OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO
THOMPSON RIVERS UNIVERSITY
PRIVACY AND SECURITY CONFERENCE
JANUARY 22, 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. Before I begin my remarks today, I would like to respectfully acknowledge that I present to you from the traditional territory of the Tk'emlúps te Secwépemc people.

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'm grateful to be here with you – and to work and live on this beautiful land.

Today we're here to talk and learn about the Dark Web – what it is, what it isn't, its infrastructure, as well as the legal and ethical aspects of using the Dark Web, cybercrime and law enforcement of criminal activities on the Dark Web and, I'm sure, much more.

Thank you to the organizers of this conference for inviting me to speak with you about the Dark Web from my perspective as an Independent Officer of the Legislature.

What is that perspective?

Well, our work 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:

• the *Freedom of Information and Protection of Privacy Ac*t (FIPPA), which applies to more than 2,900 public bodies in BC, including public schools and post-secondary institutions.

• and the *Personal Information Protection Act* (PIPA), which governs the private sector and applies to private schools.

We mediate and investigate access and privacy issues, issue legally binding orders, and conduct in-depth investigations and audits into compliance with our laws.
As an independent officer of the Legislature, I am not beholden to any political party.
The independence of my role – indeed, of all independent offices of the Legislature – is critically important. It means that we are able to provide objective, unbiased, oversight of the laws we are mandated to enforce.

Not being beholden to any political party means that we hold government to account – we're external, impartial, serving the Legislature as a whole, the "People's House."
And that transparency fosters trust. People can understand what decisions are being made and why. They can feel confident that there are functioning checks and balances in our system and feel more connected to governance.

This role is vitally important given the increasing polarization we see all around us. Mistrust in elites can quickly translate into a mistrust of institutions. The latter is an existential threat to our democracy.

The remedy for mistrust is transparency and the reason why is that in a democracy trust is not something that is given by faith; no one just *deserves* to be trusted. Trust has to be earned through what we do. And that means that people need to *see* what we do.

There are many ways to engender trust, but one of them is through strong independent officers. BC has a robust and enviable system of governance. We have to be careful we don't lose it, because it's something that needs to be defended.

This is something I will not lose sight of over the course of my term because trust in our institutions is fundamentally important to our democracy – it cannot function without it. That trust is equally important in our use of the internet – trust that our online interactions will be safe, secure and protected. I need to be clear that the OIPC is not anti-technology. We like to remind people that we are not the "Office of No." What we aim to do is to recognize how best to achieve the public purpose in a way that enhances the privacy of the people of British Columbia. Personally, I would say that while I'm hardly a techno-utopian I am a techno-optimist.

The internet is often compared to an iceberg. It has three layers: the surface web, the deep web, and the dark web.

The surface web represents the top of the iceberg, with about 5% of total internet content. Sites that can be indexed and easily accessed from search engines, like Amazon, Facebook, and Wikipedia are part of the surface web. Below the water line is the less visible Deep Web. It represents about 90% of the internet and is comprised of sites that cannot be accessed from search engines alone, such as email inboxes and bank accounts, which are typically protected by authentication forms, passwords, and firewalls. The deep Web is said to be about 500 times larger than the surface Web and growing rapidly.
Why is it growing?

Well, I would suggest it is because holders of large datasets are attempting to fence off their valuable assets from being scraped. They're removing that data from the public domain and adding firewalls. We've seen the increase of data scraping in our own investigations, most recently, in regards to a company called Clearview AI.

This joint investigation by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information Privacy Commissioner of Alberta and my office examined 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.

Clearview amassed a database of over three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, children, too. BC's Supreme Court affirmed our decision last month, 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.

The issue of what is "publicly available" information was front and centre in this case – and we are encouraged to see the court affirm we do not exhaust our right to control our personal information once it is in the digital world.

