OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO
FRASER VALLEY REGIONAL LIBRARY
May 28, 2025

Michael Harvey
Information and Privacy Commissioner for British Columbia

Hello, my name is Michael Harvey and I'm the Information and Privacy Commissioner for British Columbia.

I would like to acknowledge that I am grateful to be speaking to you today from the traditional territories of the Stó꞉lō people, the Sumas first nations and Matsqui

As an Officer of the BC Legislature, I also acknowledge that I am privileged to work with people across many traditional Indigenous territories, covering all regions of our province.

I'm grateful to be here - and for the opportunity to benefit from the knowledge shared with us by Indigenous communities throughout British Columbia and Canada.

Thank you to Emily Ducette for inviting me to join you today. It is a pleasure to be here with you in the beautiful Fraser Valley at the beginning of your meeting.

I am also here in Abbotsford as part of my office's listening tour – a public forum that will help inform the direction of our strategic plan going forward. We are asking British Columbians to share their thoughts about what matters most to them in the areas of access to information, privacy and lobbying.

I think you all have other plans this afternoon. But we also welcome written feedback from individuals and organizations. I'll have some information for you at the end of my presentation. Back to the subject at hand – libraries.

My relationship with libraries and librarians is a personal one but one that is hardly unique. Since I was a child, libraries have been, sometimes at the same time, sanctuaries and places of discovery. I have distinct memories as a child, as an adolescent and as an adult, of moments in libraries where I made some connection between an idea and my own identity. Epiphanies happen in libraries. And throughout my life, librarians have been guides on that journey. I will always remember my high school librarian – her name is Joanne Sharpe – and I know that she remembers me because my mother ran into her recently. She helped me understand who I was. And I tell you all this not because it is a special story, but because it is so normal. These relationships are forged every day and that is part of what makes libraries and librarians so special.

But as I have progressed in my professional field of Information and Privacy policy and law, I have come to an even greater understanding of the role that libraries play with respect to information. I say this to you not because you don't know it – because of course you know it more intimately than I ever will – but rather so that you know I know it: Libraries are not just collections of books and periodicals; they are now and have been for millennia, critical nodes in information networks. And information networks are one way of conceiving how individuals interact with each other to form societies.

Libraries don't just house information, they carefully organize, catalogue and curate it. And while the most visible forms of that are those familiar physical things – books, newspapers, journals, microfiche, card catalogues, you name it, libraries also have played a critical role in the digitization of information as well.

We sometimes say that today's youth have grown up with the internet. But my generation – and I expect many of you are of the same generation - have grown up with the internet in a slightly different way in that we grew up while the internet was growing up and participating in its development. I was using personal computers just as they were being invented, and much of that was *in libraries*. Libraries have continued to play this role as societies have become more digital, always at the forefront of information innovation.

But libraries are even more than that – even though for many people the stereotypical image of the librarian has been someone pleading for quiet, the reality has through the ages been that libraries have been community hubs – secular (and often non-secular) temples. Because libraries have never been just about the storage of knowledge but are really about the *sharing* of knowledge. The irony of the shushing librarian is that in truth libraries have never been about stifling communication but about precisely the opposite. They are and always have been about *maximizing* communication.

And a last personal note – my first date, with the woman who is now my wife – was in a library, more than 30 years ago. In the weeks and months that followed I romanced her with silly poems written the newly invented email on a library terminal while she sat at another terminal probably 50 feet away. So, when I say libraries hold a special place in my heart, I mean it in more ways than one.

So… down to business: I'm here today to talk about some of the challenges around patron and employee privacy, to answer a few common questions that Emily provided, and hopefully impart some practical tips for navigating the *Freedom of Information and Protection of Privacy Act.*

….

First, I must tell you about my role as BC's Information and Privacy Commissioner.

My mandate is centered around protecting and promoting the privacy and access rights of people living in British Columbia as they are set out in two laws, which we enforce:

- the *Freedom of Information and Protection of Privacy Act* (or FIPPA), which applies to more than 2,900 public bodies in BC, including libraries,
- and the *Personal Information Protection Act* (PIPA), which governs any private sector organization in BC collecting, using, and disclosing people's personal information..

