OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO THE
SPEECH TO THE VICTORIA INTERNATIONAL PRIVACY AND SECURITY SUMMIT
March 13, 2025

Michael Harvey
Information and Privacy Commissioner for British Columbia

Thank you for that introduction.

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.

Thank you to Greg for inviting me to speak with you today about an issue that has become increasingly important to my way of thinking about privacy regulation, particularly in the era of AI. While it's hardly a new concept, it has gotten a bad rap lately in privacy circles. It's been recognized as something that is broken … something we need to get over.

I'm talking about consent.

But I'm not here to bury consent. I'm here to praise it.

I'm here to argue that consent remains at the heart of a rights-based approach to privacy protections in this country. I'm here to convince you that if the consent model has been broken, it does not mean that it should be abandoned… even if there are valid arguments that consent is not feasible for certain purposes, not appropriate for others and, in some instances, not fair to put on the shoulders of every individual. Rather, we should reinforce and supplement it.

I'm here to argue that in the Information Society, our personal information is our essence and the core of our unique identity. It is at the very heart of who we are as individuals.

When we have control over our own personal information, we are free, autonomous and dignified individuals who also collectively govern each other. Understood in this way, privacy is a fundamental right – and consent is always going to be a key way in which we exercise that right.

….

It's been hard times for consent lately, though.

Consent was missing when Clearview AI used data scraping to amass a database of more than three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, children, too.

In this joint investigation by my office, the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, and the Information Privacy Commissioner of Alberta, we looked at whether the company's collection, use and disclosure of the personal information by means of its facial recognition tool complied with federal and provincial private sector privacy laws. We found that it did not.

Last December, BC's Supreme Court affirmed our decision, confirming that privacy and consent are not dead in an online world, and organizations do not have the right to scrape our personal data just because it is available online.

Consent was also missing in other recent investigations we've carried out independently and with our fellow regulators across Canada

….

Cadillac Fairview had hidden cameras lodged in mall directories that collected and stored millions of shoppers' images without their knowledge or consent.

And four BC Canadian Tire stores captured detailed biometrics through facial recognition of anyone who entered the store, children included.

….

When people contact my office about issues like these or other everyday encounters with surveillance, they may not use the term "consent," but that's often what's at the heart of the matter.

They want to know what choice do I have? Can I opt out? Why do I have to accept my biometrics being taken – and stored – just to do some shopping?

It's about control of their personal information – control they can feel slipping away in all aspects of their lives – physical and digital.

And let's face it, there is no longer any meaningful distinction between the two. We don't need a Metaverse – we already live in one. Ours is a thoroughly digitized reality, and that's been ongoing for a generation now. We are, in effect, our own avatars.

And increasingly, we generate vast amounts of data in almost every aspect of our lives.

But the newer trend is that alongside that exponential growth in the supply of data is a similarly exponential growth in the demand for data.

New AI applications have an insatiable thirst for data to train their systems.

And I'm not just talking about new large language models, which are the most voracious of all. I'm talking about how the main approach to computer programming is transforming from being deterministic to being probabilistic.

We will move from programming based on "if x then y" to programming based on the odds. And to play the odds you need data.

I've recently been saying that in five years, AI will just be called "computer programming." And probabilistic computer programming for every use case is going to require huge amounts of data.

So where are companies going to get this data? Some of them will do as Clearview did – scrape for it without telling anyone or seeking anyone's consent.

Clearview was an extreme case – it reached into people's social media accounts, collected highly sensitive biometric data through their images, and sold it to law enforcement. It was easy to see how that was beyond the pale.

But other use cases are more nuanced. And some will argue that when we go about our daily business on the internet, we are basically in public, and the internet is our 21st century sidewalk. So if we happen to leave behind a trail of digital footsteps with those activities, and someone wants to collect that and make something of value out of it, what's the harm? What kind of reasonable expectation of privacy do we have in public, anyway?

