OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO THE

VANCOUVER INTERNATIONAL PRIVACY & SECURITY CONFERENCE

March 11, 2022

Michael McEvoy

Information and Privacy Commissioner for British Columbia

Thanks for that introduction, Drew.

I would like to begin by respectfully acknowledging the Coast Salish Peoples, on whose land we find ourselves today, including the unceded territories of the Musqueam, Squamish and Tsleil-Waututh Nations.

It's amazing to be here in person after a physical absence of two long years.

I need to start with something of an apology to my good friend Greg Spievak. Greg, I know you work very hard at acquiring sponsors for this premiere international event and that for the most part they have exclusive right to product placement.

But I would be remiss if I did not acknowledge my own sponsors from the past two years while I have been captive at my residence in Victoria.

Of course, I speak of my friends at Patagonia whose products have received robust workout over the last 24 months and Costco the makers those inexpensive yet durable sweatpants that have been worn out over the course of the pandemic.

Greg, I trust you can forgive me for that indiscretion.

That business aside… I'd now like to take you back to my world four years ago. I am sitting in a non-descript boardroom in the Information Commissioner's Office in Wilmslow, in northern England.

Across the table from me and my team that day are representatives from one of the planet's most powerful tech firms. The topic? How political parties are using their platforms for conducting political campaigns in the UK.

An issue obviously important then – when the UK was just coming out of Brexit – and certainly just as important now as events unfold on the global stage.

So back to the boardroom…. Although the ICO had formally summoned the corporate representatives for this interview, those tech officials made it crystal clear to me that, although they did business with political parties in the UK, they were not subject to the country's regulations. They also made it clear to me that their presence in that boardroom was only voluntary, a benevolent gesture of goodwill on their part.

What this scenario draws into focus is what we in the regulatory and legal world call jurisdiction – who has authority over who and what.

And in these ongoing battles about who has authority over what in private sector privacy there is an increasing sense of technology actors operating everywhere but seemingly accountable nowhere.

The truth is, these companies don't often pay much heed to local regulators, especially in smaller or less wealthy jurisdictions, even though organizations like Airbnb, Clearview AI or Uber, just to name a few, rely on accessing the markets of many countries of all sizes to create the scale necessary to be successful.

Therein lies the irony.

There is no cogent reason why these companies should not respect the laws of the local jurisdictions they operate within.

But four years after my UK experience, the posturing of these tech companies continues.

Down under, my colleague, Angeline Falk, Australia's Information and Privacy Commissioner, attempted to investigate a claim that Facebook committed serious privacy offences in contravention of Australian law.

Facebook's response? They said the Commissioner should not be permitted to even serve process documents on them because they don't carry on business in that country.

I am sure that came as quite a surprise to the millions of Facebook users on the continent as well as Australian businesses spending good money to advertise on the platform.

But just a few short weeks ago, the full bench of the Australian Federal Court ruled against the company… and Commissioner Falk's investigation continues.

And of course, right here in Canada and in British Columbia, we've had the spectre of an American surveillance company named Clearview AI.

This company prides itself on scraping billions of images worldwide, including yours and mine here in Canada. They insisted that my office and those in Alberta and Quebec had no authority over their actions.

We of course disagree.

If life were simple, we would have one privacy law that extended beyond national boundaries, to regulate these companies.

But even though challenges of properly protecting personal information is a collective worldwide problem, there is no escaping this reality: we don't have and we never will have a single global privacy cop.

Still, laws must be developed nationally and internationally that recognize the true character of the technology paradigm of the 21st century.

Nation states need to think in terms of developing legislative frameworks that enable their own regulators to work across borders despite what will inevitably be differences in legal frameworks.

As my maternal grandmother was fond of saying: "Let us use the imaginations God gave us to figure this out."

It's been done in other areas: international tax treaties and family law child support regimes that allow us to enforce laws and if not laws at least common standards across borders.

And think about the regulatory fabric that has woven the world together: planes can go from one country to another with a minimum of friction and money flows seamlessly through the SWIFT system, which has gained public notice since the Russians began to inflict their terror on the global stage.

