OSLER

Canada's new privacy legislative reform

JANUARY 13, 2021 110 MIN READ

Related Expertise

- Privacy and Data Management

On November 17th, 2020, the Federal government introduced a Bill, entitled the Digital Charter Implementation Act, 2020 (DCIA), proposing significant change to the national framework for the protection of personal information in Canada. If passed, the Bill would establish a new private sector privacy law in Canada, the Consumer Privacy Protection Act (CPPA), and a new Personal Information and Data Protection Tribunal.

The Osler Privacy Team is offering a series of events and resources to help you prepare for the impact of the proposed legislation on your operations.

Webinar on Demand – Initial insights and commentary

Watch our special 1-hour AccessPrivacy webinar for an initial commentary on key features of the proposed new federal privacy rules.

AccessPrivacy Podcast: Reflections on Canada's proposed federal privacy law – The Consumer Privacy Protection Act

In our November 2020 AccessPrivacy Call, we continue our series on Canadian privacy legislative reform with a conversation with Professor Teresa Scassa, Canada Research Chair in Information Law and Policy, and Professor at the University of Ottawa, Faculty of Law, about key themes and features of the federal government's proposed private sector privacy law.

Your browser does not support the audio element.

Transcript

AccessPrivacy Podcast: Canada's new privacy legislative reform – a data litigation expert roundtable

In our December 2020 AccessPrivacy Call, Adam Kardash moderates a round-table discussion featuring Osler's data litigation experts and their insights on the enforcement regime set out in the federal government's proposed private sector privacy law.

Your browser does not support the audio element.

Transcript

AccessPrivacy Podcast: Canadian Privacy Legislative Reform – Key Issues and Considerations arising from the proposed *Consumer Privacy Protection Act*

In our January 2021 AccessPrivacy Call, Adam Kardash moderates a roundtable discussion with Osler subject-matter experts on a range of key issues and considerations arising from the Federal government's proposed *Consumer Privacy Protection Act* (CPPA).

Your browser does not support the audio element.

Transcript

Register for future AccessPrivacy Calls

Already registered as a member with AccessPrivacy?

Register for Upcoming AccessPrivacy Calls

Not registered as a member with AccessPrivacy?

Create a free AccessPrivacy account to register for events and our free e-newsletters. Once you are registered, click on the Events Tab to sign up for Upcoming AccessPrivacy Calls.

Transcript

AccessPrivacy Podcast: Reflections on Canada's proposed federal privacy law – The Consumer Privacy Protection Act

PRESENTER: All participants please stand by your conference is ready to begin. Good morning, ladies and gentlemen. Welcome to the AccessPrivacy monthly conference call. I would now like to turn the meeting over to Mr. Adam Kardash. Please go ahead.

ADAM KARDASH: Thank you. And hello, everyone. And welcome to our November monthly privacy call. For colleagues who are not able to join us today, note that all of our AccessPrivacy calls are incorporated under the Resources tab of our online platform for subscribers to listen to at any time at their convenience. And while we don't have an

opportunity to answer questions during the calls given the number of attendees, subscribers to the site can find more information on today's topics and many others in this month's monthly scan also available under the Resources tab, including our expanded legislative reform topic hub on our subscription platform.

This scan is intended to provide subscribers with a convenient one page snapshot to a consolidated list of hyperlinks to recent decisions, guidance, documents, and other notable developments that have occurred in the privacy arena together with easily accessible links all in one place to help keep you in the know and save you about valuable time.

So today we are privileged to be joined by Teresa Scassa, the Canada Research Chair in Information Law and Policy, and Professor at the University of Ottawa, Faculty of Law. Teresa is an expert in privacy law, a frequent commentator, very highly respected in the Canadian privacy arena.

And among her countless endeavors, Teresa is also just a driving force for a publication that AccessPrivacy puts out, Privacy In The Courts is a quarterly publication. It's a superb summary, a consolidation of privacy jurisprudence that have occurred over the last three or four months of each publication. I encourage you, if you haven't to take a scan at that.

We're going to pick up where we left off on this past Friday, and continue the discussion that we've been having about Bill C11, which is the proposed Consumer Privacy Protection Act or the CPPA. And Teresa, on Friday I provided a snapshot of the CPPA. It was initial reflections and comments on it. And for those of you who haven't had an opportunity to see where– didn't have an opportunity to attend, you can go on our site and we have the webinar on demand and accessible.

But Teresa, during that session I provided some initial thoughts and initial impressions. First and foremost, as you and I have discussed lots to digest here and it's early days. And we're continuing to really think about this.

The second thing that struck me as I'm continuing to go through this with the team here, continuing to have conversations with other stakeholders in Canada, it strikes me that it's really important to consider these rules which will be the guardrails for perhaps a year's. An Important set of guardrails for the knowledge economy. And as we do that, it strikes me as I have heard these discussions that we really need use cases, like very granular use cases, to ground much of this discussion.

But overall this remains in my view a thoughtful a proposed legislative framework. It takes elements of PIPEDA that has served us well, the balancing of interests of individuals, the protection of privacy for individuals, as well as the needs of organizations to process data. The rules appear generally drafted and principles based technologically neutral, sectoral agnostic fashion.

And it's founded on an accountability, a strength and accountability model, but an accountability model. And there's other features within the legislative structure, including a number of locations within the statute where there's regulation making power for which really contemplate details that would probably, would be best suited for a first, of all further discussion and consideration before they're put into a statute.

But also perhaps at least in my view best suited for that including the rules relating to data portability which safeguarding considerations, and interoperability considerations that we need to have addressed thoughtfully. There's breach notification content requirements and other examples. But I wanted to get your reflections and initial thoughts about this statutory framework. Can you share, can you share that with us and the attendees?

TERESA SCASSA: Yeah, sure and first let me start by thanking you for this invitation to be part of this conversation. I think you're absolutely right, there's a lot going on in this bill and a lot for us to be thinking about. And so you know I find it a real advantage to myself as well to be able to engage in conversations with people like yourself over what's actually happening in this bill.

I think that the federal government was doing two main things with this bill. One, was obviously it needed to be reformed, to be updated for the modern or the contemporary digital economy and also with a view to GDPR adequacy assessment. So there was a real need for major reform. But the second thing that it was doing with this bill was turning it into, taking it from that strange hybrid thing that PIPEDA was with the normative provisions at the end in the CSA Model Code as a schedule to the act and turning it into a proper statute.

And– and that had to be done. And I'm glad it's done. And I think it will be, I think it's going to be a very positive thing going forward. But the result is that it's as if we're confronting a new piece of legislation. And it's not that some of the provisions aren't familiar to us. It's just that everything has been changed sometimes in subtle ways that are hard to notice at first glance. So normally with an Amendment to a bill you'd have the new parts underlined or you'd be told specifically which provisions are being amended.

And really the whole bill has been rewritten and sometimes the language is the same. Sometimes it's slightly different and sometimes it's quite significantly different. And even in those slight differences there can be changes or nuances in meaning that have to be thought about. And so I think that what everybody in the privacy field is experiencing right now is the real challenge of looking at something like this and trying, you know we're all trying to get our heads around this in part because there's lots of new stuff in there.

But in part also because of the old familiar stuff may have been tweaked or changed in ways that we need to think about. And so it's enormously challenging. I mean I can mention some of the new things that are in the bill as well, which I think are very interesting. And I think where we see more rights of control for data subjects, for individuals in this bill, a la GDPR, but framed in it I think in a Canadian context.

So for example, there's going to be a data mobility, you know, there's a data mobility provision as you mentioned. This is one of the ones that's going to have to be fleshed out by regulations. There's a right of erasure for individuals who want to have an organization delete or erase the information that's been collected about them. And in the AI context, a right to an explanation, and a very interestingly framed right to an explanation. So there are new things like this in the bill.

And then there are things that we had before like consent, and I think we're going to talk in more detail about consent later on, but which have been tweaked. And I think in ways that may be quite significant. And so yeah, lots to, lots to think about in the bill.

