BC Privacy Commissioners have long supported for our own *Personal Information Protection Act*.

It speaks to the consent issue I referred to – how we make consent make sense in the modern age.

To that end, it proposes new exceptions to consent for modern data handling practices.

It would also strengthen protections for sensitive personal information, including biometrics and children's information and would give individuals functional controls.

It would introduce new safeguards, like telling people when AI is making decisions about them, and new rights, such as the right to demand deletion of your data.

Stronger enforcement tools, including penalties for non-compliance, would serve as a practical check on power.

That bill is, understandably, centred on big tech and digital safety.

These issues are crucial; however, they form only part of the picture – for millions of Canadians, privacy concerns come up much closer to home.

...

The files that come before me at the OIPC reflect this.

The story of privacy shows up in residents' unease about cameras going up in their buildings, parks, schools and sidewalks.

In tenants' unease when landlords seek more personal information than necessary when housing is limited.

When non-profits maintain records about the people they support at a time when those organizations are a lifeline, or when politicians come knocking on doors at election time.

They extend to the fields, camps, worksites, and home offices where employees are monitored on the job.

Privacy needs to be understood in this context, in all of the levels where it resonates: families, communities, provincially and nationally.

And that need is why Canada has a strong tradition of independent privacy regulators embedded within local communities and delivering on the issues that matter most to people and their communities.

Empowering local regulators strengthens Canada's ability to adapt to the Information Age by staying responsive to the specific needs of our diverse country.

As independent regulators, we strive to rebalance power, to put it back in the hands of individuals and affirm that no single entity holds unchecked authority.

Through that work we give our economy, and the emerging technologies driving it, legitimacy and staying power – we reinforce trust.

...

We need rules that make sense for the situation we're in now – that respond to today's challenges and strengthen independent oversight.

But the challenges we're facing – the fractured trust at so many levels of our society – require more foundational solutions.

Organizations cannot just tick off compliance boxes.

An organization can follow every law on the books and still lose people's trust, if it acts irresponsibly.

That's where the concept of social licence comes in.

...

This is an idea that came from the environmental sector, but is useful when we talk about tech and innovation.

It refers to the trust and acceptance an organization or institution earns from the people it impacts, beyond whatever legal authority it holds.

That idea is important – that trust is not a one-off transaction, but that it must be continuously and deliberately earned.

It means that organizations must recognize that they are interdependent with society – that the more society flourishes, the more fertile ground a company has to flourish in.

Data driven innovation carries the greatest value when it's anchored in an identified need.

Innovation for its own sake drives a tendency to bend every problem to match the solution at hand.

Technology should serve humanity, not the other way around.

We see this in the framing of AI as a panacea to a wide range of issues, when it is one tool among many, suitable for some problems, not all.

How can organizations earn trust and build their social licence to operate in the Information Age?

There are some clear paths:

- **Purpose driven technology:** anchor innovation to an identified need
- **Human-centred design:** this approach prioritizes user wellbeing, effectiveness and accessibility through direct engagement with those impacted – have the people impacted in the room from the earliest stages.
- **Privacy by design** embeds privacy protections from the start of any program or initiative. Institutions using these approaches earn social licence because they act on their obligations toward people and their data.
- **Robust data governance:** Retention policies, limits on what you collect, controls on who can access, auditing procedures – this kind of due diligence demonstrates that a company is taking its responsibility to individuals' data seriously and honouring their control over their own personal information. Privacy protection is a core outcome, not merely a checkbox.

These are not limitations on innovation – they create the ground in which innovation can thrive, and, crucially, be trusted.

One-sided arrangements – where the focus is solely on seizing and exploiting value from individuals – are inherently unstable.

They're doomed to fail and the fallout is costly for everyone.

Organizations that find ways to empower individuals and extend the gains of innovation across society can build trust and encourage more people to participate in the Information Age.

It starts with putting human dignity at the centre and building from there.