It's a reasonable question to ask whether we have made any headway in getting our global act together to regulate data use, because as it stands, it is fair to say that the advances of technology to date have run well ahead of society's ability to properly govern them.

It is an even more important question to ask in considering events of the past two years. And yes, if you have the phrase “COVID has accelerated digital trends” on your conference speaker Bingo card, congratulations you can blot that square now.

It may be a clichéd phrase. But it doesn’t make it any less true, whether it’s in the field of education, medicine, or online commerce, to name just a few industries. The virus has rocketed the trajectory of our digital infrastructure.

That fact further emphasizes the need for regulatory reform and strengthened enforcements mechanisms, globally and within Canada’s own borders.

So, what is happening on this front across the globe and here at home?

First, the drumbeat of reform is getting louder and louder, and it’s driving an advance of new enforcement approaches and new legislation.

The advancement is not, and will not be, linear, and this is a source of uncertainty for business and citizens alike. I get that.

But make no mistake: there is a trend towards reform across the global landscape.

In general, we’re seeing a move towards several GDPR type requirements, as well as increased privacy protections for children and other vulnerable groups.

For example, the Australian government has released a draft bill which proposes among other things the creation and enforcement of a binding Online Privacy Code.

Of particular note are the proposals for new and more proactive regulatory tools and approaches.

I mentioned the importance of regulatory interoperability. The Bill enhances the Commissioner’s ability to share information with other enforcement bodies, including foreign privacy regulators. It also speaks to her ability to publicly disclose information about their enforcement actions – an important tool that is lacking in British Columbia.

Finally, the Bill addresses the matter of extraterritorially and makes it explicit that the law will apply to the personal information of Australians even where that information is collected and held in cyberspace outside its borders.

That latter issue is, of course, at the heart of the current court action between my Office and the face-scraping company Clearview AI.

Speaking of facial recognition, I wanted to tell you about another important action a world away in Austin, Texas.

There, the state's Attorney General has just filed a civil lawsuit against Meta Platforms, Inc., the company formerly known as Facebook. (I'll stick with Facebook for the purpose of this morning's discussion.)

The suit goes after Facebook for its use of FRT. And as only a plain talking Texan could say it:

"Facebook's omnipresent empire was built on deception, lies, and brazen abuses of Texans' privacy rights."

Amongst other things, the AG says Facebook's algorithm "secretly forced millions of Texans into a facial-recognition scheme without their informed consent."

The stakes are huge: each violation of the Texas biometric protection law can result in a fine of up to $25,000 and the suit alleges Facebook violated its laws on literally billions of occasions.

Over on the left coast of America, the State of California is looking to adopt a "children's code" which would limit the data that companies could collect from young users and the location tracking of children.

This California Bill is really important because of course many of the world's biggest tech companies are headquartered in the Golden State.

If adopted, the law would place restrictions on profiling younger users for targeted advertising, mandate the introduction of "age-appropriate" content policies, and ban serving up behavioural nudges that might trick children into weakening their privacy protections. Significantly, the Bill has bipartisan support in the Legislature, which these days is a rarity anywhere in the United States.

If one needed evidence of cross-pollination between the privacy reforms across jurisdictions it is plainly evident that California's efforts significantly mirror the UK's recently introduced children's code.

Indeed, Buffy Wicks, the California assemblywoman who co-authored the bill, referenced the UK code as an inspiration and a "proven concept."

And that same inspiration has now spread to Ireland, where that country's Dáil is following suit, adding further momentum to this reform.

In the EU, the GDPR continues to move forward. Although its mechanisms appear, at times, cumbersome, I would suggest to you that is the price of many jurisdictions working together toward a common good. I think the most noteworthy of recent events in the EU are the rulings by the CNIL in France and the Austrian Data Protection Authority. They have found, that in the absence of an adequacy agreement between the US and Europe, Google's transfers of Europeans' personal information to the US to feed the Google Analytics algorithm contravene EU law.

