Transcript Episode 6 Michael McEvoy

Ron Kruzeniski:

Today I have the pleasure of talking to Michael McEvoy, who is currently the Information and Privacy Commissioner in British Columbia. Just to tell you a little bit about Michael, he was appointed to this position in 2018. Prior to that, he had been deputy Commissioner since about 2013, had an opportunity to spend six months in England. And if you ever get to hear his presentation on his experiences there, it's really worth listening to, and he's very proud of the jacket that the Information Commissioner of England gave to him. And really notable. You can learn more about Michael by checking on the BC information privacy commissioner website. But of note, there he is a charter member of the Grey Leafs Seniors Hockey team. Now, we're not going to talk about hockey today, although it's Canada's favourite sport. We're going to talk about some access and privacy issues. For those who have not been following BC media, the Parliament there has passed Bill 22, which is a bill that has an impact on freedom of information and access to privacy in British Columbia. Michael, what was the main thrust or main purpose of that particular bill?

Michael McEvoy:

First of all, Ron, thanks for having me and thanks for not wanting to talk about hockey. I'm smarting a bit of a bruise in the back of my leg from yesterday's performance, so I don't want to get into that too much. But I really appreciate you as a colleague, and again, thanks for having me as part of your podcast.

Yes. So Bill 22, which was introduced in the fall of last year, just a few months ago, was the first really significant reform to our Freedom of Information Protection and Privacy Act in, I was going to say a decade, but even a decade ago, those changes were in the whole scheme of things, fairly minor, really since the act was brought into force in 1993. This is the most significant reform that the bill has undergone. So in general terms, it's introduced a number of modernizations, especially on the protection of privacy front, protecting the citizen's information that's held by public bodies. There were a number of changes made that we can get into and talk about, but those are actually very welcome, ones that have been advocated by our office for a number of years, and we were pleased the government moved forward with.

There were also changes made on the access to information side of the equation, and I was very public in the concerns that I expressed about some of those changes that were made including a fee for access to information, again, which we can talk about in a little more detail, as well as the government taking out of the scope of the act, access to certain records. In other words, certain things that were once known as records for access were no longer considered to be accessible. So that in broad terms is what was introduced a few months ago. And the bill which has now been passed, though not everything has been brought into force, most of it has been, there are some items that have not been brought into force. And again, we can talk about those.

Ron Kruzeniski:

You've partly answered this, but I was going to ask whether there was four or five items in the bill that you were particularly pleased with. Is there any others that you haven't mentioned that you were pleased with?

Michael McEvoy:

Yeah. So I think some of the advances I hope serve as an inspiration to other governments across the country. There is a requirement now, and will be a requirement, actually this is one of the things that hasn't been brought into force, but it will be in the coming months, is a requirement for public bodies to develop and put in place privacy management programs. So, I think any public body, even private institutions now that think about these issues in a thoughtful and a significant way, probably will have thought through privacy management programs already, but there are many that have not. So this is really important. It will become a legal obligation. So, a privacy management program would have to address a whole range of questions. Public bodies will have to take a thorough inventory of all the personal information that they handle from citizens, to think about who's got access to that information. And also, if things go badly, and many say it's not a question of if, it's when a breach might happen, how one would handle those in that situation.

That leads to another requirement that is now in the legislation, which is a requirement that public bodies have to report breaches of their data, where those breaches pose a real risk of significant harm to individuals. So they are going to be required to report those to me, depending on the situation, required to report those to the individuals who have been affected. So that's a step forward. That's another provision that hasn't yet been brought into force but will be in the coming months.

Other things that have been added, it is an offence now for people to, it's called snooping often, where people will look at other people's records. They shouldn't be, it's not for the purpose of work, it's because they're looking at an ex-spouse or somebody that they're in a dispute with or something like that. A totally inappropriate access to the information of individuals done by somebody in a public body, that will become an offence now under our Offence Act in British Columbia. And that's I think a good step forward to send a signal that that kind of activity is not just frowned upon, but in fact comes with a penalty.

I guess the other thing that I would just mention, and I think is very positive is I would say a sweeping requirement right across the board that all public bodies have to conduct privacy impact assessments when they're developing new activities or programs that involves the personal information of citizens. I mean, that's something I think most good public bodies and even private institutions to think about, but if you haven't done it in the past, you will now be required to do that in the future. So those are, I think, about four changes I think on the protection of people's information side, I think, that are very positive.