Our office was established in 1993 as an Independent Officer of the Legislature. I am appointed not by the government but by the legislature on the recommendation of an all-party committee operating on the basis of consensus. I don't report to any Minister or the Premier. Indeed, while I report on administrative matters to the legislature, as it relates to the *substance* of my mandate, I am independent from the legislature itself and accountable to and by the Act.

This preserves the independence – both actual and perceived - and the integrity of the office in our oversight role.

The aim of our office and the other statutory officers in BC like the Auditor General, Ombudsperson, Chief Electoral Officer and Human Rights Commissioner, is to help ensure a more transparent and accountable government. And that is critical for trust in our democracy.

We mediate and investigate access and privacy issues, issue legally binding orders, and conduct in-depth investigations and audits into compliance with the laws my office is charged with overseeing.

We have many statutory mandates related to that oversight function, including education, commenting on the implications of new policies, programs or technologies, and investigations and enforcement regarding how privacy laws in BC are administered by public bodies and organizations.

…

I know those of you who work for libraries are thoughtful people, so I wanted to take a minute now to reflect on the meaning of privacy.

- What is privacy? There is no single precise definition in law; interpreting what privacy is tends to be context specific. But at the highest level I think the best way to think about it is to consider it as related to the nexus of ourselves as individuals in relation to each other. This is what it means to be a human as a social animal – if we consider our

individual self in a Cartesian sense – as Descartes said, I think therefore I am, then the core definition of self is internal, what we think – *res cognitans*. However, we exist as fundamentally social animals and these relationships define our existence – whether with a single other individual, with a family, with friends and co-workers, with the broader society and with the state, these are all nexuses at which privacy needs to be considered, each in a different sense.

- Personal information is exchanged at each of these nexuses

Considered in this way, in our Information Society, our personal information is our essence and the core of our unique identity. It is 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 – a human right.

Today, we can not think about that right without considering the technologies that **permeate** and **animate** our lives… technologies that engage with our personal information daily – whether we're a student, parent, teacher, librarian, or administrator.

We connect with friends and loved ones over social media, we use smart watches to monitor our physical fitness or number of steps. We take classes, borrow and renew books, visit doctors and do our banking, all without leaving our screens.

Apps and websites track our likes, views and searches so that – we are often told – advertising and services will be tailored to our unique selves.

When it comes to personal information, what goes on behind the curtain is just as important as what is in the window.

I'm now going to take you through five more specific topics. Thank you, Emily, for providing me with these areas for discussion:

- First, I'll define what is and is not personal information
- We'll briefly discuss freedom of information requests.
- Then I'll move onto discussing the personal information of minors
- We'll look at the disclosure of personal information to other public bodies, such as law enforcement, or other libraries (such as "blacklists")
- Then we will review privacy breaches and security.

What exactly do we mean when we talk about personal information?

Personal information is information about an identifiable individual – anything from health information to a name, an image of someone or information about an individual's religion or education.

It may also include numerical identifiers like a license plate number, or biometric hashes derived from numerical measurements of a fingerprint or other biological characteristics.

Even if the information can't identify an individual alone, it can still be considered personal information:

We often refer to the concept of combining several pieces of seemingly unidentifiable information together to identify a specific person as the mosaic effect.

It's a bit like putting the pieces of a puzzle together: For some puzzles, a single piece may give away what the image is, but for others you may need to connect several pieces before you can see the image clearly.

That's the same for personal information.

For example:

Let's imagine that we were considering whether the make and model and colour of my car is personal information. I drive a bright blue Golf R. Doesn't sound particularly remarkable. Here in the Lower Mainland, that would probably not be considered personal information. But in Victoria it's one of two or three. Most people would not even notice it. But to people that happened to know what to look for, it would be quite identifying. My sister-in-law lives in a small BC town and recently bought a rose gold coloured vehicle. She's one of a relatively small number of doctors in the town. Now everyone in town knows where the doctor is at any given time.