Before I turn attention to where we are at in Canada, I think it's worth noting that one of the most significant recent changes that has circumscribed online surveillance has come not from a regulator but from a big tech company itself.

I'm referring of course to recent changes made by Apple Corporation to its operating platform.

Users of the iOS platform now have the clear choice to opt out of ad tracking so enmeshed in the digital ecosphere. By most recent reports, 62% of Apple users have opted out of tracking. For those of you who think the option of consent when meaningfully offered is meaningless, I think this result indicates otherwise.

Further evidence of the profound effect of Apple's App Tracking Transparency feature come from Facebook itself: the move, Facebook said recently, will decrease the company's 2022 revenues by $10 billion.

When faced with a real choice, it's clear most people would opt out of being tracked. It should be a choice that is easy to understand and not buried in privacy policies. That is one principle among others that need to be reinforced as we embark on reform here in Canada and British Columbia.

And make no mistake, change is happening here in Canada and more is on the way.

Just before I elaborate on this, I think it necessary to address something I hear frequently these days among some in our field: that the change that's happening in the privacy realm is very problematic because we have too many provinces passing too many laws and that people and businesses will not be able to handle it. The detractors then say, "Wouldn't it be better if we just had one single law across the country?"

My reply is this: There is nothing wrong with differing laws so long as the principles underlying them are harmonious. And second, it's time to face a simple reality. We live in a constitutional federation where responsibilities are divided between federal and provincial governments and provincial governments are entrusted with responsibility for property and civil rights. It is thus and will continue to be the case in our lifetimes.

That said, and to repeat, it is critically important that in advancing privacy reform in this country, federal and provincial legislators align the underlying principles and substantive provisions of our laws… and that regulators themselves work closely together to administer these laws.

In the spirit of advancing legal reform let me contribute the following.

First – if you are a provincial government, don't wait around or expect the federal government to lead, either quickly or boldly in this space!

The recent attempt by the federal government to advance the Consumer Privacy Protection Act died a quiet death on the government's order paper and has yet to be resuscitated. And at that its proposals fell far short of what I believe the public expected or what is required to meet the moment.

It is also worth remembering that British Columbia did not wait around before improving upon the federal government's PIPEDA legislation in 2004.

In passing the *Personal Information Protection Act* in that year, BC legislators covered huge gaps left by federal law. While PIPA was principled base like its federal counterpart, it went well beyond it on many fronts, like its application to political parties and many other organizations like charities and trade unions. It extended coverage to a broader range of employee personal information and, most importantly, gave powers to the regulator to back up its rulings with order making authority… a very important responsibility the federal commissioner still does not have.

And as we boldly move forward in 2022, we need keep in mind – and I paraphrase here the wisdom of Canadian philosopher Wayne Gretzky – when you do lead you need to focus on where the law is going not where its been.

And where is the law going here?

Much like what I have described is going on globally. The trendlines point towards greater protection for citizens and tougher sanctions on companies who violate those protections. Whatever emerges will undoubtedly reflect some influence of Europe's General Data Protection Regulation.

And though the federal government's Consumer Privacy Protection Act died on the operating table as I noted, the autopsy reveals trace elements of the GDPR being implanted.

And the shadow of the European Regulation is clearly obvious in the Quebec government's recent passage of Bill 64. To my earlier point, Quebec did not wait around for the federal government to act on privacy reform.

The new law there establishes requirements for the private sector previously unseen in this country.

And look, Bill 64 has its advocates and detractors and is no doubt imperfect, but the trajectory we see here is clear – it includes a further gloss on Canadian concepts of accountability together with the adoption of measures lifted from Europe, such as rules around the conduct of privacy impact assessments, automated decision-making systems, de-identified and anonymized data. And it is backed up by the imposition of significant administrative penalties.

The inexorable drumbeat of reform has now made its way to British Columbia.

A committee of BC legislators whose task it was to review our province's *Personal Information Protection Act* tabled a report just a few short months ago that addresses many of the same issues tackled in Quebec, in the UK and by the GDPR. And their recommendations point towards similar reforms.