Ron Kruzeniski:

So, you mentioned earlier fees, and I was going to ask you about changes that you have a little bit of a concern about, but on the fees, is it mandatory that they charge a fee or discretionary?

Michael McEvoy:

So, it leaves it now, the law, as it's worded, permits public bodies to charge a fee of $10 for what would be called general information. So information that you seek about yourself. So I have a file with say, a Ministry of Children and Family. I want to get more information about that. It's about me. There will be no charge for that. But if I want to find out about how my government or health authority is doing with regard to COVID restrictions, or I want to find out how decisions are being made about COVID matters, I would be charged a $10 fee if I'm going to a public body or certainly British Columbia government public bodies. So a ministry, for example, would charge $10.

It leaves an open to other public bodies, school boards, municipalities, all those kinds of institutions about whether they would like to charge for those. At this point, we haven't heard of any of those public bodies instituting the $10 per application fee. And I have certainly been saying publicly that I would not

encourage any of those public bodies to consider implementing the fees because I believe they are an impediment and an obstacle to accessibility and accountability of our public institutions. But it does leave the door open to every public body to charge $10 for FOI applications.

Ron Kruzeniski:

You also mentioned that they sort of changed the rule on the access to certain documents. What kind of restrictions are there?

Michael McEvoy:

So couple of things that they've done is that if an employee of a public body deletes records that they can no longer retrieve, so if depending on the system, if it's double deleted or whatever and goes into the public body sort of system archive as it were, but the individual cannot access it, that record is now considered not FOI-able, which in the past, those records, if somebody made an access request for records that what would be called stored on a server, you wouldn't necessarily get access to those, you would have to demonstrate some good reason why and there would be some issues around the practicability of getting access to those records. But in some cases, it would be important to have a look to go into the backup records to get that information. That was a discretion that my office had, to be able to order that. I have now no discretion. Those records are out of bounds insofar as FOI applications are concerned, and that I don't think is a good step.

One of the other things that they've now taken out of the scope of the act is so-called metadata. So this would be data about data. In the digital world in which we operate on, as you are well aware, some of that data can be really important. So it would track a record, for example, who edited a record, when they edited a record, the kinds of work that went through many drafts. That you can tell from looking at metadata, it can be important information. And for reasons that are not entirely clear to me, the government has determined that metadata is not something that should be subject to FOI, and therefore has been put outside the scope of the legislation, so that my office did not think was a positive move and I don't think adds to public body accountability.

Ron Kruzeniski:

Were there any other changes that you had concerns about? Or have we flagged the main ones that gave you concern?

Michael McEvoy:

Well, there was one thing that really jumped out at everybody at the very outset of the changes that were made, and it appeared to remove the Premier's Office from accountability under the act. I pointed out that this, at the very least, could create confusion and ambiguity about whether the Premier's Office was covered. To the government's credit, they responded to that and said yes, they would make absolutely clear that the office, the Premier, was covered by the legislation, and so they bonded to that.

Other changes and significant changes were made around data residency. British Columbia was unique in Canada in the sense of prohibiting disclosure of people's personal information outside of Canada by public bodies, although that was subject to certain exceptions. Nova Scotia had something of a similar rule but not quite as stringent British Columbia's. That over time came under a lot of criticism from universities, health care, authorities, and so on who wanted access to, particularly US companies, platforms, servers that were in the US that could provide, they would argue, state-of-the-art services and so on. That was made very difficult by the provisions of our act. And the government responded to

that by essentially removing the prohibitions on the storage and access of people's personal information outside of Canada.

They put a little bit of boundaries around it if the information and questions considered sensitive personal information, that the special PIA has to be put together to address issues about where the information is and what measures are being taken to protect it. But my view is, look, anytime you're going to be sending information anywhere to begin with to a third-party company, whether it's in the US or Europe or anywhere else, public body needs to consider the jurisdiction to which it's going. That just to me is just common sense, and you need to put your mind to that to determine whether you have proper measures in place contractually with who you're dealing with.

But also, you need to think about, say the jurisdiction of which it's being stored. I don't think British Columbians would be particularly comfortable if that information were being stored in Russia, for example, or some other country when you think about the kinds of protections that are in place in these other jurisdictions. So in any event, long and short of it is, even though the restrictions have been lifted on storage and access outside of Canada, public bodies still must put their minds to ensuring that that information is properly dealt with when they do send it to companies outside of the country.

Ron Kruzeniski:

Really, that should be done whether it's sent to a server a block away from their office.

