OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

**CHECK AGAINST DELIVERY**

# SPEECH TO THE
# VICTORIA PRIVACY & SECURITY CONFERENCE

**February 5, 2021**

**Michael McEvoy**

**Information and Privacy Commissioner for British Columbia**

Thank you, Drew.

Good morning. I want to respectfully acknowledge that I present to you today on the traditional territories of the Lək$^{w}$ əŋiṅəŋ people, also known as the Songhees and Esquimalt First Nations.

I find it almost surreal that one year ago I was wandering the stage of Victoria's Convention Centre, addressing many of you. All I can say is, what a difference a year makes! I applaud Greg and Christine, and the Reboot team, for bringing us all together once again, because the discussions we are having, virtual though they may, really are more important than ever.

This year's meeting reflects digital trends, many of which have been prophesized by this conference for more than two decades. The coronavirus epidemic has at once diminished our physical interactions and accelerated our virtual ones.

I confess to having encountered my first two virtual doctor visits in the past six months – a rather different experience that made me think that those crazy Jetson cartoons I watched as a kid were perhaps more prescient than any of us might have imagined.

But of course, our virtual interactions don't end with conferences and doctors. Abetted by stay at home orders, retail has continued its explosive online migration. Our offices have also been radically reshaped, with millions working from home where circumstances make it possible.

As an aside, I was something of a skeptic pre-COVID about how work from home might alter the operational effectiveness of an office like ours. Well, I have had my eyes opened…. I've been absolutely blown away by how well our team has adapted to the new environment imposed upon them.

Education is another area significantly reshaped by the pandemic, as a lot of learning, whether K-12 or college and university, has gone online. Together, these changes have significantly impacted society and, of course, of special interest to all of us, their reshaping of privacy and security.

What has this meant for my role as a regulator? My mandate is multifaceted, of course: I am an investigator, a mediator, an enforcer, and an adjudicator of laws. But this crisis has, more than anything, called upon my office's role as a dispenser of guidance and advice to a wide array of interests, from businesses and school educators to the general public.

We have offered our expertise on matters ranging from how retail establishments should collect and use their patron's personal information to how educators should deploy new technological learning tools for kids; from how seniors shopping online, often for the first time, should protect themselves to what businesses can do to make sure work from home doesn't expose the sensitive information of clients and customers.

In all of this, one major thing bears repeating – and in saying this, I am far from alone among my regulator colleagues globally: BC's legislation is designed to facilitate the sharing of personal information necessary to ensure the public's health and safety… the protection of personal information does not pose a barrier to ensuring public health and safety. Quite the contrary: it serves to ensure the necessary critical flow of information – and it's worth emphasizing the word **necessary**, and not beyond that which is necessary.

It is not without worry or precedent that governments of all stripes over history have used a crisis to reshape their relationship with those they govern. That is especially so on matters of privacy protection.

Witness the mass domestic spying programs in the US developed in the wake of 9/11 and later revealed through whistleblower disclosures. That is obviously a very dramatic example, but it is a reminder that all us as citizens and regulators must be wary of government overreach at a time of societal disruption.

It is why we had a careful eye on the BC provincial government when it moved to implement emergency measures to deal with the pandemic. Specifically, they temporarily lifted BC's data residency requirements. For those of you not familiar with BC law, for the most part public bodies are not allowed to store or access personal information outside of Canadian boundaries. Some have viewed the government's measures with suspicion, given the pressure already exerted by industry and public bodies alike seeking to use shiny new tools that are based largely in the US.

The government's special orders broadened the use of communication tools by public bodies to use technologies hosted outside Canada to communicate and collaborate for delivering services

during the public health emergency. To the government's credit, they moved early to consult with my office, detailing how they intended to draw the orders in a narrow fashion.

In the end, I regarded the temporary provisions as tailored and reasonable, given the immediacy of the challenges we found ourselves in. Importantly, the order has a defined end date, and we continue to carefully monitor its use by public bodies.

Meanwhile, fellow regulators have been keeping a close watch on other COVID initiatives, like those apps designed to assist with tracing the disease. The potential for personal data collected on a mass scale to be misused is enormous. My fellow Canadian commissioners and I have pushed for a solution in this country that is privacy protective.

