OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO
PUBLIC SECTOR NETWORK: GOVERNMENT INNOVATION SHOWCASE
December 2, 2025

Michael Harvey
Information and Privacy Commissioner for British Columbia

Thank you for that introduction, and good morning, everyone.

I'm Michael Harvey, the Information and Privacy Commissioner for British Columbia.

Before I begin my remarks, I would like to respectfully acknowledge the traditional territories of the Lekwungen people, of the Songhees and Esquimalt First Nations, where we gather today.

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.

I would like to thank the Public Sector Network for inviting me to speak to you today during what I believe is a critical time for all of us working for the people of this province.

We are in what I would suggest is a crucible moment for privacy.

Our personal information rights are under pressure from rapid advances in AI at a time of economic uncertainty, political polarization and a shifting world order.

All of us in the public sector are feeling the pressure to push innovation forward that will help us improve service delivery, to do more with less.

I support that. I believe that we can and should use technology to improve service delivery, and that includes artificial intelligence.

What I'm here to talk about today is how we get there – how we move forward with innovation while protecting the rights of the people we serve.

And privacy rights are front and centre.

That's because in the Digital Age, our data is no longer about us – **it is us**.

Nearly every aspect of how we live – from our social lives, to our education, healthcare, and our democratic participation – flows from our personal information.

Our personal information is central to our identities and controlling it means controlling how we participate in society – how we live our lives.

This is what gives us autonomy and dignity as free individuals in a democracy

The choices we make today will determine whether we emerge from this crucible moment with that autonomy intact.

A rights-first approach to innovation means finding solutions that work for people, that uphold their rights, their autonomy.

It's an approach that builds trust – and innovations in the public sector cannot succeed if people don't trust them.

….

Right now, we're facing a trust crisis.

The 2025 Edelman Trust Barometer Canada Report showed that 67% of Canadians believed government leaders mislead the public.

StatsCan research shows that only 24% of British Columbians have high confidence across major institutions – police, justice systems, schools, parliament and media – and that's below the national average.

My office's own file numbers tell a similar story. Comparing the most recent reporting year to the year previous, we noted:

- A more than 30% increase in the number of people reporting that public bodies failed to respond to FOI requests within legislated timelines.
- A 13% increase in people asking us to review public bodies' FOI decisions that they disagreed with.
- A 25% increase in the number of privacy complaints across the public and private sectors.

….

These numbers tell me that people are losing faith in the institutions and organizations that are part of their lives – that people don't think public bodies are being transparent, and that they feel their privacy is under threat.

Our personal information is our identity and the more control people have over their own information, the more empowered they feel.

The reverse is also true.

Our Information Society is shaped by powerful centripetal forces – forces that pull that power away from individuals and draw it inward toward systems, platforms, and algorithms.

Our information is collected constantly, often without our knowledge or consent, and used in ways we shouldn't be expected to understand to predict and shape our behaviors in the private sector and to determine the availability of services in the public sector.

Each time this happens, our sense of autonomy diminishes by degrees that may seem imperceptible at first, but cumulatively they lead to people feeling like they're losing their footing in society and in their democracy.

When that happens, trust breaks down – among people and between people and the institutions and organizations that serve them.

….

AI systems can accelerate this downward spiral.

They come with an added layer of opacity – they might be a black box even to the people who created them.

If they're inscrutable to their creators, where does that leave people whose lives could be shaped by decisions made by these algorithms?

What happens to trust when people can't understand why they lost out on a job, why their loan application was rejected, or why their benefits were denied?

And what happens when people don't even know that an algorithm was used to make such an important decision about them?

Right now, there's no requirement – in either our private or public sector privacy laws – to notify people when they've been subject to an automated decision-making system.

That needs to change.

When members of the public don't even have the basic ability to know if an algorithm was used to make a decision about them – *let alone the ability to challenge that decision* – we cannot expect them to embrace and trust the use of these technologies.

As it stands, our laws require neither transparency nor accountability.

We recommend that FIPPA be amended to include this provision as part of a thoughtful and comprehensive approach to the regulation of AI in the public sector.

….

Trust suffers in these cases and people can be left with privacy fatigue.

A feeling of malaise – of throwing hands up in the face of endless complexity – sets in.

I think everyone of us in this room can do something to address that malaise.

And it starts by flipping the script.