...

Emerging technologies test us – they test our values, the kind of society we want.

We're seeing our values – and the laws in which those values are embedded – tested by technology in the courts, and in investigations conducted by my office and other regulators.

Perhaps the most prominent example of this is the discussion around what privacy means in public spaces.

Specifically, the idea that once a person is out in public – whether online or off – their personal information is up for grabs.

That idea is not only antithetical to our values as a free society, it's also been expressly rejected in our courts.

In *R v Jarvis* (2019), the Supreme Court of Canada found that despite being in a public place, high school students had an expectation of privacy to not be recorded by their teacher's pen camera.

The Court was unequivocal – holding that privacy is “not an all-or-nothing concept,” and that being in a public space “does not automatically negate all expectations of privacy with respect to observation or recording.”

Nor do we lose our privacy rights when we go online.

In the Supreme Court of Canada case, *R v Bykovets* (2024), police investigating online fraud obtained a suspect's IP address from a third-party payment processor without a warrant.

The Court said that an IP address can be the first thread that unravels someone's entire online life, so police need a court order to obtain it.

The Court affirmed the principle from the *Jarvis* ruling that privacy is not an all or nothing concept, and that our right to privacy doesn't disappear online.

...

This principle was affirmed in decisions from the BC Court of Appeal and the BC Supreme Court upholding our Order that followed our joint investigation into Clearview AI.

In a joint investigation with our counterparts in Alberta, Quebec, and the federal regulator, we found that Clearview AI, a facial recognition company that sold its services to law enforcement agencies, had scraped billions of images from the internet to feed their technology with no legal authorization to do so.

Millions of Canadians, children included, had their images scraped from social media accounts and other online sources.

Nobody consented to having photos they uploaded fed into what was essentially the world's largest police lineup.

My office's Order prohibited Clearview from offering its facial recognition services to clients in BC, to cease their collection use and disclosure of personal information from individuals in the province without their consent, and to delete what they've collected so far.

Clearview requested a judicial review of that Order.

The BC Supreme Court upheld the Order in 2024, and in February, the BC Court of Appeal reaffirmed that decision, dismissing Clearview's appeal and upholding the Order in full.

The tremendous potential of emerging technologies raises the question of not only what can we do with these wonderful tools, but what we *should* we do, how do those uses align with our laws, and with the values that unite us.

We need to consider technology in this light and reject the ethos of “move fast and break things” – because it is too often people – and their trust – that bear the brunt of the damage.

...

I'd like to pause before I close to recognize and commend the work that so many of you in this room do to protect personal information, and, by extension, so much more.

My office hears every day about the severity and scope of the challenges you're facing.

Cyberattacks were the single leading cause of private sector breaches reported to us last year – the cause of just under half of those reported.

Earlier I spoke about the lens that a risk-based approach to data sovereignty provides: deciding what's important to us and protecting that.

The decisions you make every day– on security safeguards, access control, data retention, among other concerns – are a part of that.

Those choices also help determine whether an organization builds or loses trust with the people it serves.

And trust is vital to the effectiveness of your work because the best technological solutions cannot be effective *unless people trust them*.

...

Trust runs through everything I've discussed today – our sovereignty, our laws and what they mean in the Information Age, the choices organizations make, the choices all of you make.

We're stronger – our country's sovereignty is stronger – when we stand on a foundation of trust:

- on institutions people believe in, and that they have meaningful recourse to challenge when they disagree with them;
- on innovations that excite, empower and inspire rather than confuse, obfuscate, and exploit.

The path we choose now will determine whether we can achieve the future we want, or whether we'll be left watching our personal autonomy and our collective sovereignty further erode as the bonds that hold us together fracture and fall away.

This is our moment to determine our destiny in the Information Age. To answer the question: Who do we want to be?

We don't need to accept what feels inevitable.

We're in a position to choose – our own path, on our own terms.

Thank you.