Looking abroad, my colleague Commissioner Angeline Falk in Australia supported legislative measures prohibiting police from dipping into COVID-collected data. She did this with a view to enhance public trust in the app and encourage its uptake. This thinking was not without justification, given what has just happened in Singapore. There, local law enforcement confirmed they were given access to the TraceTogether app data to aid in criminal investigations. This gives new meaning to a quote from W.P. Kinsella's bestselling novel *Field of Dreams*: "If you build it they will come." These kinds of stories undermine the public's trust in what might otherwise be part of a solution to bending the pandemic's curve.

But other even more critical matters are impairing society's ability to reshape the curve. Millions of people believe the pandemic is a hoax, perpetrated by the likes of Bill Gates and George Soros, and that attempts to arrest COVID's spread through a vaccine will cause autism, or worse, that nano chips infused in the vaccine will be activated by 5G technology.

This pandemic, it has been said, has exposed many societal vulnerabilities across the globe. I want to spend a moment talking about one of those within the remit of all of us who work in the data collection world.

If there were any doubt, the past year has completely unmasked the untrammeled powers of big tech. Facebook users have given over much of their personal information only to have it mediated in a way that has wreaked havoc and destruction. You will note I have not called Facebook, or for that matter other companies like Twitter, social media platforms. The word "platform" connotes a stationary, neutral setting where people go to express ideas and those ideas are shared organically. But of course, that's not how it really works.

Even though you choose your friends or who you follow, the companies determine what you see on your screen. It's all carefully calibrated to hold your attention for advertisers.

Tristan Harris, the former Google design ethicist, summed it up well, saying that: "The people behind the screens have a lot more power than the people in front of the screens."

Outrage, hate, and conspiracies fuel the spreading of lies and disinformation that capture our attention. Such is the vulnerability of the human brain. By Facebook's own account, 62% of people who join Facebook extremist groups did so as a result of the company's recommendation algorithm. The US, and they are far from alone, is being torn apart on a sea of disinformation that claims that their President was elected through subterfuge.

All of this raises a big question about how we bring these companies, and others who aspire to be like them, to heel. This is not an easy question. Things seem to have happened so quickly over the past 15 years that at the outset it was not exactly clear who was in the best position to regulate the burgeoning industry in a manner that would protect society's well-being.

It turned out that we as privacy regulators were the first responders to the scene. That made some sense. These new companies, connected to the world wide web, were devouring and using vast amounts of personal information, the collection of which we were tasked to regulate. But our personal data protection laws weren't a perfect fit; they were designed largely to remedy individual, transactional harms.

While laws based on OECD fair information principles contemplated computing, I don't think they foresaw the scale of damage it could inflict on entire societies. But if we as privacy regulators seemed the reasonable candidates to initially answer the 911 call, our medical kit was ill equipped to diagnose, let alone properly triage the patient. We lacked even a basic microscope to analyze the underlying operations of these new systems – but that began to change.

You know, it's fascinating to talk with my friend Elizabeth Denham about her time as the Assistant Canadian Privacy Commissioner, when she visited Facebook's campus in 2008. She undertook a surgical examination of this rapidly expanding enterprise. Her work was pioneering, as we watched the dawn of the surveillance age in real time.

That OPC investigation revealed a number of serious ailments, including Facebook's failure to police third-party apps that were allowed to download Facebook users' data. The diagnosis was clear, but the treatment was not: no order-making power and no ability to levy sanctions that might serve as a remedy.

As an aside, it shouldn't surprise anyone this very same malady identified in 2008 arose a decade later, when Facebook failed to properly police third-party apps who used the company's network

to siphon off the data of millions of its users. I, of course, refer to the Cambridge Analytica scandal – a seismic event with which I am intimately familiar, having helped lead the UK ICO's investigation into it. If this were a medical malpractice case, the harm at issue was absolutely foreseeable.

More than a decade ago, calls for legal reform began to mount. My office was among many in Canada and around the globe that highlighted the lack of guard rails around tech companies. We advocated for changes to private sector laws like Canada's PIPEDA and BC's *Personal Information Protection Act* if the public were to be properly protected. And we warned governments about the potential consequences of their inaction.

The tech companies of course pushed back at all levels.

U.S. lawmakers got this treatment during a session before Congress in spring 2018. Mark Zuckerberg used a variation of the phrase "my team will get back to you" more than 20 times in answer to questions. Other times, like hearings before the International Grand Committee in 2018, composed of nine parliaments, he failed to show up at all.

While at the ICO, I had my own brush with Facebook's character the night the company tried to pre-empt our forensic examination of the scandal. We were seeking a warrant to enter Cambridge Analyica's office — Facebook used its own relationship with the company to enter their premises in advance of us, to apparently do their own "audit" of the company. That they would do this, given they themselves were under investigation in the same matter, says a good deal about the company's view of who really runs the world.