Not by trying to find where we fit into and adapt to the Information Society, but by asking how we build an Information Society that works for us – one where we can enjoy the benefits of innovation, without sacrificing our autonomy.

We do that by creating countervailing forces that push power back out to individuals.

Strong, effective and independent oversight is one such force.

Another is transparent, independent and inclusive governance within organizations and institutions backed by legislation that puts strong guardrails in place.

I'd like to talk first about oversight.

Now there are many systems at work in our democracy that serve this purpose, including an independent effective judiciary, regulatory bodies, a free press, and more.

What I'd like to talk about is where my office fits into the democratic framework of this province, and that's as an independent office of the legislature.

While the factors we face today are unique, we can trace the struggle against forces that centralize power back to the signing of the Magna Carta.

My office and other independent officers, including the Ombudsperson, Auditor General, Human Rights Commissioner and Chief Electoral Officer, serve as countervailing forces to that centralization of power.

We push power back to the people.

We provide independent oversight of the laws we enforce – we're often called "watchdog" agencies – and we give people recourse when their rights under those laws are violated.

By promoting transparency and accountability in government operations, we build trust.

Indeed, we are stewards of trust in our data-driven democracy.

….

What does that look like in the era of artificial intelligence?

AI poses fundamental questions for the work all of us do.

In the public sector, AI and automated decision-making processes have the potential to transform service delivery – from healthcare to environmental protection, education to social services.

But these potential advances come with risks to our rights.

From my perspective, I see the challenges it poses to fundamental privacy principles:

- Data minimization: The idea that you should only collect what you need for a specific purpose. AI systems require massive amounts of data to function – the more the better.
- Purpose limitation: Information collected for one purpose shouldn't' be used for another without authorization. AI systems might use data for training, or other uses.
- Transparency vs. opacity: People should understand how decisions that impact them are made. AI systems may not be explainable.
    - And again our laws don't even require that public bodies or organizations let someone know when they've been subject to an automated decision-making system. This is a requirement elsewhere, including in the private sector in Quebec.

These are profound challenges, but they're not insurmountable and they don't mean that AI solutions should be off the table, or that AI is ungovernable in the public context.

Rather it means that we must reflect on and improve our governance approach and make sure that the legislative safeguards we have in place are up to the task.

….

AI Is advancing rapidly – far faster than our legislative processes move.

While our public and private sector privacy and access laws are based on fundamentally sound privacy principles, they do not lay out the explicit safeguards we need in the age of artificial intelligence.

What could those safeguards look like?

It's part of the mandate of my office to offer public comment on emerging technologies that have a direct impact on the privacy rights of people in this province.

I would like to highlight two sets of recommendations around the use of artificial intelligence that my office has offered.

In 2021, my office, along with the Ombudsperson of BC and the Ombudsman and Information and Privacy Commissioner of the Yukon released our report, "Getting Ahead of the Curve: meeting the challenges to privacy and fairness arising from the use of AI in the public sector."

The recommendations remain valid today, and include:

- **Human oversight:** Clearly identifying who in a public body is responsible for engineering, maintaining, and overseeing the design, operation, testing and updating of any automated decision system.
- **Making systems explainable:** If AI systems make decisions about individuals, authorities must notify the individual and describe how that system operates in a way that's understandable.
- **Data minimization:** Organizations should use anonymized, synthetic, or de-identified data rather than personal information where the latter is not required to fulfill the identified appropriate purpose.
- **Challenge mechanisms:** Individuals must have an effective means to challenge any administrative decision, should be able to understand how that decision was made, and have access to review by a person.

I'd also suggest limitations to prevent function creep - Information collected for one purpose should not be repurposed without appropriate authorization.

We're also missing a clear requirement for public bodies to correct people's personal information when they're requested to do so.

Right now, under FIPPA, public bodies are only required to make a note that they've received the request.

We've called for this amendment previously and the need is more urgent now as automated decision-making systems could make decisions that impact people's lives based on inaccurate information about them.

In 2023, my office joined other Federal, Provincial and Territorial (FPT) Information and Privacy Commissioners to provide recommendations around the use of AI, with special consideration for vulnerable groups.