ADAM KARDASH: Let's turn to one of the features that is really often the initial focus for good reason is the new enforcement regime. Potentially very severe monetary penalties depending on the particular offense, could be up to 25 million, or 5% of gross annual revenues. There's the private right of action. There's order making power. There's appeal rights which is really something that was noticeably absent albeit in a different type of regime. But PIPEDA, it's just not there expressly for organizations.

And this tribunal concept which among other things, it is going to have the power to impose the fines, the commissioner has the power to make a recommendation to the tribunal. At least my view very thoughtful and appropriate approach towards what could be potentially

very severe penalties. We've had some interesting discussions already you and I, Teresa, about this regime. Very interested in your thoughts and reflections at least as we're initially considering this key feature of the act.

TERESA SCASSA: Yeah, and you're right there's a lot packed in there. And I think there's going to be that whole section on enforcement is going to require a lot of thought and study by privacy experts. And I know that process has already begun. And people have been commenting on it. I mean enforcement, an upgrade to enforcement powers I think was inevitable in this bill partly because of GDPR, and partly because I think this had become a sore spot for it certainly in terms of public perception of PIPEDA.

And I think something that was a factor in undermining public trust that you could see things that were perceived as abuses of personal data take place with nothing more than you shouldn't do that, or stop doing it. And I think that there was a public sense that this wasn't enough. And so there's a lot more in this bill. And a lot more to sort through. There's a lot of things to think about I mean there are, for example, there's the potential for substantial penalties to be imposed.

Although those penalties are only imposable with respect to certain types of behavior. So it's not penalties with respect to any breach of the act but there are very specific breaches of the act. There's also a provision that the purpose of the penalty is to promote compliance, and not to punish, and it'll be really interesting to see how the imposition of penalties plays out. I mean it looks very significant, and there is the power there. I'm not sure that it's going to be one that's exercised particularly often. So it'll be interesting to see how that plays out.

I think that the tribunal raises some really interesting issues and some of the concerns that I've already heard being raised around the tribunal relate to its composition. Who's actually going to sit on this tribunal? What's their expertise going to be? How is this tribunal actually going to work? And so I think those are some interesting questions.

But a couple of the questions that jump out the most for me with respect to the private right of action, and here I think your thoughts and input would be really helpful, well one of the questions is, how do class action lawsuits fit with the private right of action in this bill? In other words, we've seen a lot of class action lawsuits over the last two years. The number seems to be growing with respect to data breaches or abuses of personal data. And so the class action lawsuit has become I think very common and very significant in the privacy context.

Personally, I don't think this private right of action is going to stop class action lawsuits but one of my questions is whether the private right of action for breach of PIPEDA could be a basis in its own right for class action lawsuits? Or whether that's simply not something that fits under the way in which the private right of action has been constituted in the statute? So that's one question and I don't know what your thoughts are on that, Adam.

ADAM KARDASH: Well, there's two thoughts. One is, it goes back to the initial comment that both of us has made. There's a lot to unpack and a lot to consider. What struck me in terms of this statute looking at this regime is that you have a new set of rules, many of them are similar, some are new. They effectively set a new standard. And as exactly as you mentioned, it doesn't seem that this is going to do anything to preclude the commencements of civil proceedings based in part on the standards set out in PIPEDA, like divorce from this private right of action. And other common law claims that are very, very common when you read statements of claim.

And so it seems to me that, that will continue. And I do highlight it's a perfect segue. We're working right now with our colleagues in the litigation team, and doing a deep dive on this.

And this is going to be the focus of a detailed brief and a focus of the conversation because, Teresa, you nailed it. There's a lot going on with this enforcement regime with the tribunal, lots of things to consider, including the appropriateness and sufficiency of the procedural rights.

There's some excellent aspects of this bill where express provisions relating to administrative law principles baked in to the act but there could be, and in my view it might be very helpful to have additional elements of that. In other words, just to gauge and provide some balance to organizations, not to be subject to merit-less claims, and not to be subject to undue burden. What's really interesting to me is your comment about public perception and it just didn't deem to be enough.

Anecdotally in the course of acting on numerous investigations, 99% of the investigations we worked on with the OPC, were resolved to the satisfaction of the OPC. Recommendations were made, discussions ensued between the organization and the OPC to address the practices in question. And changes were made to those practices. And yes, it didn't have the fining aspect to it. But in terms of an enhancement to the actual practices of organization and then those practices being, or recommendations being codified in, we'll call it the quasi jurisprudence of decisions and guidance, it was effective more than I think than it has been given credit to.

So it's a fair, fair comment, and it's an appropriate comment to make that for trust you need at least some ability to appropriately address very egregious behavior. But what hasn't been discussed in any type of detail, is the success that the so-called limited suite of enforcement powers that the OPC currently has. Let's turn, oh, sorry–

TERESA SCASSA: Yeah, no, I agree. I mean I think you make a very fair point that there was a lot of good work that was done in improving compliance. And in fact, in a lot of cases the problems that are raised by complaints are ones that perhaps the organization had not turned its attention to or didn't realize were a problem. And I think that there are many, many instances where the soft compliance model works extremely well in achieving results. I think the problem was that in the more egregious cases, the public face of compliance was not very, there wasn't anything to show the public in the more egregious cases.

There wasn't a big stick to wield as we would see in with the FDC in the United States, or with the UK data commissioner, or in the EU, and Canada looked like it just didn't have anything when there was a really egregious case. So you know, I do agree with you that there's a lot to be said for the soft compliance model. And there's still room for that within this bill but the additional compliance, I think was necessary.

ADAM KARDASH: Let's turn to a change in the act, and I think that falls under the category of you say looks and feels similar, but pretty significant tweak. It's the appropriate purposes or data minimization provisions collectively. Just to level set here, the act contains restates the provision in PIPEDA that organizations are only permitted to collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate.

So that's restated. It's enhanced with a mandatory consideration, an obligation for organization to consider certain factors when considering what is appropriate, including and it's not exhaustive here, but including a proportionality consideration loss of privacy proportionate to the benefits in the circumstance. And then that ties in to an express obligation for organizations not just to identify but record those purposes.

And then when you look at the data minimization principles, you're only able to collect personal information that's necessary for the determined and recorded purposes. And my initial reading like one of the phrases, or in fact word that popped right off the page for me,

was that word necessary in a circumstance, which is not just reasonable, if it's necessary. And if you think through, and as we have been starting to think through and apply use cases here that could be challenging. What's your thoughts on those principles that I just elaborated on?

TERESA SCASSA: Yeah, I think this is in section 12 and 13. And I think that these are very, very significant changes in the legislation, and really interesting ones. And certainly I think one of the anxiety producing issues around necessary in that context is, of course, that if there's a complaint, then there's a review, and necessity is determined according to, not according to the perspective of the business but according to, or is assessed from a perspective outside the business, right. So from this objective standpoint outside the business.

And I that's also extremely challenging, to have somebody to have an external perspective on what is necessary in the circumstances. So I think this is a really significant change. It's necessity and proportionality. And necessity and proportionality is a framework that is typically associated with a human rights based approach to data protection. It's an approach that I have argued in favor of. I think that the human rights basis for data protection should be explicit in the legislation. And it isn't.

And yet you find in the legislation 12 and 13, which introduced necessity and proportionality as a basis for assessing data collection. And this is at its core a human rights based approach. So I find that interesting, just as an academic I find that interesting. But I do also think that this provision makes, it really significantly increases the onus is on businesses. And I've heard it described by somebody as possibly privacy by design.

And I know I've also heard criticisms of the bill for not including a specific requirement for privacy by design but I think if you look at 12 and 13 you could argue that this is kind of a privacy by design obligation, in the sense that it would require, in order to anticipate and prepare for this kind of analysis, it would require businesses to think about what data is necessary, and perhaps to document what data is necessary to collect, and for the specific purposes, and why it's considered necessary.