Michael McEvoy:

Absolutely right, absolutely right.

Ron Kruzeniski:

So, sort of at the same time, but on a different track, you had a special parliamentary committee that was looking at PIPA, which is your private sector legislation, and really quite shortly after Bill 22 got passed, their report was released. And I'm curious whether some of the features that you found really helpful or encouraging in that committee report.

Michael McEvoy:

There are a number of features that are encouraging about the report of our private sector privacy law. Once again, it's legislation that came into force 2004, and it has not really received any reform since then. And, of course, the world has changed a lot. Facebook was just an operation in Zuckerberg's dorm room, I think at the time that the act was brought into force. The world has changed a lot. So that requires our laws to move in sync. I think the committee, the special committee of our legislature looking at that, recognize that fact. They looked at what was happening in places like Europe with the general data protection regulation, changes that were happening across our own country and as well as other places on the globe, and realized that British Columbia really, it's important that we're in step for a couple of reasons, in step to ensure our citizens are properly protected, but also to ensure that our businesses are on a level playing field with those across the country and those globally.

Innovation and all of the things that come with technologies in particular are really important to the economy. And we want to make sure that the people who are doing that innovative technology well are supported and protected, and that the laws are in place that are going to make sure that those who want to be bad actors are properly dealt with. So the committee has made a number of recommendations that I think are positive and, if they're brought into place by the government, will keep us aligned with what is happening across the globe.

Ron Kruzeniski:

Was there any recommendations that stand out there that you particularly liked?

Michael McEvoy:

Yeah, no, absolutely. I talked about mandatory breach notification in the public sector. We don't have that here in the private sector in British Columbia, which I think still surprises a lot of people. But the recommendation by the committee is that breach notification be made mandatory by all organizations, where that breach poses a real risk of significant harm to individuals, to report it to me as the commissioner, but also as importantly, to report it to individuals who may be harmed. One of the other things that the committee has recommended, and I think this does, if implemented, keeps us in lockstep with what's happening in developing globally, is the role of our office to impose significant penalties where organizations are misusing or abusing people's personal information. And I think that's really critical, that our office have the power to levy administrative monetary penalties. It exists in Europe, it exists in other authorities. Quebec now has that authority. Canada is kind of moving along at a bit of a glacial pace in that regard, the federal government. So we hope they will follow what is clearly a global trend.

I think one of the other aspects that the committee recognized, and I think the legislation has to as well, is the importance of meaningful consent to ensure that individuals understand how organizations are collecting and using their personal information. So often we run into these things where there's pages and pages of legal lease where people really don't fully understand or comprehend how their information is being used. And these companies in turn rely on these tick boxes that an individual might make to saying, "yeah, I'm okay with that," when really there's no meaningful understanding. So, it's really important that the law ensure that when it comes to the issue of consent, that it be clearly stated on the part of organizations and that it be clearly understood by the individuals at the other end of the tick box. So those would be, I think, a few of the things that stand out in terms of the recommendations that I think if government implements will be very positive for citizens and businesses both.

Ron Kruzeniski:

Now I know you made the presentations to that committee. Was there anything you would've liked to see as a recommendation that they didn't put in the report?

Michael McEvoy:

Well, there are a few things. To the committee's credit, and this is not really a criticism of the committee, things are moving at a very rapid pace in the world. So keeping up with everything that's going on and being rate on the cutting edge of things sometimes is a bit of a challenge. But I think a few things that we could benefit by in British Columbia, and that, for example, would be my office had the ability to impose codes of conduct.

These are really flexible tools that rather than having to wait for the legislature to deal with such and such a technology and change the laws, that there be some code making ability within the purview of my office, a regulator's office. This is something that exists in other parts of the world, Australia, for example. So having the ability to create codes of conduct I think would be a very positive, and it can be very targeted within specific industries that have their own particular foibles. So it allows for a targeted protection and set of rules. So codes of conduct I think would be something that could be permitted under legislation that would be I think very good.

The issue of children's privacy has very much come onto the front burner, I think across the globe. I think one would look at the UK's approach to this issue, and I think there's some wisdom in some of the steps they've taken. I think that's a matter that I think legislators should consider. And there are certain uses of personal information that maybe should just simply be no-go zones in terms of use of information by companies or organizations. I think certain biometric identification systems, for example. I would think of, for example, the social credit systems used in China as a way of denying or giving people access to public services based on computerized algorithmic functions, geolocation functions, and so on.