Some of those same people will argue that putting barriers in place to their ability to collect and use information for this purpose stands in the way of enormous gains for productivity and innovation. They will argue that they need this data. And they will argue that because we need innovation to generate the economic growth, prosperity improvements, and service delivery enhancements that we expect, we need them to be

doing this, too.

But, and to paraphrase the Federal Court of Appeal's recent ruling on the Privacy Commissioner of Canada vs Facebook, we cannot talk about a company's needs and individual rights as if they are equivalent. Companies are limited by law in how they can harvest data. They cannot just scoop it up without legal authorization. The notion that we have no reasonable expectations of privacy in public is a dangerous idea that strikes at the very heart of our liberal democracy because it undermines our individuality.

And this brings me back to consent. The Federal Court of Appeal found in the favour of my federal colleague because of the primacy that consent plays in the federal statute, the *Personal Information Protection and Electronic Documents Act*, in the same way that it does here in British Columbia's *Personal Information Protection Act*.

But all those arguments are hard to dismiss out of hand. Because we do need innovation. And there is a lot of value in data that doesn't serve anyone if it goes unused. And the consent model is indeed in trouble.

So let's take a close look at the so-called shortcomings of consent.

In privacy circles, we often hear how the consent model is broken.

I'd like to shake up the structure of that sentence. I'd instead ask: who broke the consent model?

The consent model is broken not because of any inherent flaw, but because it has been weakened to the point where the principle is often meaningless in practice.

Consent, as it is currently implemented, is often not actually about consent at all but instead focuses on limiting legal liability for those collecting the information.

And privacy policies are more likely to serve as liability disclaimers for companies than any kind of guarantee of privacy for individuals.

We all know that these notices are long and repetitive, with text in small print. They describe situations of little concern to most consumers and then mix in things that are of concern. They also are changed all the time, often when you least expect it.

Users are expected to make complex risk assessments about their data, which is unrealistic.

And, with the ubiquity of smartphones and advent of Internet of Things, constrained interfaces on mobile screens and wearables make the privacy notices extremely difficult to read.

How can we keep our privacy rights in focus when we need a magnifying glass just to read a privacy policy?

We also know that organizations are using deceptive design practices to manipulate or coerce users into making decisions that may not be in their own best interests.

Earlier this year, my office and others released a report on these practices, as part of our work with the Global Privacy Enforcement Network, or GPEN.

This report found that almost all Canadian digital platforms used at least one deceptive design pattern. The study found a particularly high level of these patterns on platforms designed for children.

Let's look at a few examples of how deceptive practices work.

The first one I'd like to mention is the "take it or leave it" approach, where individuals are pressured to consent.

They either agree with the long privacy notice or choose to abandon the desired service. This naturally sets up a power imbalance between the user and the company.

When collecting consent, some companies also use misleading language, pre-checked boxes, hidden privacy settings, emotional pressure, nudging, and so on.

A simple example is a prompt that says, "Are you sure you want to exit?"

Research also tells us that even the presence of the term "privacy policy" can lead people to the false assumption that the company has placed substantive and responsible limits on how data is handled.

Then there's consent fatigue, caused by the requirement to make too many choices, sometimes several times in a day. In this scenario, the burden and responsibility of carrying out a risk analysis has been placed on the individual.

Finally, and we've all experienced this one, users are affected by the lack of any real alternative.

Big tech companies dominate digital services, meaning users cannot easily switch to a more privacy-friendly alternative. They often feel forced to accept privacy-invasive practices just to participate in modern life.

…
Many critics are vocal in their criticism of the consent model, saying that it cannot be fixed for several reasons.

One argument is that consent cannot be truly informed.

Here's the logic with this one.

The value of data resides not in its primary purposes but in its numerous secondary purposes, where data is re-used many times over.

Since these secondary uses are, by their nature, unanticipated, they are rarely evident at the time of collection, and it is impossible to provide any explicit details about how a given dataset will be used or how it might be aggregated in the future.