And then to also take into account the issues that are listed, including you know how sensitive it is, what are the legitimate business needs of the organization, how effective is this collection use or disclosure in meeting those needs, are there less intrusive measures, and is the privacy impact on individuals proportionate to the benefits in light of any security safeguards that could be imposed, or any other protections that could be imposed. And so you know, I think that's privacy by design to a large extent. So 12 and 13 really, really interesting in terms of what they're trying to do and whether they actually serve as this kind of implicit privacy by design requirement in the legislation.

ADAM KARDASH: Teresa, you mentioned something in conversations we have about the distinction between the approach here and what might be happening in the public sector privacy–

TERESA SCASSA: Yes.

ADAM KARDASH: –provision can you share your thoughts on that? That to me is very interesting.

TERESA SCASSA: Yeah, the federal government, the Department of Justice, so this bill comes from industry. The Department of Justice is responsible for the Federal Privacy Act, which is the public sector data protection law. And they have launched a consultation, and comments are due in mid-January, I think. So they've just launched a consultation one day before this bill came down asking for input into reform of the Privacy Act. And frankly reform of the Privacy Act is also I think urgently needed and would be part of adequacy response for the

response to the GDPR for adequacy assessments. So you know I think this is a serious– another serious data protection reform that's going to be moving forward.

But in the discussion paper, the consultation paper when they talk about the– essentially, that they've been in the privacy commissioner has been pushing a necessity and proportionate proportionality approach in the federal public sector context as well. And they say in this document that may not be the right approach to take and they're looking at something limiting federal bodies to collecting only the personal information reasonably required to achieve a purpose, indicating that this better reflects the balance that needs to be struck.

So I find it really interesting to see an explicit kind of move away from necessity and proportionality and a suggestion that reasonably required is a better standard in coming from the Department of Justice in the federal, for the federal Privacy Act. Yet for the private sector context, you've got necessity and proportionality. And I think that the two need to be, maybe talking to each other a little bit more about that.

ADAM KARDASH: I think that's really good point. There should be alignment in basic principles. And I think this is one that needs further discussion. And when you mentioned the privacy by design, if we just look, for instance how it's framed in the GDPR there's some contextual factors that would be taken into account. And so this is layered on, or we have to consider how this seems to be a requirement that sits in some ways it works in conjunction with, but it's distinct from the, what is now that the [INAUDIBLE] proportionality test.

So we have to consider that because the idea of, and we've gone through this on countless occasions with clients. When you think of complex data arrangements and you asked folks who want to do the right thing, what's necessary here, not what you might like, what you want, what's actually necessary. You're going to get really well-intentioned folks saying I don't know what reasonable, if even the word reasonably in there would be extraordinarily helpful. But anyways to be discussed.

Let's turn now to one of the thoughtful provisions in the act. It relates to codes of practice, and certifications. So in essence the CPPA provides for statutory recognition of the codes of practice, and certification programs. And in essence, and it doesn't use this terminology per say, but in essence the concept would appear to provide for the establishment of what I've referred to as voluntary accountability frameworks.

And those would be overlaid in on to the existing skeleton of rules that are in the act and allow, whether it's a complex data ecosystem like interest based advertising, or it could be information sharing for fraud protection cybersecurity, or it could be for a de-identification process, I mean I think it's limitless, which it's drafted well in that regard.

Now of course, and I think this is appropriate, another example where it's appropriate, the details of all of this are going to be set out in the criteria for the code. I mean how helpful it will be, how problematic it will be, all of that will be, well what is the criteria, and those will be set out in regs. And with good reason, I mean there needs to be a discussion. So I thought that was very thoughtful. But without going on I'm interested in your impressions about this feature of the code, of the statute. What are your impressions of this?

TERESA SCASSA: Yeah, I think that both the codes of practice and the certification programs are really interesting additions. And one of the thoughts I had particularly about certification and there's been a lot of talk before the bill. And I think the bill will also generate a lot of talk around the consent burden on individuals, which is I think everybody will agree that it's too much. In the sense that we're being asked with everything we do, anything digital that we do, as well as many other things. We're being asked to consent to data collection practices

and the privacy policies are long. And we don't have time and you know, and so the consent burden is actually really high.

And I think one of the things that's interesting about certification programs and having a more formal process within the legislation for the approval of certification programs is that it can give consumers a kind of a shorthand to relieve some of the consent burden. That if you see that an organization is part of a certified program that has been approved by the privacy commissioner, so that their practices are, basically their data protection practices are certified. You know, that could for many people be the kind of shorthand that will help them to make an easier and more informed consent.

And so I think from a consumer perspective this can be very, very helpful. And obviously it could be very helpful for organizations as well. And the legislation is clear that it doesn't relieve organizations of the obligation to comply with the legislation, they'll still face accountability under the legislation. But it is I think a good way to not only assist organizations with their own compliance burden but also to communicate to consumers that they can have some confidence in how their personal information is going to be handled.

ADAM KARDASH: So I agree. My sense is this is some tweaks away from being a potentially superb feature of the act and one feature of the act that might prove to be perhaps its most profound benefit, and maybe that's an overstatement. But I'm not sure right now I don't feel it is. But I think you hit on something where you focused on a certification or whether it's a code of practice, or certification assuming, but you said certification and it's interplay with consent.

One of, it's appropriate that to me that the code of practice or program would be layered on. It would be a tailored made. It would allow for a group of organizations to construct a means to address certain type of data processing. In a way that makes sense. And it's elaborated these will be the particular data processing in question. But the interplay with consent, I think there's a gap. But I think it's worth exploring. And I think we're just a couple of tweaks away to address that. And it naturally segues to the next point that we wanted to speak to which is consent.

So the consent provisions are the consent as a feature of the statute was expected. What we didn't know, what we were going to get is how consent would be viewed, like formulated as an authority for processing. What it did, what the act does do is at least to me, and I'm very interested in your comments on this, Teresa, it really seems to reinforce this idea of consent being the primary authority for processing. And it does this by restating the structure that you get consent, and if you don't get consent there's an exception to consent. But, you know, by implication that consent is the way to go in order to get the processing.

Distinct from for instance the GDPR, which doesn't ascribe some sort of value to the court hierarchy to the authority for processing, like there's different, all legally valid, and equally valid, forms of authority for processing under the GDPR. This is not the case here. And it's reinforcing this concept of quote "a consent based statute" which is always poses some issues. And the main thing about it, and it goes into and ties into the codes of practice discussion is we're reinforcing the primacy of consent, and at the same time there's broad based acknowledgment, including from the OPC itself to an excellent consent consultation, about the challenges faced by organizations obtaining of our consent and in this current environment.

Fast forward five, six years it's going to be even more complex data processing. So you're going to have those challenges in getting it. Now we have a regime where there's significant ramifications from an enforcement perspective, if you get it wrong. And what we don't want is, what we want to do is enhance trust. What we don't want to do is introduce reticence,

introduce uncertainty, and reticence. That, that's a problem. That's a risk that I'm concerned and I think at minimum, we should be having a fulsome conversation with it.

And not only do they double down on this it's a consent based statute. It's an express consent default because if you look at the form of consent, the articulation in 15.4 is that you've got to get express consent unless you can establish that it's appropriate to rely on an implied consent. So a lot to unpack there. A lot to think through. And it's highlights to me let's think through with use cases. Let's be forward thinking. Let's future proof this statute.

Let's at least have a very healthy conversation about this because the moment, and I've had this happen to me personally I would mention, these concepts and I'd be pilloried for even suggesting a somehow the travesty of suggesting that we don't abide by the religion of consent. And maybe I'm overstating it but I really feel strongly that we can let go a permission is important, but it's not the be all and end all. And it's illusory in many respects in terms of privacy protection, especially within the context of a statute that has this enhanced and strengthened accountability. So let me pause there and I'm very interested in your thoughts about what the structure and form of the consent provisions in the statute.