And then there is the evasion tactic that I saw numerous times when sitting directly across a table from big tech representatives in the course of various investigations. "We don't really have to be here" was very often the phrase used, with a smile of course, but adding helpfully they would answer questions voluntarily to the extent they felt so inclined.

The magic word of course is "jurisdiction"; a term of resonant syllables that has a wonderful ring to companies whose operations know no boundaries. And it has never failed that whether it is here in BC or in the UK, I always lacked that necessary jurisdiction as a regulator to investigate matters on behalf of citizens. That these companies collected data from millions in those jurisdictions and accepted the advertising payments of businesses in those places was of no consequence.

And this continues. Commissioner Falk brought an action against Facebook for the data it collected from Australian citizens related to the Cambridge Analytica scandal. This was the result: The Australian Federal Court did not find the company's arguments persuasive. It found that they did collect and store information in Australia, through among other things, caching servers located there. The decision is now under appeal, with Facebook saying there are "important questions"

about how privacy laws define what it means to carry on business in a particular country and "collect" or "hold" personal information.

Indeed, there are. Profiting from everyone, everywhere, but seemingly accountable to virtually no one, anywhere.

I suppose in an ideal world we might have one global regulator with enforcement powers that match the reach of companies that extract and move data without regard to borders. I expect that is not likely any time soon.

But still, the pulse of reform is beating more rapidly. And a convergence of privacy law principles among a number of jurisdictions is beginning to emerge. The ICO in the UK got expanded enforcement powers in the wake of Cambridge Analytica, and our counterparts in the EU now administer the GDPR. California, home to some of the world's largest tech companies, has taken the lead in the US in passing its own privacy law.

And what of our country? We of course have more than one privacy regulator in Canada because we live in a federal system: one federal and three provincial authorities. Although PIPEDA often gets top billing in the country, the reality is that the three provincial authorities cover almost 50% of Canada's population. And at that, provincial legislation is more comprehensive than the federal counterpart.

I raise this not to rank the importance of offices, but to point out the opposite: the pressing need to ensure that privacy legislation across Canada is substantially similar and that all Canadian authorities work in concert when matters affect more than one province. This is critical because it means that companies can't play one regulator off against another. It also benefits organizations, because for practical purposes, they have a one-stop shop to deal with.

That's exactly the way we Canadian privacy regulators have conducted ourselves. Witness our recently released Cadillac Fairview investigation, jointly undertaken by my office with the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Alberta. Cadillac Fairview, one of North America's largest commercial real estate companies, embedded cameras inside their shopping mall information kiosks in several Canadian locations.

Despite the company's claims to the contrary, we found that it used facial recognition software without customer knowledge or consent; the company's service provider collected and stored approximately 5 million numerical representations of people's faces. No-one who pauses to view an information kiosk in a shopping mall would reasonably expect their image to be captured and analyzed in this way. The good news is that company has now removed these cameras in the wake of our investigation and says it has no plans to reinstall the technology.

Facial recognition technology also figures prominently in our ongoing joint investigation of Clearview AI, a company that scrapes facial images from a myriad of places and makes its FRT system available to law enforcement. This investigation includes our Quebec counterparts along with ourselves, Alberta, and the OPC.

I'll be frank in saying joint enforcement work is challenging. Remedial authority, I believe, falls short across the board, but is made even more challenging when enforcement tools between regulators are substantially different. For example, I can issue orders; the federal authority cannot. Our laws between jurisdictions need not be identical, but we do need to strive for some coherent level of harmony; a level that truly advances protections for our citizens when it comes to their privacy rights.

There is some reason for optimism on this front. More than two years ago, Europe's General Data Privacy Regulation moved the dial for privacy on a global scale. Its influence has extended to Canada; Quebec's Bill 64, Ontario's recent call for a modern private sector privacy law, and of course, very recently, the introduction of Bill C-11 in the House of Commons, the long-awaited federal privacy proposal.

The *Consumer Privacy Protection Act* seems at first glance to be a major overhaul of Canada's federal privacy legislation, and it is. I mentioned order-making powers lacking at a federal level; the CPPA finally fixes that. The remedial tool kit however is not without problems. Administrative monetary penalties are absolutely critical as a deterrent to bad actors abusing personal information. The new legislation provides for them, but it comes with a very large catch – rather than allowing the Commissioner to administer monetary penalties in a consistent manner using his privacy expertise, the Bill turns that task over to yet another administrative body, the Personal Information and Data Protection Tribunal.