The recommendations included:

- **Rigorous bias testing** to ensure systems do not disadvantage these groups.
- **Enhanced oversight** when vulnerable groups are impacted.
- **Extra care for children** who face a higher risk of negative impacts from AI
- **Extra caution in sensitive domains** like healthcare, education, policing, criminal justice, housing and finance.
- **Consideration of Indigenous peoples'** perspectives on data sovereignty.

These principles don't require that you be able to explain or even understand every technical detail of an AI system – they're about creating clear accountability frameworks, and providing human oversight and meaningful recourse for people.

….

These are specific considerations for AI but they speak to a broader approach that can apply to any innovation in the public sector.

It goes back to the question I asked: How do we build an Information Society that works for us?

It starts with taking control back – specifically empowering people to take back control of their personal information – and that means putting rights first.

People need to be empowered by controlling their personal information, knowing how it's being used and for what purpose, and how it's protected.

We are serving people who have rights embedded in laws, including rights to privacy. Services offered by the public sector do not exist apart from these rights. They're two parts of the same whole.

….

So what does a rights-first approach look like in practice?

That's where privacy by design comes in.

Privacy by design means embedding privacy considerations from the very start of any project or initiative.

It means asking questions around data collection – how much of it do you need, can you achieve your goal with less, how long are you going to hold on to that information, how are you going to protect it, what about the vendors who will be handling the data? How will people know what you're collecting, and why?

If you're using automated systems to make decisions about people, can you explain how those decisions are made and how humans are part of that loop?

Privacy by design is about thinking ahead – anticipating privacy issues before they happen.

Ultimately, it's about building the kind of trust that is needed for any innovation in the public sector to be viable.

….

Privacy impact assessments are a practical tool that you can use to put privacy by design into action.

PIAs are legally required under FIPPA for any new initiative or significant change to an existing information system.

When you're facing demands for service and have an exciting innovation that you want to get out the door to help people, PIAs may feel like they're slowing you down.

Here's the thing: If you approach PIAs as an inconvenience at the END of a process – when contracts are signed, decisions made – then they may well be inconvenient and potentially costly as you seek to rectify problems.

But if you do the PIA early, it will help you make better decisions and embed privacy rights at the earliest stages of your project.

You'll benefit from asking the hard questions up front.

And the most important one might be the simplest: Do we even need this technology to begin with or would a simpler approach achieve the same goal.

This requires some effort up front, but when you think of all the consequences of what could happen if you *don't* do this work – privacy breaches, media scrutiny, and the risk of losing people's trust – it's an investment worth making.

My office is here to help.

We regularly consult with public bodies on their PIAs.

We do not approve or reject them. We offer our expertise and advice on how you can build solutions that people will trust.

I'd like to note here that more needs to be done to make sure that public bodies have the tools to properly assess initiatives that involve algorithmic tools.

Our 2021 joint report with the Ombudsperson of BC and Yukon colleagues on AI use in the public sector recommended the development of Artificial Intelligence Fairness and Privacy Impact Assessments - or AIFPIAs.

These would consider *both* the privacy and fairness implications of initiatives that plan to use algorithmic tools.

Right now, these are not a requirement under FIPPA and the tools available to public bodies to thoroughly gauge and understand the potential impact of algorithmic tools on people's rights are limited.

We will continue to advocate for our legislation to be amended to address these concerns, and are committed to developing our own resources and capacity to help public bodies address these issues.

….

I'd like to close by reflecting again on the moment we find ourselves in.

I talked about the crucible moment for privacy and the stakes we're dealing with here.

All of us who serve the public –front-line staff, policy-makers, and regulators – need to think deeply about how whatever innovation we're considering impacts the fundamental rights that make this province a wonderful place to live.

Because our rights are precious, and they are vulnerable to the pressures of the moment we face today.

Privacy isn't about hiding what you don't want to share with other people.

It's about controlling what we do share. It's about expressing who we are.

As people lose control over their personal information, they lose control over their own stories, their own lives.

But I'm optimistic that we can emerge from this crucible moment stronger. That's because of those of you with us here today and the thousands of public servants across this province who are committed to getting this right.

We have the opportunity now to build the Information Society we want through strong independent oversight and transparent, independent and inclusive governance, with legislation that puts the guardrails we need in place.

Will we build an Information Society that serves technology or one where technology serves us?

The answer lies in the decisions that all of us will make when we leave here.

We can start by focusing on the rights of the people we serve, and building from there.

Thank you for your time today.