TERESA SCASSA: Yeah, so I mean, you raise a lot of really interesting points. And I do think that, I think you're right that, that consent remains at the heart of the legislation. It's clear that the government has tried to carve out areas, and we can talk about those in a bit, where consent is not required. And to create some space and some exceptions, but with consent being the default rule, there are considerable exceptions to consent.

But many of those are not necessarily ones in, those are ones from the old legislation. And they're not specifically in the interests of business but serving other interests. And so this bill does have some other exceptions to consent oriented towards business. So maybe we can talk about those in a bit. But in terms of the, I was really interested in these consent provisions because I do see a shift in from PIPEDA to this bill in terms of the form of consent that I think is significant.

So under PIPEDA, there was this provision section 6 1, 6.1 that was added in a more recent round of revisions which states that consent is only valid if it's reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which they're consenting. And it's, so it's a model of consent that focuses on whether it's reasonable to expect that the individual to whom the organizations are directed would understand. And I think that's really interesting and it was a really surprising change to the legislation. And I think substantially reinforced the nature of consent.

But if you look at the CPPA, the provision in 15 sub 3 that addresses the validity of consent really just creates a list of things that basically says the consent is valid if the organization provides the individual with the following information in plain language. And so the focus is on did, was this information provided in plain language, not is the individual capable of understanding the nature, and purpose, and consequences of the collection, use, or disclosure.

And I think it's a subtle shift because it focuses attention more on was there a clear, plain language policy rather than the particular individual, and I have flagged this as one of the instances where at least on PIPEDA it didn't mention children and youth's privacy either but it had that more nuanced consent provision. And that's completely absent from this one, right. Children and youth privacy orientation at least with 6.1 you could look at that and say, is this the kind of consent language, is it being presented in a way that a minor would be able to whom the services directive would be able to understand it. Whereas this one just says, is there a plain language list of things in the consent form.

And so I think it's a subtle shift, and one that is less, what's the word for it, I think less ambitious in terms of the informed nature of the consent that's being sought. So I do think there's a significant shift in emphasis there which with the new bill focusing really on being sure that there's a plain language list of stuff. And we know that people don't really read those plain language, those lists of stuff whether they're in plain language or not. Hopefully it will help if they're in plain language but that's a bit more of a challenge. So you know, I see that as a significant shift in emphasis and consent.

ADAM KARDASH: Yeah, and on one of those significant shifts as well, I agree with you. I thought it was very thoughtful the way they frame it. And we need to think through what that means but with the default to an express form of consent that needs to be presumably an affirmative action taken by an individual before the processing, or a new type of processing occurs. And so the question is, how do we, does that make sense, and this is where the use cases come in. Does that– does that really make sense? It can be just adjusted so that consumers don't get slaughtered with notices that we all like, we're all acknowledging that no one reads it. It's an existential issue for us in private sector law firms to read. So we draft these things, right.

And it's like a well understood phenomena that they're not read and that's a problem for as an individual, me not reading them, that's my problem. It's been made available to me but we have to recognize that's the case. So having me take an affirmative action for something where everyone's requesting instantaneous type of service. It's a tough one. So how could these provisions be overlaid for instance with the codes of practice provisions? What change do we need? Like I think we need to carefully, carefully think this through.

TERESA SCASSA: Yeah, I agree and I mean that is partly where I see certification playing a role in that if it's a sort of a shorthand way of communicating to individuals that the practices of this organization conform to a standard that has been vetted and approved by the privacy commissioner. I think that, that may be something that makes a choice between one service provider that is part of a certification program and one that is not perhaps makes that choice easier. So I do, I think there's a role there.

I think another interesting issue in consent is also that the legislation now makes it much clearer that you cannot make consent a condition of the supply of a product or service beyond consent to what is actually necessary, the personal information necessary for that product or service. And this provision is linked to the penalties under the legislation as well. So you know the penalties are not available for just anything but this one is.

And I think that's a really interesting one as well. Because many organizations do collect data that goes beyond what is basically essential, or they have an argument about why this collection of a great deal of additional information is ultimately essential in indirect ways to being able to offer the product or service. In other words, it can't be for free unless all this information is provided or whatever.

And so I think that there will be some interesting issues around this question of what personal information is actually necessary for the provision of the products or services with pretty high stakes going along with that. Because this is now, it's now an obligation that you can't refuse to provide it without the additional information collection unless you can basically justify that additional information collection is justified. And there are very substantial penalties potentially if there's over collection.

ADAM KARDASH: You raise such an important point. Over the last dozen to 15 years the amount of time we have focused on the refusal to deal provisions under the current regime has been incredible. It's been a real focus of our advice and consideration and it's going to get amped up. And it's just, the risks and practical issues are amplified with that necessary

provisions that you articulated so well, those issues.

Let's turn to exceptions to consent. This is a part of the legislative scheme that I feel that I said has done a very good job with, very thoughtful again. And there's aspects to it where the intention appears to have been, and it manifests itself, that there's an expansion of circumstances where organizations may collect and use personal information without consent in terms of standard or expected types of business operations.

So this only to me just reinforces why is it a quote "exception to consent". I mean it's just as valid these things are taking place and I'm an exception. But anyways I've made my point on that. But very helpful for instance no consent required to transfer personal information to a service provider. We all are, the almost unanimous view about the interpretation of the current PIPEDA right now, is that no consent was required for these transfers. And this puts to bed that particular issue, very helpful.

No consent required for the process of de-identifying personal information processing, which is a processing of data, but to take this step to de-identify it. Even conceptually whether you're de-identify it for the purposes of a security measure, or you're de-identifying it to render it no longer subject to a legislative scheme. It clarifies you don't need consent for that, or an exception to consent, or don't need to consider it now, it's no– no consent is required for that right now and right now under PIPEDA it was being raised. This is an issue that was raised in Europe and raged for years. And then manifested itself very recently. So those are helpful.

One of the provisions is getting a lot of attention is the provisions relating to standard business activities. So the act provides that no consents required for the collection in use, not the disclosure, but just a collection and use of personal information for a broad range of activities necessary to deliver a product, or service, or due diligence to reduce organization's risk or security purposes, or product, service, or safety.

And so there was lots of discussion about this. And I think it's a fairly good list of these types of activities that no one would expect to ever provide their consent, certainly not express consent. And we were always relying on an implied consent for these types of activities which I think is appropriate under the current regime. This clarifies, you don't even need to go through that analysis. But let me pause there, Teresa, what's your thoughts about at least the current articulation of this standard business activities authority for processing?

TERESA SCASSA: Yeah, I think it's really interesting. The one thing I would emphasize is it isn't just that no consent is required, but no knowledge or consent is required. And so that's an interesting nuance because that means you don't even have to put it in the privacy policy. You don't have to give notice which is I suppose is partly intended to relieve some of the burden of having these long and involved privacy policies.

But at the same time I think removing the notice requirement as well as the consent requirement is really interesting because it means that you can collect that information without letting the individual know that, that information is being collected. And I think there's a case to be made for at least letting people know what information is being collected, even if their consent to that collection is not necessary. So I find the inclusion of knowledge in there to be really interesting because if an activity falls within that list of business activities than the individual may not even know that information is being collected.

The two provisions in the list that are I think causing the most concern are 2e, which talks about an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual. Now admittedly all of these provisions are limited. There are limiting provisions in

18.1 that talk about reasonable expectations. And that the information is not being used for the purpose of influencing the individual's behavior or decisions. And so that can put I think a limit on what is done with these exceptions for business activities.

But 18.2e is really open ended and I've had conversations with a number of people about what it means. And I've had people say, oh, it means this very simple little activity down at one end of the scale and that's all it is, don't worry about it. And others say, it is potentially, it's collection from data brokers, it's scraping off the internet. It's all sorts of things in circumstances where you don't have a direct relationship with the individual. And so you know, I think that the potential breadth and open mindedness of this one is problematic. That's probably where your use cases would also be very helpful to sort think through how it might apply in certain circumstances to see whether there is a problem, what the extent of the problem is.

