Ron Kruzeniski:

In Canada, it's Privacy Awareness Week. And I'm particularly pleased to be talking to Michael Webster, who is the Privacy Commissioner in New Zealand. Welcome to Canada, Michael.

Michael Webster:

Kia ora, Ron, thanks so much for the welcome and for having me on your podcast.

Ron Kruzeniski:

Now, before we talk about some issues of legislative change, I wonder if you'd tell us a bit about yourself, how you came to become the Privacy Commissioner, and most importantly, what you think Canadians should know about you.

Michael Webster:

Thanks, Ron. It's been almost two years that I've been in the role now, I started in July 2022. And before that I spent many, many years, Ron in the New Zealand Cabinet Office, part of our Department of the Prime Minister and Cabinet. So at central government, federal level, where I was secretary of the cabinet and clerk of the executive council. And in that role, I guess I had two main areas of focus. First as the principal adviser to the New Zealand Prime Minister of the day on the running and operation of government. So I was a political public servant. And second, the adviser to the governor-general in office, and the prime minister on the exercise of their constitutional duties. So absolutely privileged to do that role.

And the interesting thing, Ron, about that role is that it was all about being very clear about expectations, about guidelines, and providing advice within that context. In New Zealand we have something called the Cabinet Manual, that is the guidebook, the rule book in a sense for how government runs. And it was my central role to apply that in a day-to-day setting. And the interesting thing about that is that the New Zealand Privacy Act, our legislation, is of course based around and has at its heart 13 information privacy principles, which are principles which have a degree of flexibility about them. And so I am used to and enjoy working in that environment where context is important, where things aren't necessarily completely crystal clear, where you need to apply the existing guidance and rules to the situation that you face. And so there was a natural attraction when this opportunity came up. And I was looking for, as you do from time to time, Ron, when I was looking for new challenges after eight years doing that role.

Ron Kruzeniski:

So, to help Canadians, how would you describe the mandate of your office as Privacy Commissioner?

Michael Webster:

We are an independent crown entity, which means we are at some distance in terms of government control. Yes, we are centrally funded out of taxpayer revenue. So we do rely on the government setting our budget every year. Yes, we are monitored in terms of our performance by a central government department, the Ministry of Justice, which is actually the department responsible for privacy policy and regulatory change, but we are very independent in how we go about our role. And we have for a team of about 50 people, Ron, a very broad mandate. The New Zealand privacy legislative framework applies to all government agencies, the entire private sector, so from the corner store to the major listed company, the non-profit sector, schools, hospitals, churches, and even to some extent intelligence

agencies. So an enormous field on which to play. And there are some interesting aspects of our legislation. One of which caught my eye when I started was that in carrying out my statutory functions or duties, I need to have regard to government and business being able to achieve their objectives efficiently. So there are a number of kind of pointers in the legislation about how I should go about my role as well as, I guess the ambit and the extent of it.

I guess, Ron, like a lot of privacy regulators, we have some standard functions and some additional ones on top. So we do investigate complaints by individuals. Since 2020, we've had the responsibility with a mandatory serious breach reporting regime to investigate and look into privacy breaches by public and private sector. But we also do a lot of work on responding to government policy and legislative proposals that have privacy implications. And increasingly we're providing more, I guess education products, more guidance and advice which relates, I guess in many ways to the increasing focus of the office.

Ron Kruzeniski:

So you were appointed in 2022. And like many of us, I'm curious, did you set for yourself a series of goals or priorities for your term? And since you're two years in, have you achieved all of them, and how many more would you like to achieve before retirement comes your way?

Michael Webster:

We are in the middle of a pretty ambitious work program, and I was appointed for a five-year term. I would like to think that we've made significant progress against, I guess what I'd call my strategic priorities in that time, Ron, but time will tell. We've started with, as we say in New Zealand, a hiss and a roar. I have, I guess three main, what you might call polestars for me in doing my wrong. First is when I arrived here, we were in the middle of looking at our strategic priorities, our strategy, and I said for me, the change I want to see in New Zealand is privacy being treated as a core focus for agencies, not just some add-on where the board of directors gets a report once a year, where the CE doesn't really care, that it's a core focus as much as say, health and safety or good financial reporting is for organizations these days.

So that was the first polestar for me, privacy as a core focus. Second, I wanted to make the most of what I call the privacy ecosystem. And I can talk more about that. And the third was the old saying, building the fence at the top of the cliff and not just being the ambulance at the bottom. I want in New Zealand to be the regulator that sets the expectations, provide the guidance on good practice in such a way that actually my teams that deal with breaches, my teams that deal with individual complaints, end up having less to do because agencies are taking privacy much more seriously.

Ron Kruzeniski:

So you've got about three more years to go?