But back to our iceberg. The Dark Web sits at the bottom tip of the deep web. It represents about 5% of total internet content and is not indexed by regular search engines. It requires specialized software to access and uses encryption to provide anonymity and privacy for its users.
The Tor ("The Onion Routing" project) network browser gives users access to visit websites with the ". onion" registry operator. I find it interesting that this browser service was originally developed by the United States Naval Research Laboratory in the 1990s.

Although there are many s activities that are performed on the dark web, there are uses that some may view as good. The dark web is more resistant to surveillance, making it a space for whistleblowers, researchers, journalists, and political dissidents to communicate sensitive information.

In 2019, the BBC made its international news website available via the Tor network, in a bid to dodge censorship attempts.

With great care, even the average internet user can visit the Dark Web, perhaps to tune into a number of radio stations that specialize in different genres.

Just don't click on any illegal sites.

Still, given its anonymity, the dark web *does* enable and encourage illegal activities. About 6.7% of global users turn to the dark web for illicit activities such as sharing malware, distributing child abuse content, or selling illegal substances or weapons. That's why the dark web is monitored by a lot of people, all the time, around the world – government agencies, national security agencies and law enforcement.

The "Silk Road," launched in 2011 and shuttered by the FBI in 2013, was the first dark web black marketplace. More than $200 million in illegal drugs and other illicit goods were bought and sold on the Silk Road before enforcement action was taken. Its founder Ross Ulbricht, who used the pseudonym "Dread Pirate Roberts," was arrested and charged with money laundering, computer hacking, and conspiracy to traffic narcotics. Ulbricht was sentenced to life in prison in 2015 and fined $183 million, presumably as a deterrent to other cybercriminals.

Closer to home, CanadianHQ was one of the world's largest Dark Web marketplaces. It may sound like a department store, but unlike the Hudson's Bay, it specialized in the sale of illegal goods and services, including spamming services, phishing kits, stolen credentials and access to compromised computers, which were used by purchasers to engage in a variety of malicious activities.
The CRTC's investigation of CanadianHQ focused on four individuals who allegedly sent emails mimicking well-known brands to obtain personal data including credit card numbers, banking credentials and other sensitive information. The enforcement actions though were nowhere near as harsh as those for the Silk Road founder. Fines issued by the CRTC in 2022 ranged from $50-$150,000 for these individuals' actions.

The Dark Web is also a marketplace for personal information stolen from a data breach. At the OIPC, we hear about the Dark Web most often in the context of privacy breaches that are reported to our office.

Selling stolen data – or threatening to sell or just release it - on the Dark Web is a quick way to monetize personal information, though cybercriminals may have already used the data for their own purposes. Or perhaps they have traded or sold the data to other cybercriminals and want another way to monetize it. They hold the data for ransom and if that ransom is not received, they post the personal information on the dark web. It's an act of extortion, though some organizations refuse to pay the ransom.

Okanagan College was one of these organizations. After a cyberattack in 2023, the college alerted authorities to the incident and did not entertain conversations about paying a ransom. The hacker group Vice Society extracted and published more than 850 gigabytes of sensitive data, including passwords, photos of passports, social security numbers, and credit card numbers.

Ashley Madison, a commercial website that enabled marital affairs, was another organization that refused to pay the piper. Its parent company, Avid Life Media, ignored its demands to shut down its websites. In August 2015, a large number of database files containing emails, source coded and details from some 26 million user accounts were posted online. More than 60 gigabytes of company data in all were publicly released, including the personal information about users who had paid the site to delete their personal information.

Then there was the London Drugs cyberattack. Ransomware operation LockBit claimed responsibility for the April 2024 attack, posting a $25 million ransom with the threat to release stolen data if it wasn't paid within 48 hours. After the retail and pharmacy chain refused to pay the ransom, the cybercriminals made good on their threat, leaking sensitive employee data onto the dark web. The company had to shut down its nearly 80 stores across B.C., Alberta, Saskatchewan and Manitoba for a week after the cyberattack was reported.
The retailer confirmed that while some employee information was potentially compromised in the breach, neither its primary employee database nor its customer and patient database appeared to have been compromised. But even with Dark Web monitoring, how would you know for sure?