And the other one that causes concern is F, which says any other prescribed activity, and you mentioned regulations before and I think there are a number of places in the legislation where regulations make total sense. You need to develop a scheme and you need to have input into that scheme and so on. But a list of business activities for which no knowledge or consent from the individual is required that's left open ended to regulations to add new ones, I think is something that will cause consternation in the privacy community because it opens the door to just adding things which will expand the scope of this.

And so on the one hand, if it's done carefully that can be a good thing from a business perspective because it leaves it open ended and you can as situations evolve, or emerge, you can respond to them. But from a privacy perspective it is it's something that I think causes a bit of consternation because it creates this rather open ended exception, not just to consent, but to notice and consent.

ADAM KARDASH: The points are excellent. My overall thought is that we just need to, number one use, use cases to ground the discussion as you mentioned, and as we mentioned earlier on in the call. Because some of the concerns that have been expressed to me of examples would actually be covered off by other– that will be covered off by other provisions in [INAUDIBLE] in other words, the publicly available exception, or a provision on the prohibition on email harvesting. So it's really important to ensure that with actual use cases that it doesn't open the door way broader than it needs to be.

Because in the conversations that were predating the actual act about this, the intention was let's just remove the burden of consent where it just doesn't offer anything, no one would expected, and like let's just get on with allowing organizations to do really the core basic business processing of data that's just not going to be impactful. That's not the focus of concern. I think this needs just to be tweaked a bit and it's an opportunity to have something really, really helpful. And so again another example, not just use case but of discourse that's there.

TERESA SCASSA: If I can just jump in on that, you mentioned publicly available information exception as being something that adds protection. But that's one that's left open to definition by regulations as well. And it has been before. And as you know this issue of whether information that is on the internet, on social media sites, or whatever should be, whether there should be an amendment to the regulations to add that is publicly available information has come up before. And you know there's a certain sector of the industry that wants that exception and has been pushing for that exception. If you get that added by regulation, then the web scraping and 18.2e becomes even more evidently a problem. So there's, you're right, there's a check in the legislation and regulations as they currently stand but those regulations, the publicly available information is also governed by regulations. And there's a lot that could be done with that in terms of personal data. So that's I think that's

another example of where the regulations are going to be very, very interesting.

ADAM KARDASH: It going to be interesting but also an example where I think you'd find common ground from those, like the vast majority of organizations, who just want to do the right thing. But there's a type of data processing that's occurring that we just got to all recognize that will continue to occur. So the question how do we just make sure that the framework doesn't allow egregious activity with that. So I like again publicly available information is something that is worthy of its own focused discussion and [INAUDIBLE] the best, the best example is the use case.

And you take examples you frame it out and you say, well, what about this, what about that. And these many, many of them are not perceived to be too problematic because of other checks and balances there. This could be but we just need to flesh that out. We just have a few remaining moments here. And we could go on for so much longer, Teresa.

There's an exception to consent also for research activities, internal research, and development activities. And the good news with that provision is that it allows for, it's drafted in a technologically neutral fashion, and it allows for internal research and business development and development activities internally. And nice language, technologically neutral. And it's going to stand the test of time.

The problem is it's subject to this condition that the data be de-identified. And this is causing in and of its own a lot of churn for a lot of different reasons. What's your thoughts about that provision?

TERESA SCASSA: Yeah, and I've heard some of those concerns being raised that if it's– I mean, the definition of the de-identification, you know, is quite clear that the information can't be capable of re-identification for it to be de-identified. And if it's internal, if it's a business's own data and they want to use it internally for research purposes then presumably if they also have that data, stored elsewhere that it's going to be inherently capable of re-identification. And so, so I think that's one of the challenges with this.

And some have suggested that maybe pseudonymization and sort of strict rules around pseudonymization might be more appropriate for this kind of circumstance. And so that maybe we need a little bit more range in terms of whether information is pseudonymization or de-identified is sort of along the lines of the GDPR. So that's certainly one of the issues I've heard around this, that it's, that the identified is maybe not the best way to go with this.

And of course, the other thing is that if you are using data for research purposes and you need to link various data sets then you really want pseudonymous data and not de-identified data. Otherwise it's not going to be as useful for those purposes. And so it may be that we need to have a conversation about pseudonymization.

ADAM KARDASH: Well, Teresa, again, we could go on for so much longer. I just thank you so much for your time. And you're always very thoughtful, insight, and commentary. I really appreciate it. And I'm sure all attendees found that very, very valuable.

Just before we end, we're at the firm here have a lot of initiatives to help folks stay abreast of all the legislative developments. Many of you have already signed up but if you haven't, please sign up for the news blasts which we're going to be coming out with key developments. We have our monthly calls but the December call of course will feature yet another session on this. We have other webinar planned in the– webinars planned in the interim, which will be announcing soon.

And as I mentioned at the up front if you haven't already, please take a look at the legislative

reform hub and a wealth of other information on the AccessPrivacy platform. We're really focusing a lot and in very short order we're going to be having very, very detailed commentary on the particular stat, on the CPPA, and the companion statute that I think folks will find very valuable, not just to understand compliance obligations, but as we look towards having a very fulsome, and constructive, and successful consultation period for this legislative framework.

So thank you very much for your time, and joining us. We hope you found it helpful. And we look forward to having you join us next time. Bye bye.

PRESENTER: Thank you. The conference has now ended. Please disconnect your lines at this time. And we thank you for your participation.

Transcript

AccessPrivacy Podcast: Canada's new privacy legislative reform – a data litigation expert roundtable

PRESENTER: Good morning, ladies and gentlemen. Welcome to the AccessPrivacy monthly conference call. I would now like to turn the meeting over to Mr. Adam Kardash. Please go ahead.

ADAM KARDASH: Hello, everyone, and welcome to our December monthly privacy call. For colleagues who are not able to join us today, please note that all of our AccessPrivacy calls are incorporated under the Resources tab of our online platform for subscribers to listen to any time at their convenience.

And we don't have an opportunity to answer questions during our calls. But subscribers can find more information on today's topics and many others in this month's monthly scan, also available under the Resources tab of our new subscription platform. The scan is intended to provide subscribers with a convenient one-page snapshot to a consolidated list of hyperlinks to recent decisions, guidance documents, of course, legislative reform developments, and other regulatory developments that have occurred in the privacy arena together with easily accessible links all in one place to keep you all in the know and save your valuable time.

So let's begin our call. Bill C-11, which was tabled in parliament mid November, proposes significant change to the national framework for the protection of personal information in Canada through the establishment of a new private sector privacy law in Canada, the Consumer Protection Privacy Act, or the CPPA.

The central feature of the CPPA and the focus of our call today is a new enforcement regime that exposes companies to significant financial penalties, potential litigation risk for companies who contravene the statute. Now, the change to the enforcement framework under the federal private sector privacy law was widely expected.

The minister of Innovation, Science and Economic Development Canada, or ISED, released the digital charter in May 2019. And this digital charter strives to establish what it terms as a foundation of trust. And it expressly provides that as a basic proposition that in a digital world an evolving and dynamic data environment, Canadians must be able to trust that their

privacy is protected and that their data will not be misused and that appropriate enforcement measures to hold players accountable is necessary to ensure Canadians have confidence and trust in the privacy protections set out in a statutory framework.

The strengthening of enforcement mechanisms, including penalties, were also referenced as a key element in June 2018's federal government response to recommendations made in a parliamentary report on PIPEDA, and were noted in the 2019, federal government's budget announcement.

And in December 2019, prime Minister Trudeau sent the minister of ISED a mandate letter, setting out that privacy law reform was a key priority for the government and that such reform must include enhanced powers for the federal privacy commissioner.