Michael Webster:

That's right

Ron Kruzeniski:

Now, and I think this is where I first caught attention, it was an article back in December where you gave a briefing to the Minister of Justice and aligned a series of priorities or policy changes that you wanted

to see. And I just wondered if you could elaborate the important things that you were able to brief the minister on in that process.

Michael Webster:

What I wanted to do for the incoming minister, Ron, was set out some context about the nature of the privacy environment. And I mean, you can bury people in statistics, but just your audience might be interested to know that year on year we've had a 79% increase in complaints and a 59% increase in privacy breach notifications. So our stats, our work are going off the charts. And so I wanted to be very clear with the incoming Minister of Justice, and with the officials who advise him, that actually concerns about privacy, complaints about privacy, risks to trust in government, risks to businesses from breaches are a significant and increasing factor. And I also wanted to set out for the minister, Ron, that all around the world, and I think of our cousins in Australia across the Tasman Sea there and in other places, governments are looking at their privacy regulatory frameworks because, I guess of the increasing digital innovation we are seeing, and because of the increasing voice from citizens about wanting their rights protected, those sorts of things. We've had a number of surveys done here in New Zealand which show that people are increasingly concerned about their right to privacy, they're increasingly concerned about their personal information being protected by the agencies that hold it, being respected by the agencies that hold it.

And so Ron, we also advocated, as a result of that, for legislative reform in a number of key areas, such things as introducing in the New Zealand regulatory privacy framework a right to erasure or right to be forgotten, a greater civil financial penalty regime for major non-compliance, a what you might call an accountability principle that you see in other legislative frameworks, so agencies required to demonstrate how they're meeting privacy requirements, and some other changes around ensuring greater transparency and protection in relation to things like automated decision making. So happy to talk bit more about those, Ron, but those were the main areas that we are focusing on at the moment.

Ron Kruzeniski:

So out of those, are you assuming or hoping a number of them get turned into legislative changes?

Michael Webster:

Well, what we have actually right now before the New Zealand Parliament is a change that has been in the works for a while around introducing a further information privacy principle in New Zealand about indirect notification, a bill, that if passed, will mean that individuals will be notified when an agency collects their personal information indirectly through a third party, with obviously some exceptions. So the government does actually have a legislative initiative underway at the moment, which we support as an office. And that's good, but we want more. And I guess if I think about the work that we've done recently on children's privacy, the right to erasure, the right to be forgotten, a right that exists in a number of regulatory regimes in other countries, became a particular focus for the people we spoke to. People sometimes do things they regret, and forever their lives sometimes are affected by the digital record that's been left there. And so we are strong advocates for that.

I think the one that is probably the most central though is the civil financial penalty regime for major non-compliance. I'm not sure what your financial penalty regime is like where you are, Ron, but in New Zealand, even when they updated the act in 2020, they didn't introduce such a financial penalty regime. There are some small fines of trifling amounts of money for people who don't meet some of the statutory requirements under the act, but if there's an egregious or serious breach or repeated failures or breaches of privacy by agencies, I don't have the ability to impose a significant financial penalty on

companies and agencies. And they know they're wrong. And so therefore in some cases they're responding to that by, when I insist that they change the way they're doing things to improve their privacy practices, there is a bit of, "Make me," going on, you need, you need a bit of stick with your carrot, Ron.

Ron Kruzeniski:

So in Canada it's a bit of a patchwork, a number of the commissioners, and we're a federation with the federal government and 14 provinces and territories, for example, Ontario has gotten the right to administer some financial penalties, but I think we're just getting into the game. When I see the headlines, certainly Europe has gotten into the financial penalties in a big way, and some of them are pretty hefty too.

Michael Webster:

Yes, that's right, and do they get paid or do they get caught up in endless court appeal systems as well, Ron? I think you need to look at that. I'm not asking for that kind of thing. What I'm asking for is something that's proportionate to the other financial penalty regimes that exist in consumer law in New Zealand, so something that's fair and reasonable, but will make those at the top of the organization, will make those that sit around the boardroom table, sit up and pay attention to the fact that they have let people down, they've let their organization down by not taking privacy seriously.

Ron Kruzeniski:

And I think another article that caught my attention, in April you started a consultation, and your office has drafted some biometric data guidelines dealing with facial recognition, fingerprints, etc. I'm curious what motivated you, first of all to develop the proposed guidelines, and then secondly, the motivation to have a public consultation and get feedback. I'm curious in this whole area, and obviously it's an important area in Canada in terms of biometrics and the issues that arise in this particular area. So what caused you to get on this track?