I think as a society, I think we have to ask ourselves, are these places we want to go? It doesn't matter kind of how much consent might be involved or whatever, it's a place where we shouldn't be going at all. I think that's something that I think we need to be thinking about going forward. So those would be I think some of the issues that I think the government should consider as they move forward to develop legislation.

Ron Kruzeniski:

So, you have a report of a parliamentary committee, and I presume at some point it gets into the government thinking tanks. Do you have any idea as to how long you might see some of this turned into legislation and back in the house?

Michael McEvoy:

Well, as much as I'd like to forecast these things, I think probably your own experience at Saskatchewan would tell you that it's a bit of a fool's game to start making these kinds of predictions. I mean, governments, of course, at one point they may say things are a priority, but then suddenly other crises arise and suddenly it's not a priority anymore. I really hope that within the next, I'm hoping the next year and a half or so, this will come on to the front burner because it's really long overdue. We've had some indications from government that this is something that is important and that they would be prepared to move forward on.

Our office will be certainly there and will be working with them to assist them in that way to develop legislation. But yeah, I've got a couple of years left in my term, just over a couple of years left, and one of my main priorities is reform. We've had some reform on FOI front. I still think there's some work to be done there, but the other major element of reform is here in the private sector, and I really want to accomplish that before I complete my time here in British Columbia.

Ron Kruzeniski:

Well, and I hope you're successful. Okay, I belong to an organization in British Columbia, part of the private sector there, or a Saskatchewan organization, and I want to do business in British Columbia or already doing business. Should there be anything that I should start preparing for either now or getting it into my goals for the next year? Anything organizations should be doing based on all that you think could be coming?

Michael McEvoy:

Yeah. So, I maybe would divide this up into two in terms of organizations. One would be private organizations. The law has not changed in respect of matters like mandatory breach notification, but you should be gearing up for that. And in fact, more than gearing up for it. As a practice, it is very advisable where you have breaches that are affecting your customers, your clients, your patients in British Columbia, you should be reporting that to my office. We do get quite a number of reports, not

the number we would get if it was mandatory to do so, but we do. I think that's really, really good practice for businesses to do that.

This is not a gotcha exercise. It's not something where you get punished. We have experts in our office who can help guide organizations, especially small and medium enterprises who may be not quite sure about how to find their way through these kinds of crises. We have people who can help, and we do this every day to assist in stopping the breaches, sitting down to talk about whether people have to be notified of the breaches and so on. Again, not a gotcha exercise. We're there to work with and assist these, again, particularly small and medium-sized enterprises with those kinds of matters.

On the public sector side, well, again, breach reporting will be mandatory shortly. So getting ready for that is really important. The privacy management programs, getting ready for those, preparing those, that's something we can assist with. I guess one of the most significant changes, as I mentioned earlier, is now there is an ability for public institutions, if you're a school board or you're a health authority, to now store that information, to have it sent outside of Canada to utilize some of these other big tech tools that maybe they couldn't do that in the past, but you need to do it in a responsible legal way to ensure that information is properly protected. So public bodies will be absolutely preparing for that now. In fact, many of them are going through this process. And again, our office is here to help as they think through those issues and ensure that the personal information of British Columbians is properly secured when it leaves their servers here in British Columbia.

Ron Kruzeniski:

So, I've listened to this podcast, and I say I need to find out more. Where would you suggest somebody, citizen or organization, start in terms of learning a bit about Bill 22 or learning something about the recommendations that the special committee put forward in its report? Where'd be the best place for them to start?

Michael McEvoy:

Well, I can think of no better place than our own website here at the OIPC in British Columbia. So if you just Google OIPC BC, you will get to our website. The long version I think is www.oipc.bc.ca. That'll get you there. But again, just Googling our office will get you there. It's a very good summary of the bill and its implications for public bodies and for citizens. So that's a great place to start.

Ron Kruzeniski:

So, Michael, I want to thank you for taking the time today to record this podcast. I know you're probably dying to get out into the rain in Victoria, so I should let you go. But, thank you very much for the preparation and the time and for your advocacy on behalf of all the access and privacy commissioners across Canada. Thank you for your dedication.

Michael McEvoy:

Well, thank you for having me on this podcast, and thank you for your work in Saskatchewan and the work your office does to serve the citizens of your province. It's extraordinary. I certainly have valued the work that we do together as colleagues. And again, really appreciate this opportunity, Ron. Thanks.

Ron Kruzeniski:

Thanks, Michael.