And for years, civil society, academics and most vocally, Federal Privacy Commissioner Danielle Therrien, have been repeatedly calling for significant enhancement to the powers of the commissioner with a common theme that the current suite of enforcement powers under PIPEDA, is wholly insufficient for the Office of the Privacy Commissioner of Canada to provide meaningful and effective enforcement.

Now, in the wake of these calls, civil society, academics and our privacy commissioner, it is important to highlight the remarkable success of the OPC over the past 19 years, given what the commissioner has called, the so-called extremely limited suite of enforcement powers. PIPEDA currently provides a range of different powers to enforce compliance with the act.

They could investigate complaints, they can self initiate an investigation, they could commence pretty detailed audit on reasonable grounds, they compel production of information, summon witnesses, enter premises, critically, and of key concern for organizations is the name and shame, publicly named organizations and decisions finding contraventions of the act, they can enter into compliance agreements.

And they can issue fines, is limited in scope, but they can issue fines with respect to contraventions of the pending security breach notification requirements. Those fines actually are not, can't be awarded by the commissioner him or herself. They would be referred to the attorney general but there is a finding, a limited scope of finding power under the act.

The OPC also has discretion and this has been powerful to enter into information sharing arrangements with its foreign counterparts for among other things enforcement purposes. Now, without order making power or the ability to levy large fines, as a direct result of the OPC enforcement activities under PIPEDA's ombudsman model, the OPC has become widely respected in the international privacy arena.

And the reason for this is because they've had tremendous success throughout the course of its investigative activities. Simply put, any suggestion that the OPC has been materially hampered in its ability to successfully conduct, conclude investigations, is simply not borne out by the facts.

Based on stats published by the OPC in its annual reports, of the approximately 1,500 investigations that the OPC concluded from 2015 to 2020, 98% were resolved or conditionally resolved. And for the handful of investigations that were not successfully concluded to the satisfaction of the OPC, over this five year period, the commissioner had full discretion under the statute, in each case, take the matter to federal court for a hearing.

It would be a de novo hearing, but they could take the matter to federal court and where the court had discretion to award damages, issue orders or provide any other relief it deemed appropriate, in the circumstances. In any event, the public policy freight train for a significant

enhancement of enforcement powers is now upon us, it's arrived.

It's arrived at the station with the proposed new enforcement regime set out under a bill C-11. So with that context, let's begin our discussion about the looming risks of the proposed enforcement framework with our roundtable of data litigation experts.

As call attendees have noticed in the invite to the call, we've assembled a superb panel from our national litigation practice consisting of Mark Gelowitz, Chris Naudie, both partners, in our Toronto office. Céline Legendre, a partner in our Montreal office, and Evan Thomas, counsel here in Toronto. Our privacy team works regularly, on data litigation matters with this core team and a whole bunch of others here at the firm.

And individually, and collectively, the data litigation experts on this call have a ton of expertise in this burgeoning practice area. So before we dive into the risks and other impacts, let's just start with a brief level set on the core features of the proposed enforcement regime set out under CPPA. So Evan, can you just provide us a snapshot, summary of these core features.

EVAN THOMAS: Thanks Adam, happy to. Yeah, as I see it, there are really five major changes with respect to the enforcement regime under the CPPA. So the first is the introduction of a new inquiry phase where the OPC would be making findings, making conclusions about whether or not the act was contravened and potentially issuing orders, and this would be an inquiry phase that takes place after an investigation by the OPC.

And I mentioned that the OPC could make orders at this phase and this leads into the second major change, which is the new order making power under the CPPA which confers on the OPC the power to make orders for compliance with the act, to orders to preserve documents and data while an inquiry or an investigation is ongoing, and most notably and interestingly, the ability to make interim orders while an investigation is underway.

And the third, and you referred to this earlier Adam, are the new monetary penalties that can be recommended, but not imposed by the OPC. So these are administrative monetary penalties that can be recommended by the OPC, up to a maximum penalty of the higher of $10 million or 3% of an organization's gross global revenues.

Now, there are also some, there will also be fines under the act for, under the offense provisions. And just for comparison sake, fines on conviction for an indictable offense under the proposed act would be up to the higher of $25 million or 5% of global revenues. So very significant monetary penalties or fines under the CPPA.

Major change is the creation of a new personal information and data protection tribunal. And the role of this new tribunal will be twofold. First, it will be the body that actually imposes monetary penalties. The OPC can only recommend penalties and it will be the tribunal that decides whether or not those penalties are in fact imposed.

And the other important function the tribunal would serve is to hear appeals from decisions of the OPC during the inquiry phase. And lastly, the fifth major change is the creation of a private rate of action for damages for any loss or injury caused by a contravention of the act, and this would be a private right of action that could be pursued, not just in the federal court but also in any of the provincial superior courts.

Now, obviously, there's a lot more details. But with those out and those are the five major changes that I see, in terms of the enforcement regime under CPPA.

ADAM KARDASH: All right, thanks for that. The tribunal structure is a key element of this

enforcement model. Chris, can you provide a snapshot of the key features of the tribunal structure and process and how it compares with other federal or provincial enforcement regimes and any elements of the structure that you found particularly noteworthy?

CHRIS NAUDIE: Sure Adam, I'd be happy to and it's great to be here. So as Evan outlined, the general theme of this proposed legislation is a move from traditional ombudsman model for privacy enforcement to a traditional enforcement model involving, Investigation, inquiry, findings and penalties, including penalties with significant teeth.

And as part of the migration to that former model, the government clearly felt that they needed to build in some more robust protections especially, from the perspective of institutional fairness and dividing both the prosecutorial function and the adjudicative function with respect to inquiries that result in penalties.

So the general enforcement structure that exists in the division between the OPC and the tribunal is as follows. So the commissioner, generally, has the power to investigate potential contraventions of the act and if he or she sees a potential issue, the commissioner can go on inquiry and exercise a range of evidence gathering powers.

Following the completion of the inquiry, the commissioner can issue a set of findings and a compliance order, and recommend a penalty. But to impose the penalty the commissioner has to go to the tribunal. And in particular, the commissioner files his or her findings and it's recommended fine with the tribunal.

And then the tribunal has the limited jurisdiction to consider whether or not it's appropriate to impose a penalty. In assessing the penalty, the tribunal is required in the first instance, to rely on the findings of the commissioner, and that's important. In other words, the tribunal's primary role is focused on issues of penalty.

Now, there is an ability for organization or affected party to appeal the underlying factual or contravention findings of the commissioner. In other words, the organization that may be subject to the penalty can file an appeal, but presumably the tribunal will apply some deference to those findings.

And if the tribunal ultimately concludes that the penalty is appropriate, it can issue an order imposing that penalty and that order is the equivalent of a court order. Now, the tribunal is designed to be separate, it will have a list of designated members ranging under the act from three to six members, and the act requires that at least one member must have experience in information and privacy law.

But it's important, there's no requirement to have any lawyers on the tribunal and no requirement to have any sitting judicial members, or judges on the tribunal. And its general rules of practice are flexible.

The tribunal is not bound by any legal or technical rules of evidence, and it must deal with all matters, in the words of the statute, informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.

So generally speaking, the tribunal is the master of its own procedure. There are some procedural protections that we'll talk about separately, but generally it's a pretty flexible process.

But just as a general observation, the tribunal statutory design does fall short of the traditional trappings that we see in other federal and provincial tribunals, including the Ontario Securities Commission competition tribunal, as well as other federal tribunals.

Doesn't have a clean separation of prosecutorial and judicative functions. And on its face, it looks like the OPC doesn't even have the obligation to prove its case on liability in front of the tribunal, rather it just files its findings and the tribunal must rely on them.

And quite frankly, I find that a bit surprising. When you look at the penalties that Evan just listed, their pretty eye popping penalties that can be the higher of 10 million or 3% of an organization's global gross revenues, and I stress global revenues. So we could be talking about proceedings that entail fines of $10 million, potentially, hundreds of millions of dollars or even higher.