Despite its name, the tribunal requires only one member with expertise in information and privacy law. Moreover, I simply do not understand the government's almost fetish-like desire to separate certain of these functions and to do so in a less than logical manner. What's the principle here? That investigation and enforcement mechanisms should be strictly separated? But that's not actually what they have done. In fact, the Commissioner has been given the extraordinary enforcement authority to invoke what is essentially injunctive relief, that is, he can order a company to stop its non-compliant actions. This is a good thing. And yet somehow the CCPA goes on to stipulate that the Commissioner is incapable of levying a fine. The total effect will be to have a law with the significant potential to be applied inconsistently, with less expertise taking more time and costing more money. This cannot be to the benefit of citizens this legislation is designed, in part, to protect.

There are a number of other provisions, some of which are positive and others not so much; we canvassed those thoroughly in yesterday's panel and I won't revisit those here …. Other than to say this: As we do our own version of GDPR catch-up, I do worry that the current approaches we are pursuing may already have gone beyond their best before date. For one thing, it is evident to me that privacy laws alone cannot sufficiently restrain the predatory behavior of technology companies and particularly the giants among them. While we privacy regulators were the first responders to the tech crisis scene, ongoing treatment will require a multi-disciplinary approach to legal enforcement…. It will likely require the use of anti-competition and anti-trust laws.

We have begun to see this in Europe, with the EU pressing major cases against Google for manipulating its search engine to direct people to its own products. The US is examining the same company with its trust-busting legislation. The Texas AG's case against Google could lead to criminal sanctions, including jail time, a sobering prospect for executives who in past have reached monetary resolutions as a way out of difficult situations.

Consumer protection law is another angle of regulation which we did see with the Federal Trade Commission's $5 billion fine of Facebook. And human rights and Ombudsperson forces bear directly on questions about the fairness of, for example, artificial intelligence. We as privacy regulators need to be coordinating more action with those whose seek the same general outcomes on society's behalf. I can say in BC, we have recently joined forces with the Ombudsperson to develop guidance for use of AI by public bodies.

Beyond the legal enforcement mechanism is the law itself. Can even our most current progressive laws curb the amplification of disinformation and hatred that keep people tuned in? Can they stop harms, not just to individuals, but to society at large and democracy itself? We may need to start thinking about whether the principles of the current legal framework itself are fit for purpose. At a federal level, it means the Canadian government needs to look at privacy through a human rights lens, as advocated by my colleague Commissioner Therrien.

We are also beginning to see the emergence of other approaches espoused by thought leaders and "data reformers" around the globe. People like Shoshana Zuboff, the author of *The Age of Surveillance Capitalism* and Roger McNamee, a former Silicon Valley investor and an early mentor to Mark Zuckerberg. Now he's a crusader for data reform. I had the opportunity to talk with him at length recently. His book: *Zucked-Waking Up to the Facebook Catastrophe* is a fascinating look into what's gone wrong with the corporate giant. He likens the state of the tech business generally now to that of the chemical industry prior to the passage of the US Clean Air Act or the pharmaceuticals industry before the Food and Drug Administration entered on the scene.

Or consider the building industry, long regulated by codes. When a bridge collapses, the engineer and associated company are responsible for any harms to life or property. But what would happen

if a company designed technology to accelerate the propagation of disinformation during a pandemic for example, causing harm to the population as whole? Where is the responsibility on the part of the computer engineers who design these products and the companies that employ them?

Others who have caught my eye are two US academics, Woody Hartzog and Neil Richards, who make a compelling case for a new legal framework that companies collecting and using your personal information should be subject to a Duty of Loyalty.

Duties of loyalty would be similar to what we would think of as a fiduciary duty placed on professionals including lawyers as well as corporate directors. The suggestion is that loyalty is the key component in generating trust in modern "information relationships."

Could this be a serious option for privacy reform in future? Time will tell. But I would challenge all of us to start thinking differently if we are to meet the modern challenges confronting us. We are compelled to do so if we desire to foster innovation that can benefit all of us. And those benefits can only flow if the public has faith and trust in the ecosystem which potentially gives rise to them.

Thank you, Greg and Christine, for inviting me to speak with you today. Hopefully we will all be back together in person next year. I welcome any questions you might have.