I would also like to talk about employee personal information:

- First, employee personal information is personal information under FIPPA.
- It's a special type of personal information, so whether its disclosure is a reasonable invasion of privacy or not will change from case to case.
- FIPPA does not specifically define employee personal information.
- However, it does define how public bodies must handle personal information related to their employees.
- For example, in responding to an FOI request, FIPPA says that disclosing personal information is not an unreasonable invasion of a person's privacy if the information is about the person's position, functions or remuneration as an officer, employee or member of a public body, or as a member of a minister's staff.
- And FIPPA also consider volunteers and service providers of public bodies as employees.

It is also important to understand what is NOT considered to be personal information:

- Contact information is not considered personal information under FIPPA, including information that allows a person to be contacted at work.
- Contact information is what you would generally find on a business card - an individual's name, position title, business telephone number, or business address.

Personal information is **valuable** – to you, your patrons, and the organizations behind the apps and websites that libraries use to connect people with online services and content.

Before I go on answer the question about when libraries can legally disclose personal information, I want to explain how FIPPA works, because it can be confusing.

…

There are two ways that a public body like a library discloses personal information. The *first* is in response an FOI request. Anyone can make an FOI request for any record held by the library. For the purposes of our talk today, keep in mind that FOI requests cannot go unanswered – by law, the public body must respond, even if it is to tell the person requesting the information that the library is not granting access to it.

The *second* way that a public body discloses personal information, is when another public body or agency asks for it. These disclosures are under a different part of FIPPA than FOI requests. Unlike responding to FOI requests, which is mandatory, responding to these requests is discretionary.

For example, the police, a government Ministry, a school, or another library might ask your library for information about someone, even without a court order. The thing to remember about these requests is that a library does not have to respond, and they do not have to give up the personal information. They can **choose** to, if there is an authority in FIPPA that lets them.

A public body may exercise its discretion about when to voluntarily provide personal information to police for the purposes of assisting them with an investigation, and when to demand a court order.

….

Moving on to the personal information of minors….

Sometimes there are situations where a parent makes an FOI request for their child's borrowing history. The library must determine if the parent is asking on behalf of a child who is not capable of exercising their own rights. If they aren't capable, then the library must decide if the parent is truly asking for the information on behalf of the child. If yes, then the library can give the parent the child's borrowing history as if they were giving it to the child themselves.

If, however, the parent is asking on behalf of a child who **is** capable of asking for the information themselves, the library should tell the parent to have the child ask for their own personal information from the library directly.

If a parent insists on getting their child's information for the parent's own purposes, then that parent must make an FOI request.

The same applies for anyone asking for the child's information who is not their legal guardian. And the mandatory exception against a public body disclosing personal information that would be an unreasonable invasion of a third party's personal privacy may well apply.

For those of you who may not know already, the process for individuals requesting personal information of a minor is set out in s. 3 of FIPPA Regulation 155/2012.

This naturally raises the question "at what age can a child exercise their privacy rights under FIPPA." The answer is that **it depends**. There is no age. The test is whether the child is **capable** of acting under the section in FIPPA.

Other times, a relative or a noncustodial parent requests information about a child. Again, FIPPA has rules about that which are set out by Regulation. Typically, these individuals will not get access to that information under the rules in FIPPA. Only the child's guardian can request access, and only if the child is incapable of exercising their rights to access their own information..

In any case where an individual makes an FOI request, either on their own behalf or on behalf of someone incapable of exercising their access rights, like a young child, FIPPA contains several exceptions to access. Some exceptions under FIPPA provide that public bodies *may* withhold certain kinds of information, while others require that a public body *must* withhold information.

For example, s. 19(1)(a) of FIPPA permits the head of a public body to refuse to disclose personal information if disclosing it could reasonably be expected to threaten a person's safety or mental or physical health, including minors.

….

Let's take a closer look at requests from law enforcement, public bodies and other agencies for personal information held by a library about an individual.

FIPPA contains many authorities that would allow a library to exercise its discretion to disclose personal information without the consent of the individuals the information is about. Section 33(3)(d) gives a public body the discretion to disclose to a law enforcement agency to assist in a specific investigation, undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result.

We interpret this to require some kind of evidence that the disclosure is connected to a specific investigation undertaken with a view to a law enforcement proceeding, such as a police file number.

In addition to this authority, FIPPA has two other disclosure authorities that pertain specifically to authorizing public bodies to disclose personal information to the police.