And you would expect that those sorts of penalties that you'd have, higher standings, higher standards of institutional fairness for institutions that have to go through this process. So that's my initial general reaction, but there's more to speak about in some of the details in the procedural protections, so I'll turn it back over to you Adam.

ADAM KARDASH: Sure, thank you. Organizations, as you mentioned, face very severe penalties for contraventions of the statute. So as you also mentioned, it is critical that companies be treated fairly through all stages of the enforcement process. The data protection tribunal structure you just spoke about, by its nature provides for some procedural fairness.

So let's dig down on what you were mentioning just now, Chris, what are the checks and balances on the OPC and data protection tribunal that will help ensure companies be treated fairly in the enforcement process? And to begin Mark, I'll turn to you for some of your initial thoughts on this.

MARK GELOWITZ: Sure, thanks Adam. I think it's pretty obvious when you look at this legislation that at least some degree of thought was given to this issue of procedural fairness in the drafting of the legislation, whether it was sufficient, I think, is a question for another day and Chris's comments may give you a spoiler alert on what we think about that.

But there is in the legislation what I would call some elementary or at least baseline procedural fairness protection that's built into the legislation. So what are those key protections?

First of all, organizations are entitled to an opportunity to a hearing to be heard during inquiries and appeals, and of course, a right to be heard, I think it's fair to say, is the most basic form of procedural fairness. So not much of a give there. There's explicit protection for privileged information.

Probably, not much of a give there either since privilege is protected as a matter of common law and to some degree, it's a constitutionally protected zone of protection.

Both the OPC and the tribunal are required to give written reasons for their decisions in inquiries and appeals, and that of course is helpful from the perspective of parties knowing, what's been decided and the grounds upon which things have been decided. Not to mention the use that such reasons can be put to in subsequent proceedings.

There is an explicit requirement in the legislation that inquiries and appeals are required to conform to considerations of fairness and natural justice, and I don't think I'm going too far in saying that, Whether that was in the legislation or not, the courts would impose such a requirement ultimately in any event.

Organizations do have appeal rights to the tribunal which is a contrast with PIPEDA under which an affected organization would have a really, just the opportunity for judicial review,

under traditional judicial review principles.

And that the last point I would make under this category is that the legislation requires that a certain set of mandatory factors must be considered when the OPC is recommending or imposing penalties.

Things like, the nature and scope of the contravention that's at issue, things like, whether voluntary compensation has already been provided by the organization, whether the organization has a history of compliance with the statute.

So that's a thumbnail sketch of some of the protections that are there and maybe I can turn it over to Chris now, to say a few words about some of the other procedural issues that are going to be important as this legislation gets implemented.

CHRIS NAUDIE: Yes, so thanks, Mark. So as Mark highlighted, there are a number of quite important procedural protections that are built into the process. But what is lacking is you don't see the division between the prosecutorial and the decision making function that you would see at a Securities Commission proceeding, where there's a clear division of the bodies, as well as in competition proceedings.

And the fines in this instance, can vastly exceed the fines that are available within a securities or a competition context. So again, you would expect a higher standard of institutional fairness and I'm concerned that you're just not seeing it here.

Again, this is a process where the investigator and prosecutor makes the initial findings of liability and recommends the penalty, and simply files its findings with the tribunal that has to take it as a given. The OPC doesn't even have to prove its case in open court, perhaps in some form of an appeal.

And when you're assessing the penalty, the normal rules of evidence don't apply. They can introduce hearsay evidence, other inadmissible evidence that a court would never hear, the Securities Commission would never hear, or the competition tribunal would never hear.

So there's a lot of shortcomings here that may invite some forms of jurisdictional challenges and potentially even constitutional challenges, here. Especially, where you're dealing with the proceeding where the fines get on the heavier end and where the stigma, and potential consequences for an organization are quite significant.

She also stressed that the legislation provides that the tribunal's findings are final. If the tribunal concludes that you're subject to a $10 million fine, there is no appeal. There is an option for going through judicial review to the federal court but that's a process that generally involves a level of deference.

And again, I would have expected that with these types of consequences, that there would be further rights to protect organizations going forward. So no doubt these issues will be raised as part of the legislative process and if C-11 passes in its current form, I certainly expect some challenges to the overall structure.

And in cases that are brought in first instance, I imagine that these will be broad, in terms of, whether or not this process really gives a fair opportunity to organizations to contest these findings and to contest these onerous penalties.

ADAM KARDASH: Evan, as we spoke about a number of contacts and if we worked on files together on this, PIPEDA is fundamentally predicated on an ombudsman model. So how do you feel that the proposed regime under the CPPA will potentially change the nature and

intensity of the investigation process?

EVAN THOMAS: Well, Adam. when I look at certain aspects of this process, I find myself being driven to the conclusion that investigations and inquiries before the OPC, I expect will take on more of an adversarial tinge.

And they're likely, I would think, to be more similar to how parties conduct or defend themselves in investigations and hearings in a securities enforcement context, to use that as an example. And theirs really, I guess three reasons for that, that lead me to that conclusion.

One is just that obviously, and we've touched on this already, that stakes are a lot higher than under PIPEDA. The findings of the inquiry stage by the OPC, they can lead to significant monetary penalties and they may also lead to liability under the private right of action. So obviously the findings in an inquiry will be very important.

The other, the second reason is that these findings will be, I think, quite challenging to appeal. The standard of review that is statutorily mandated for the tribunal to apply when hearing appeals from the OPC's decision on an inquiry, is that of an appellate court.

The tribunal will be effectively like an appeal court which generally doesn't get into the weeds of the evidence and tends to defer to findings of fact and findings, or the application of the law to the facts. So it will be, I expect, challenging to overturn a finding that the OPC makes at the inquiry stage on factual issues.

I think the third reason is that, these factual findings we'll be difficult to challenge in other contexts, as well. For example, if the factual issues are mitigated in class action or other private litigation not because of the doctrines of res judicata and issue [INAUDIBLE], it may be challenging for an organization to take the position that the OPC was wrong in its findings, and it may have to live with those findings in another litigation.

So all of that leads to the conclusion that it is critical for, it's likely to be critical for organizations to put on their best case and put forward the best evidence during the inquiry phase because that's what's going to support, it's what's going to lead to the findings that the OPC makes and inquiries.

And one of the big unknowns, of course, is what are the procedural rules that will apply during these inquiries. The statute simply says, that the OPC has to develop and publish these procedural rules.

Now, I would expect, in light of the high stakes, that organizations will want rates of disclosure, rates of discovery from the OPC, to understand the case being made against them and to understand it before a hearing, and they will want the right to confront the OPC and read about the OPC's evidence through such things as right to cross-examination.

So I would expect that organizations would be pushing for procedural rules that are very like, what we see in trials, is that what we would see in court and what we would see in a tribunal such as, Securities Commissions, where it is quite adversarial in our rights to obtain disclosure and challenge the evidence being put forward.

Another effect that I think we may see is that organizations knowing the stakes during the inquiry phase, will be more guarded in the investigation phase and what we may see is a response by the OPC, in the context of its investigations, to be more liberal in its use of powers to compel documents, compel production of documents and compel testimony to support its investigation.

These are of course powers that they already have, but given the higher stakes and in a potentially more adversarial environment, the OPC may be more likely to use these powers that it currently has.

ADAM KARDASH: Thank you for that. We know that the intention was to model this investigation and inquiry framework similar to what is the case under the provincial private sector privacy legislation in DC and Alberta.

But for the various points that you made and some points that Chris made earlier, I think we're going to have to carefully consider this, certainly in advance of the parliamentary hearings which are expected to commence late January, early February and raise these issues. To the extent we see them as continuing to be problematic.

Mark, you and I have worked on multiple matters where, in essence, there's an investigation that's commenced by federal and/or provincial regulatory authorities, and once that investigation becomes public, the public is aware that it has commenced sometimes as early as a few days later, class action proceedings are commenced.