Michael Webster:

So of course Ron, we're talking about things like iris scanning, fingerprint technology, voice recording, that sort of thing. And currently the Privacy Act does regulate the use of personal information. So it does regulate to an extent the use of biometrics, but we have increasingly noticed that in other countries there are particular rules, particular regulatory regimes that govern the use of biometric technologies. And it became clear to us as we spoke to New Zealanders, spoke in particular to the Indigenous First Nations people of New Zealand, Māori, that they saw that New Zealanders see their biometric data and features as a very special type of personal information that needed greater protection under our privacy regulation. What we are seeing increasingly also in New Zealand is businesses in particular thinking of new ways of using biometric technology in all sorts of settings. And we realized that we are at risk of the wholesale expansion and use of this technology in a way where there hadn't been a national conversation about what it means, the risks around it, the risks, for example of mismatches, if you're using it for example, for identifying people, the risks of bias, all those sorts of issues were of concern to us.

Ron Kruzeniski:

And the public consultation has started?

Michael Webster:

Yes, it has. In fact, what we did was that we went out and said we're thinking about introducing under our Privacy Act a further level of regulation called a code of practice, which amends how the information privacy principles apply and gives us potentially more or different kind of tests for us to hold agencies to account in relation to the use of biometrics. And so we went out first and said, "What do you think about that?" And people said, "We think that sounds like an interesting idea, you should explore it further." And we thought so too. And so, we've now just issued what we call an exposure draft of such a code of practice. And if the feedback we get from that, and if our analysis and thinking continues, the option is before us to then proceed to formally draw up a code of practice and consult formally on that under the provisions of our New Zealand Privacy Act, and then that would come into effect and become, I guess a new layer of regulation for agencies to have to follow.

Ron Kruzeniski:

So on the consultation part, do you do that because of the education value, or there's some requirement in your act that before something becomes law, you have to consult?

Michael Webster:

Absolutely. So the formal consultation is a requirement in our act, because we are in a sense altering the provisions of the act. It's quite an extraordinary power, this code-making power. And so it's good practice that New Zealanders, agencies have an opportunity to see what's proposed, an opportunity to have some input to that. The reason why we've gone out for what you might call an informal level of consultation before that, is that we're concerned to both hear again what people think of our proposals and to ensure we get it right basically. We want this to work for agencies, we want this to work for business, but we also want it to address the increasing level of concern we hear and see about the use of biometric technology.

Ron Kruzeniski:

And this is totally an aside, but prior to coming on to do this podcast, I was reading a headline, and the announcement in the United States is that they are expanding their facial recognition program to some 400 airports. And it just made me realize that this whole biometric technologies thing is, well, growing at a rapid rate. And I haven't read, and I should after this, go to your website and take a look at that code of practice and see how we might make it applicable here in Saskatchewan or in Canada.

Michael Webster:

Yeah, look Ron, a couple of comments on that. Of course, central government can pass legislation to override provisions of the Privacy Act, and that's what happens with areas such as border security and customs, immigration, all that sort of stuff. So of course governments use biometric data for national security and safety reasons, those sorts of things, and we understand that That said, the code will apply to everybody, unless they have a legislative override. Second, there are in this side of the world, and I'm sure the same in Canada, in your province, increasing numbers of sophisticated cyber-attacks, cyber hacks happening on organizations. And significant amounts of personal information is being exfiltrated, companies are being held to ransom through the use of ransomware, or data is being sold on the dark web. Now, if you lose your, let's say your driver's license, your car license details, it's irritating, but you can go and get a new driver's license with a new number, if you see what I mean.

Ron Kruzeniski:

Yes.

Michael Webster:

If biometric data is exfiltrated, your iris that someone's captured in a digital reading, your fingerprints, you have in a sense had something that is irreplaceable stolen and monetized on the dark web by criminals. It's a serious matter, and I want agencies to take the collection and the care stewardship and protection of biometric data much more seriously and harden their systems against the increasing sophistication of the cyber criminals out there.

Ron Kruzeniski:

So Michael, getting close to the last question here, and this is, I hope a rare opportunity, what advice in the privacy field would you have for Canadians, or more particularly for your fellow commissioners up here in Canada, what do you think we should be doing better or what are we doing quite well?

Michael Webster:

Yeah, yeah. Well, we are in the middle of getting ready for our Privacy Week that's coming up, Ron. Our Privacy Week starts next week, and it's got the theme of busting privacy myths. And one of the myths that I'm keen to bust is that our citizens don't care about privacy anymore, because they live their lives digitally, they live their lives online. And therefore because they do that, they don't care. Actually, they do care. And increasingly because they live their lives in that digital environment, they care that their privacy is being protected and respected, they care that their personal information is being held securely. And what I want is to, I guess respond to that increasing level of concern. My advice to people is to keep a weather eye on certain things, and it's not as they are now, but it's how they will be in 10, 20 years time.