Another argument is that consent gives an illusion of a choice.

Critics say that with data collection occurring with every use of online services, and complex data sets being created, it is humanly impossible to exercise rational decision-making about the choice to allow someone to use our personal data.

They argue that the idea of a singular use of data for a specific pre-defined purpose, where the individual is duly informed and then makes a single choice, is no longer reflective of the complexity of the modern digital environment.

Critics also maintain that consent is not scalable… that the idea of individuals making a singular choice for each pre-defined purpose is outdated in the modern world.

Others say that the timeliness of consent collection is an issue. The fact that the consent needs to be given in real time before collection almost always results in disregarding what the privacy notices say, as consent often needs to be provided while the user is trying to access services.

In that context, users click through privacy notices, such as those required to access online applications and treat them as an impediment that must be crossed to get access to services.

And finally, some critics say that it's impossible to withdraw consent in the digital world.

They argue that opting out of data collection is not only impractical but, in some cases, impossible. As online connectivity becomes increasingly important to participation in modern life, the choice to withdraw completely is becoming less of a genuine choice.

So if not consent… then what?

Some argue that we should move away from consent.

Alternative models have been suggested to shift responsibility onto organizations rather than individuals. These models include data trusts, independent third-party organizations that manage data on behalf of individuals, making decisions about access and use, fiduciary duties, that would legally require companies to prioritize users' privacy over profit, and collective governance models that would oversee the fairness and accountability of data use.

Instead of each individual making privacy decisions, governance structures oversee the fairness and accountability of data use.

Others believe we should adopt a risk-based paradigm rather than individual control.

In this scenario, organizations would be responsible for minimizing the risk for individuals' privacy rather than asking individuals to make the risk assessment.

This approach would be framed by accountability measures, such as ethical standards and security measures, to safeguard the individual's rights.

….

The European Union's *General Data Protection Regulation* (GDPR), now almost eight years old, introduced six legal bases for data collection and utilization, allowing organizations to choose the one most appropriate to their particular processing activity.

Consent remains as one of those legal bases, but private organizations now often use the contractual necessity legal basis and the legitimate interest lawful basis.

The contractual necessity legal basis allows organisations to process personal data for the performance of a contract or to take steps at the request of the individual prior to entering into a contract.

The legitimate interest lawful basis can be used where an organization has a justifiable reason to use an individual's data, if this interest is balanced against the individual's privacy rights and does not significantly impact them.

In parallel, consent has been reinforced in the GDPR by adding or reinforcing requirements for valid consent.

Without doubt, the GDPR has transformed privacy discussions internationally and elevated the global standard. The strengthening of consent within the GDPR has also been beneficial far beyond the EU's borders.

I should also mention another key change that was introduced by GDPR. This change gave the regulator sharper teeth – I'm referring of course to major administrative monetary penalties that make companies sit up and take notice.

There are elements of a different approach emerging in Canada.

When Parliament was prorogued in January 2025, Bill C-27 died on the Order Paper. As this audience knows, C-27 would have reformed PIPEDA. It's not the first time federal privacy reforms have died. An earlier iteration, Bill C-11, suffered the same fate not four years earlier. But if C-27 rose from the ashes once, maybe it can do so again. Any good public servant knows not to be too discouraged by good work that doesn't quite make it over the line… it can always be dusted off for another try.

Among other things, C-27 would have created the Canadian Privacy Protection Act. At its heart, consent is reinforced in the Act, but unlike the GDPR, no separate legal authorizations would be available. Consent would remain the cornerstone of the legislation, and new exceptions to consent would be added, including the introduction of a "legitimate interest" exception, which would allow organizations to process personal information without consent if they can demonstrate a legitimate interest that outweighs any potential adverse effects on individuals.