As we see in your library system's privacy policy, even requests from law enforcement must be considered in terms of confidentiality and the protection of privacy.

The policy states, "If **necessary**, personal information may be disclosed to comply with a subpoena, a warrant, or an order by a court, person, or body in Canada with the jurisdiction to compel the production of information, or to **respond to a specific written request** from a law enforcement agency to assist in a specific investigation."

A verbal request is not enough.

You may also be wondering if your library can share information with other libraries about patrons who violate borrowing rules or who are disrespectful to property, other library patrons, and staff.

The short answer is that under FIPPA, most of the time, libraries cannot share this information.

As you probably know, BC's Library Act (s. 47(c)) authorizes a library board to "exclude from the library anyone who behaves in a disruptive manner or damages library property" but that power does not extend to notifying other libraries about an individual's exclusion from their own library.

If a library wanted to share information with another library about someone it has excluded, or if it wanted to collect this information from another library, then the library would need to complete a Privacy Impact Assessment to determine whether authorities existed within FIPPA to allow the sharing of this information and under what circumstances they could share it.

My office is pleased to review these assessments or comment on them.

….

Turning now to privacy breaches…

Despite best efforts at prevention, privacy breaches commonly occur for public bodies, which is why a privacy breach management process is an essential part of your privacy management program.

Libraries have been targeted globally by cybercriminals over the past few years, including attacks at the British Library, the Library of Congress, and the Toronto Public Library. The Calgary Public Library managed to thwart their 2024 attempted cyberattack. Good for them.

If a breach does occur, your breach management processes should include four primary steps:

1. Containing the breach:
    - Take steps to prevent any further impact of the breach
2. Next is assessing the risk:
    - Assess the risks of harm to the individual because of the breach and any risk of further privacy or security breaches.
3. Notify the individuals impacted by the breach, as well as our office

4. Take steps to prevent future breaches from occurring again:

In some circumstances, it is now mandatory for public bodies to notify our office and the affected individuals as well when a breach occurs.

Our guidance on our website has detailed information about breaches.

As the demand for digital services grows, more and more libraries are adopting cloud-based technologies and third-party software (e.g., Hoopla, OverDrive, PressReader), which means that patron data is no longer solely protected by the library.

These applications, as well as internet service providers, might track interactions clients have on public machines. Libraries should regularly check the configuration of their systems to make sure that the next individual who visits a library terminal cannot access personal information or browsing history of the individual who used the terminal before them.

Just as security threats are growing exponentially with respect to cloud-based services and third-party applications, so too are the operational challenges to public bodies posed by artificial intelligence. As information experts, you are all probably aware that these AI systems need a vast amount of information to be trained, and much of their training data is personal information.

The question of how AI systems collect, use and disclose the personal information of our children and youth is fundamentally a privacy question.

And, as you can imagine, children are at a particularly high risk of negative impact by AI technologies.

This is why, as a vulnerable group, children need even greater privacy safeguards.

Libraries can play an important role, particularly with children, in educating your patrons about some of these concerns. Carefully assess apps and vendor services, ask to see their PIAs, and be sensitive to any aspects of AI that could harm library patrons….

Which brings me to a brief discussion about security.

FIPPA's S. 30 is the "go-to" in terms of implementing reasonable security safeguards:

But what are reasonable security safeguards?

- Security safeguards are measured on an objective basis against a standard of reasonableness.
- This does not mean that security arrangements must be perfect, but it does signify a rigorous standard.
- Reasonable safeguards should include several layers of security, that are technical, administrative and physical (we will talk about it more below).

Completing both PIAs and security threat and risk assessments helps identify appropriate privacy and security measures to reduce risks to personal information and systems containing personal information.

For each privacy risk you identify, include a risk response that is proportionate to the level of risk.

The higher the risk, the more robust the risk responses should be.

Our office has published a self-assessment tool for public bodies and organizations, if you would like to assess your security arrangements.

As technologies we can't even imagine today continue to disrupt our society, public libraries have an opportunity to be leaders in privacy practices and technology. You are also uniquely placed as well to educate communities with workshops and discussions on privacy, online safety, and this brave new world.

And we are here to help you along the way.

Thank you again for inviting me to speak with you. And now, I believe we have time for some of your questions.