The bottom line is that whether stolen information ends up on the dark web or not, public bodies and organizations have an obligation under BC's privacy laws to protect personal information. FIPPA requires public bodies to report privacy breaches to our office; mandatory breach notification is not yet required by BC's private sector privacy law, but it is considered a best practice.

It is a reform we continue to recommend to better protect British Columbians.
Right now, your personal information may have been breached, it may actually be posted on the Dark Web, and you wouldn't know, because that organization isn't legally required to tell you.
The PIPA reform we need more than any other though is the ability for my office to levy administrative monetary penalties.

This is an important enforcement tool for all sorts of scenarios, including in cases when a company's willful negligence of the law results in people's information ending up on the dark web.

The vast majority of organizations want to do the right thing – they want to protect their customer or client's personal information and don't want to jeopardize losing hard-earned trust.
But there are bad actors out there who do not share that respect for citizens, or the law and we must have the ability to impose monetary penalties on them for their actions. When public bodies and organizations report a breach to our office, we guide them through four key steps.

The first three steps must be undertaken as soon as possible following the breach.

• Step 1: Contain the breach
When personal information ends up on the Dark Web, the potential for its misuse increases exponentially. However, regardless of where the information ends up, a privacy breach can cause significant harm, including identity theft, risk of physical harm, humiliation and damage to personal or professional reputations, and loss of business or employment opportunities. Nefarious activities can happen well before the information is posted on the dark web.
So, containment is key.

Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking or changing computer access codes or correcting weaknesses in physical security.

• Step 2: Evaluate the risks
To determine what other steps are immediately necessary, including the potential need to notify affected individuals and/or the OIPC, you must assess the risks and harms involved in the breach.

• Step 3: Notification
Notification should occur within a week of the breach if it could reasonably be expected to result in harm to the individual. As I mentioned earlier, mandatory breach notification is not yet mandated by BC's private sector privacy legislation but is a best practice. Transparency is encouraged, for your corporate reputation as well as your customers' online safety. Review your risk assessment to determine whether notification is appropriate. We have a Breach Notification Assessment Tool on our website to assist organizations to make this determination.

• Step 4: Prevention
The fourth step provides recommendations for longer-term solutions and prevention strategies. As the saying goes, an ounce of prevention is worth a pound of cure.

And of course, it's a much better option is to have robust cybersecurity measures in the first place than to have to deal with a breach.

I've heard experts say that the only really good way to know how to respond to a cyber attack is to have suffered a cyber attack. What they mean is that there is inevitable confusion when a cyber attack happens. The first symptom is often that your systems just stop working. And that kicks off two dynamics – an operational response to try to figure out how to get systems up and running and get operational again, and a separate response to deal with the bad actors.
The latter set of operations is highly sensitive because firms want to protect themselves and their clients and worry that a misstep may involve the bad actors releasing the information. Meanwhile the operational people aren't just trying to deal with missing data. They're also managing a forensic operation to ensure that there is no malware infecting the systems that still work – so system shutdowns tend to spread wider for quarantine processes until they get restored. And often the operational people feel confused and out of the loop because they don't know what is happening with discussions with the bad actors.

This can create a "fog of war" type of situation that is particularly difficult for communications people – who need to ensure that they are providing as much information to clients as possible, as clearly and coherently as possible.

So, like I said, this is very difficult to know how to do unless you have experienced it before. And that means that every organization has to have two things: a plan, even if a basic one, and a number to call. Large organizations can afford high priced cybersecurity and legal firms. Smaller organizations may feel overwhelmed. But one number that anyone can call is the OIPC.
We sometimes get concerned that small organizations are wary to call us because they view our role as one of enforcement. But our primary role is oversight, and we have resources and advice that we can provide to all organizations large and small.