Other exceptions included collecting or using personal information for certain business activities, provided the individual would reasonably expect such collection or use, public interest purposes as outlined in the CPPA, transfers of personal information to service providers, and de-identifying personal information.

In my view, this approach to consent is consistent with a rights focus. At the same time, it recognizes that it is neither reasonable nor fair to not introduce alternative methods of legal authorization. This approach avoids the notion of a privacy regime where people are left on their own to defend their own privacy.

But while C-27 took a different approach from GDPR on legal authorization, it was similar in another way. It would have strengthened the OPC by giving it order-making power and the ability to assess significant administrative monetary penalties. As in Europe, companies would have to take notice.

So, all fine and good. But where does that leave us nationally, and here in British Columbia, now that C-27 has died? There is certainly a sense here in BC that legislators were waiting on PIPA reform to see what would happen at the national level.

So, how long should we wait?

Well, Quebec hasn't waited. Quebec's Law 25, known in English as the *Privacy Legislation Modernization Act*, moved ahead on private sector privacy reform, and in doing so, took strides to strengthen consent. It also strengthened the CAI – giving it the ability to assess administrative monetary penalties.

The Government of Alberta has also signalled its intention to reform its *Personal Information Protection Act* to stimulate innovation while protecting the privacy of Albertans.

My view is that we don't need to wait in British Columbia, either. After this much conversation, it is clear what is needed to stimulate innovation, and it is clear that Canadians value privacy as a right.

On the 20th of January, Canada was plunged unwillingly into a new era, an era where we are learning that there is a lot about our economy that we can no longer take for granted… an era where the urgency to use every lever to stimulate our economy and increase our economic independence has become suddenly and drastically increased. We need to keep pace.

PIPA's principles are strong, but it was put on the books 20+ years ago, back when social media didn't exist, let alone artificial intelligence.

But we are not just in an era of economic vulnerability. We are also in an era of democratic vulnerability. A lot of the economic turbulence that we are seeing now is driven by a loss of faith that people have in countries around the world about whether their democratic and economic institutions are working for them.

There has been a loss of trust – trust in each other, trust in elites, trust in big business, trust in our institutions….

And while our democracy in BC and Canada remains as healthy as anywhere in the world, we all feel the

political polarization that surrounds us even here. We cannot ignore it. We need to use every lever that we can to support and restore political trust.

While we may need to modernize our legislation to foster innovation, we need to do so in a way that is consistent with Canadian values.

So I think the time is now to engage in a reform of PIPA in BC. An amended statute for this new age would be based on a consent model.

These are what I think the main elements would be:

Consent would remain the keystone, respecting the rights-based approach that we value in this province and in Canada.

The new model would explore ways to refresh and repair consent, by learning lessons from how the GDPR has strengthened consent and pushing against deceptive design practices.

It would recognize that consent may not be practical and useful and appropriate in all circumstances. And so, as C-27 did before it, it would open the door to new exceptions to consent, though with appropriate guardrails. It would also strengthen regulatory oversight by introducing elements such as administrative monetary penalties, following the lead of Quebec, alongside many international jurisdictions.

I started this speech by saying that our personal information was the essence of who we are as individuals in this Information Society.

If the way companies are using our information is not consistent with Canadian values, if individuals feel like they are being deceived and manipulated in the service of economic growth that benefits everyone else but them, then trust will continue to erode.

Our statutory reform must be seen to provide the people of British Columbia with strong protections – like the strong penalties in GDPR or Quebec's Law 25 – and it must maintain a rights focus with consent at its core.

Here in BC, we need a modern model to address modern Canadian challenges.

We hope that PIPA is amended in the spirit with which it was first introduced, to make sure that it is fit for purpose, a made-in-BC solution for modern challenges in today's far more complex privacy landscape… a solution that evokes the principle of informational self determination.

In a BC model, the organizations that will win will innovate and figure out how to give people maximum control over their personal information. And the real winners will be the people of this province.

Thank you for your attention and enjoy the rest of the conference.