In fact, BC's Special Committee to review PIPA explicitly acknowledged GDPR as being the "gold standard for privacy legislation" and said PIPA needs to be modernized in a way that embraces in part the European law's concepts.

GDPR is of course not perfect and Canada and its provinces will chart a course that reflects our own histories and circumstances, but one sees in all of these reform moves a desire to align broad concepts and principles to attain some form of regulatory interoperability in the privacy sphere.

This is not only a practical matter but it's also a legal one as well in that BC's law must be substantially similar to the federal law to have force and effect.

The underlying objective is that the same or similar standards should apply across the country. It means that citizens and companies will benefit from comparative privacy protections and compliance.

BC's Special Committee has done its work and it is now with our government to consider actioning its recommendations.

We have lagged behind for too long.

Fortune favours the bold: we need our legislators to be forward thinking, to realize that meaningful, modern privacy protections are possible and indeed critical to a functioning democracy.

Individuals and businesses need those privacy protections that keep pace with and even anticipate where technology will take us next.

And while legislators work to advance and align privacy laws, there is also a heavy burden of responsibility on regulators, that includes my office, to coordinate educational and enforcement work when the circumstances demand. I think you have seen many instances of this during my tenure as Commissioner: jointly investigating Facebook and Aggregate IQ with the Federal Commissioner, LifeLabs with Ontario's Commissioner and numerous other matters with colleagues in Alberta and Quebec, including Cadillac Fairview and most recently Clearview AI.

I expect you will see more joint work in the years to come. When matters involving multiple jurisdictions arise, business and the public can be assured of a coordinated response from regulators.

And just before leaving the issue of privacy law reform in British Columbia, it's also worth observing that real advances in privacy protections have found their way into our public sector legislation.

These recent amendments have generated far less attention than the more controversial access to information changes to but are nonetheless just as consequential.

These reforms broaden the requirement for privacy impact assessments, bring in formal mandatory breach notification, and obligate public bodies to develop privacy management programs.

A number of you, I would imagine, will be helping with this work.

The biggest change in the *Freedom of Information and Protection of Privacy Act* was around data residency.

Until now BC's public bodies could only store and allow access to personal data within Canada, subject to some narrow exceptions.

Some said this was necessary to safeguard British Columbians' personal information from among other things foreign surveillance while others argued that in today's online world, the requirement meant that public bodies and ultimately citizens couldn't take advantage of the many benefits that digital services have to offer.

At the outset of the pandemic, the government relaxed the rules around data residency so that public bodies could make greater use of online tools for education and the provision of health services.

At the time I said these measures, then deemed temporary, were reasonable and tailored.

It appears, that in the end, Covid-19 was the accelerant that killed data residency.

While FIPPA's recent amendments change the "default setting" of data residency, the requirements for public bodies to make reasonable security arrangements remain. It is my office's expectation that any disclosure of personal information outside of Canada's borders will require a public body to carefully assess the concurrent security risks. That means, among other things, analyzing the jurisdiction in question and the sensitivity and volume of the information at stake. My office has just issued guidance on this matter which I would invite you to check out on our website.

I often think back to that non-descript boardroom in the UK four years ago and the dismissive attitude of those big tech players across the table – the essence of which was, there was nothing to see here folks and nothing to be concerned about, when it was and is clear to everyone there is indeed much to be concerned about.

The collection and use of data, yours and mine, digested and spun through increasingly sophisticated algorithms that have taken us to sometimes benign places … but other times, far less so.

We are a more divided society. And not just divided but a society where some people live in a parallel universe disconnected from reality. Many of us have experienced this first hand with friends and relatives.

This has to change if we are going to survive on this planet.

Part of the solution is legal reform that establishes meaningful laws across jurisdictions that will ensure people's data is used legally and ethically. Those laws will allow regulators to coordinate forces to back up those meaningful laws. It is happening, sometimes at pace that can be frustratingly slow, but such is the nature of democratic governance. And in the end those reforms will be necessary for our democracy itself.

Whether you are here in the room or signed in online this morning I appreciate your time. Thank you.