But of course, the very best thing that you can do to respond to a cyber attack is to do what is in your ability to prevent one from happening in the first place. So, let's switch to talking about that:

How can you prevent a data breach?
Begin by reviewing your incident responses plan, your privacy management plans, and your privacy impact assessments. Are they current? Are they fulsome? Are you scanning for vulnerabilities?
Maintain data hygiene. Look at your records retention policies. Review the personal information you are retaining and ask yourself; do I have a legal obligation to retain this information? Do I have an obligation to destroy this information

Train your staff to recognize phishing attempts. In our experience that the majority of all cyberattacks begin with a phishing ca? Mitigate risk!

Consider and re-consider consent. Do I have the necessary consent to collect this personal information? To store or disclose it?

These endeavours, once crude and obvious, have become increasingly sophisticated. When in doubt, don't click on that link. Delete and/or forward to your IT department.
Train your staff on how to create secure passwords – and change them often.

It's also important to consider your service providers and contractors. Review your agreements and ensure there are clear roles and responsibilities for service providers in the event of a privacy breach.

The Blackbaud Data Breach, for example, affected many non-profit organizations around the world. The third-party service provider, one of the world's largest providers of education administration, fundraising and financial management software for non-profits, was targeted by a ransomware attack in 2020. The cybercriminal removed data to extort funds from Blackbaud, who paid a ransom in exchange for the deletion of the extracted data. The personal information may have included sensitive information such name, address, email and phone number, donation information, and more.

Another tool that you may wish to consider is adding an additional level of security by encrypting data at rest within a database. This was a recent recommendation we made to the Provincial Health Services Authority, when we conducted an investigation into whether the Authority had the necessary security and privacy measures in place to protect personal information in their database. Our office also recommended that the PHSA conduct penetration testing, sometimes referred to as "white hat hacking" or "ethical hacking," at least once a year.

We have an extensive library of guidance documents on our website to assist both public bodies and organizations with accountable privacy management, managing privacy breaches, and other helpful tools and resources.

Be sure to sufficiently resource your cybersecurity program and conduct regular external audits including dark web monitoring to ensure that your program is meeting your needs. Keep that barn door closed. Remember, the consequences of failing to invest in privacy and security can be catastrophic. That is precisely how the *New York Times* described a 2021 breach of a database in my home province of Newfoundland and Labrador that effectively paralyzed the province's entire health care system. I could go on and on about that breach, as I was the province's privacy commissioner at the time.

But you have a conference to attend.

Wondering how you can protect yourself as an individual? We also have identity theft resources on our website. You can check for cyber threats and advisories at the Canadian Centre for Cybersecurity or on the BC Government websites. And you can educate yourself on how to spot scammers and fake emails.
The bottom line is breaches happen. And while not all stolen data ends up on the dark web, great damage can result from privacy breaches – to you and your customers and clients, as well as your reputation. No one wants their privacy breach to be on the evening news.

In today's busy digital world, deceptive design practices that manipulate or coerce us into making decisions that may not be in our best interests have become the norm. With impossibly complex and lengthy privacy policies, who can blame people for skipping to the bottom line and agreeing in that fine print to who knows what.

No wonder people become cynical about whether privacy still lives and breathes. It absolutely does, it's just that the consent model needs a makeover. People are fatigued.

When you're online, organizations can't just collect your personal information at whim. If we allow that, we are diminishing the notion of the autonomy of the individual, and that's where we need to draw a line.

I spoke at the beginning of my remarks about how transparency creates trust. I strongly believe that companies that put privacy first and are transparent about their practices stand to gain a competitive advantage. They are also best placed to avoid a scenario where information is breached and ends up on the dark web.

In the information age, businesses are collecting far more information than they ever have before, and that trend is only going to continue to accelerate.

As it does, our mandate becomes more important than ever. And my office will be here to defend the privacy rights of British Columbians.

Thank you again for the opportunity to speak with you today.

And now, I believe we have time for some of your questions.