And I'll give an example of that. The use of AI is a thing. Tech companies, digital innovation, those sorts of things, very powerful tools right now. Can we imagine what they'll be like in 10 to 20 years time when they're applied for business purposes, for government purposes against datasets of personal information, that sort of thing. So it's the risk. I don't want us to be the frog slowly boiled in the pot as the water heats up kind of thing. I want us to be conscious now, and we need to be thinking regulatory frameworks, safety for our people in the future now, because it takes quite a while, obviously for some of the changes we might want to bead in. So that's my first concern, not as things are now, but how they could be in a few years time.

Second, and it relates to that, increasingly there's lots of talk about the value from government-dataset integration, the growth of giant government and company data warehouses, that sort of thing. And in some ways, disparate and decentralized holdings of personal information does provide some protection to people. When it gets aggregated together into huge data warehouses, into huge datasets, if someone can get hold of that, if it's accidentally leaked, you don't just lose a little bit of who you're as an individual, you can lose everything, not just your health information, but say your financial information, other personal information, justice-sector information, all that sort of stuff. And so I am increasingly concerned about ensuring that the debates and the public policy reasons for the creation of giant data warehousing initiatives have privacy at their core as well.

Ron Kruzeniski:

And those are certainly the things that some Canadians and all Canadians should really be concerned about. So very similar concerns in my daily reading. I read headlines about AI, and I cannot conceive where we're going to be in 10 or 20 years, it just blows me away. Well, finally, in preparing for this, I

found out that you are going to receive an honour shortly from King Charles as a Commander of the Royal Victorian Order. And first of all, congratulations on that.

Michael Webster:

Thank you, Ron.

Ron Kruzeniski:

And I understand you're heading to England in June for the investiture ceremony, and that's terrific. And I really need to know, so what privileges comes with this particular honour?

Michael Webster:

Thank you, Ron. Yes, we're off to actually Windsor Castle for the investiture ceremony. So of course you get the insignia of office, which is a lovely tangible acknowledgement, I guess, of the honour. In many ways, the honour reflects, as honours often do, the work of the incredible team that I had behind me that helped me contribute to the reasons why I got the honour. And in my previous role, Ron, just so you know, one of the other things I did as clerk of the executive council was look after matters royal for New Zealand, because we of course have before, of course, Queen Elizabeth II as our head of state, now King Charles III. And over the years I arranged, I think, or oversaw, seven royal visits to New Zealand, which was a delight, but also quite a privilege, but had a good team behind me.

As to what goes with it, I did find out, because of course you get this information, Ron, that we have a home chapel for the Royal Victorian Order. It's the King's Chapel of the Savoy. And so, one of the things I intend to do, Ron, is as we are arriving of course in London and before we go to Windsor, is to go and have a look at this chapel and just see what it's like. Apparently, if you're a member of the order, you can have weddings or baptisms and things like that there. So that's a lovely privilege, I guess.

Ron Kruzeniski:

So no family members wanting to get married, or no grandchildren coming where you need a baptism?

Michael Webster:

I think if people made the decision to go to the UK for that, rather than have it in the beautiful land of Aotearoa, New Zealand, there would be some family members and friends who might be a little bit put out, Ron.

Ron Kruzeniski:

So in one of your emails you said to me, and by the way, the honour can be awarded in Canada, which was total news to me. So earlier today I met with the federal provincial Commissioners in Canada, we have monthly meetings. And I certainly told them that maybe one of them potentially could receive the honour. So who knows, there may be a Canadian in the order one of these days. But with all seriousness, congratulations.

Michael Webster:

Thank you, Ron.

Ron Kruzeniski:

And the fact that you're receiving it in Windsor Castle, I think is really exciting and interesting. And I hope someone in your family can run their iPhone or video camera and capture it all digitally for you. Well, have a safe trip and a great trip. And I really want to thank you for taking the time to chat with us today. And what blows me away, but it shouldn't, is just the commonality of the issues, the things that you're talking about, that we talk about here, that some of which we talked about on our federal provincial monthly call today. And my guess is, if I was talking to someone from Australia, I might hear similar types of issues being raised. So besides all the other common bonds we have, like sharing a king, we have a series of common issues in the privacy world. So thank you very much for taking time to talk to me today.

Michael Webster:

Thank you, Ron. And just on that, I and my office benefit greatly from also looking at the regulator websites in other countries, including of course Canada as well. There is a really good network amongst the Asia-Pacific privacy regulators, and we do share initiatives, ideas, advice, concerns, what we're seeing. And increasingly, I think with multinational companies operating in that space where they're using a lot of personal information, collecting it and processing it, increasingly, I think regulators around the Asia-Pacific region and beyond will need to work more closely together. So it's been a delight to speak to you, and I will look forward to keeping an eye on your website about the initiatives and things that you're doing, as well as your colleagues in Canada.

Ron Kruzeniski:

Well, thank you very much, Michael, and safe travel in June.

Michael Webster:

Thank you, Ron.