So that's the current environment, what's your sense of how the proposed enforcement regime under the CPPA will impact privacy class actions?

MARK GELOWITZ: Yeah, I've given this a lot of thought, I mean, I think that in some ways, I think we're going to continue to see exactly what we've been seeing in recent times. And of course, I don't think one needs to be even a particularly, close observer of privacy law developments to know that we're really seeing a golden age of privacy class actions, we're going to continue to see that.

So the private right of action and the enforcement regime that's in this new legislation is not going to change the way the plaintiffs class action bar approaches this subject. They are of course, entrepreneurs, their business model is designed to strike while the iron is hot. So we're going to continue to see them launching class actions, as quickly as possible after investigations are announced by a regulator.

What the enforcement regime under the CPPA is going to do, is it'll add another arrow to their quiver, I think, because, while it's certainly the case that nothing in this legislation is any sort of an obstacle to the kinds of class action proceedings that we already see based upon provincial legislation, based upon common law, causes of action for privacy matters.

What it does is, it creates perhaps what you might consider as a secondary ground or an additional ground for the class action to stand on. Now, under the act as it's drafted now, this private cause of action, the statutory cause of action will only kick in, it'll only become available once there's been a final finding by either the OPC or the tribunal, which could take years.

So an important factor that's related to that is the limitation period, because the limitation period for the statutory cause of action, again, as it's drafted now, is two years after an individual becomes aware of that final determination of the regulatory proceedings whether that's the commissioner's finding of breach or a tribunal decision, or a conviction for an offense under the act.

So that additional or that two year limitation period for the statutory cause of action, could ultimately have the effect of quite significantly extending the limitation period for privacy incidents because this statutory period might only start running after other limitation periods in the provinces, which are typically, two years from the incident.

The statutory limitation period might only start running after those limitation periods have either partially or completely expired. So it adds an additional level of risk that organizations don't have now. So of course, a plaintiff can always just commence the claim at the outset amended later on to reflect the decision, or a decision by the OPC, or the tribunal.

We see that happening routinely in privacy class actions, even now, and you can be certain that it'll happen, once there's a related statutory cause of action. But either way, these proceedings they're going to continue at least at the pace they're going now, if not if not at a greater pace. Adam, back to you.

ADAM KARDASH: Céline, what's your sense of how the proposed enforcement regime under the CPPA will impact privacy class actions in Quebec?

CÉLINE LEGENDRE: A good question Adam, similarly to Mark's answer, there will definitely be more and more privacy class actions in the Quebec landscape, as well. Also in light of a new regime, that's the Bill 64, enact and modernize the legislative provisions respecting the protection of personal information, which have similar increased enforcement, in terms of administrative sanctions, as well as penal sanctions, and a cause of action for a private cause of action.

There are some nuances that should be brought, first, to Mark's point with regard to the limitation period. In fact, it will, in Quebec as well, extend that limitation period, which is traditionally three years in the Quebec jurisdiction as opposed to two years. And another important nuance to bring is with regard to what are compensable damages and privacy class actions in Quebec.

For the moment, there's a little bit of a gray zone, but certainly, the Quebec courts are a bit more severe than the common law courts, to the effect that essentially, damages awarded for fear, stress and anxiety related to a risk of injury, will be considered, provided that there's evidence adduced to demonstrate that this fear reaches a certain degree of seriousness.

And so that's an important nuance that will remain despite of the statutory modifications. And then finally, as Mark mentioned, similarly to common law, the cause of action in Quebec largely depend on the breach of the statutory obligation. That said, those breaches are certainly for court indications of a wrongful behavior.

But in Quebec, we still have a standard under a civil code of a prudent and reasonable person. So this means that, in the class action world, plaintiffs will not have to wait for the results of an investigation prior to instituting actions, similarly, to the common law province's. Moving back to you Adam.

ADAM KARDASH: Thank you. We've spoken several times already on this call about, the CPPA's private right of action, where an individual whose affected by an act or an admission by an organization that constitutes a contravention of the act as a cause of action against the organization, for quote, damages for loss or injury that the individual has suffered as a result of the contravention.

So let's dig down on this private right of action which is getting, as you would expect, a lot of airplay among observers in the privacy arena. Mark, what's your sense of the damages exposure to companies under the private right of action?

MARK GELOWITZ: Yeah, I think this is the sort of thing that is ultimately going to have to be litigated to figure out what the scope of it is actually going to be. I think organizations for the time being should assume the worst.

But what we've got in the legislation, as you've identified, is a description of the damages that are available and they're described as damages for loss or injury that the individual has suffered as a result of the contravention.

And if that language was just standing alone, I could probably pretty easily give a confident opinion about what it meant, but of course, it occurs in a context, a context that includes PIPEDA. And so in that context, we have to ask ourselves, what does loss or injury mean? Does it mean, just financial loss? Or other tangible types of harm, or injury?

And the reason I refer to the PIPEDA context is that, PIPEDA has got a private right of action, which I should say, requires a whole bunch of hoops to be jumped through including proceedings in the federal court which we won't bother with now.

But under that statute there's a provision for an award of damages that would include, explicitly damages for any humiliation that the complainant has suffered. And so that creates an obvious question and Céline, maybe you could just give us some further comments on that.

CÉLINE LEGENDRE: I think, it is important to note that the CPPA does seem to be narrower, there is an absence of an explicit reference to damages for any humiliation. However, and this now, coming back to Mark's point about, there are a lot of issues will have to be litigated to determine the scope, but CPPA and privacy law, generally, has a broad conception of harm.

It includes, bodily harm, humiliation, damages to reputation or relationship, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damages to or loss of property. Definitely, plaintiff lawyers will be arguing for broader interpretation to recognize the infringement of the privacy rights.

ADAM KARDASH: Chris, how will the private right of action be relevant in class action?

CHRIS NAUDIE: Yeah, so my assessment on this question is pretty similar to Mark and Céline, I don't think this new remedy to the extent it comes into force, is going to radically reshape our class action regime.

The plaintiffs bar have access to a broad range of statutory and common law rights of action under the laws of the various provinces, and they haven't been suffering from a lack of federal cause of action of this nature to date. But as Mark put it, it is another arrow in their quiver.

But it's also important to stress, it's a relatively tailored remedy. It is conditional on a ruling from a tribunal and only matures once there has been a finding of liability under the act. It's only damages is for loss or injury, and you've heard the arguments that that may be limited to economic loss and there is a hard two year limitation period.

So I don't think it's going to change things radically. One tactical door that it does open for plaintiffs is, because it is a federal cause of action, it does open up for private plaintiffs to go to federal court and seek certification of class actions in federal court.

And that's important in light of some recent provincial procedural changes that we've had in Ontario that have imposed a higher burden on plaintiffs to get class certification in Ontario. And we've seen a migration of claims in the competition area to the federal court and I think, we'll see that as well, to the extent that this passes.

But otherwise, it's just another tool that the plaintiffs have and it's certainly not going to

diminish this wave of privacy class actions that we're already seeing in provincial superior court.

ADAM KARDASH: Thanks Chris, let's end the call with just a lightning round of a query and I ask you each to fast forward five years from now, and based on current trends, and assuming the CPPA is enacted in its current form, what will the Canadian data litigation landscape look like in five years? Mark, I'll begin with you.

MARK GELOWITZ: Well, five years from now, one aspect of the new data litigation landscape will be that, we'll actually be going to court live and in person, we'll be meeting with people in our offices and we'll be going to restaurants, again.

So let's start with that, but more pertinently, I guess, I would say that, what we're going to have is, I think, and I previewed this earlier in my comments, but I think we're going to have, if anything, much more privacy data litigation than we have now.

I think, this legislation is part and parcel of a momentum toward greater exposure for organizations that find themselves on the wrong side of the commission. My prediction is a much busier court docket for this sort of litigation.

ADAM KARDASH: Chris.

CHRIS NAUDIE: Yeah, I would echo that as well. General takeaways, over the next five years enforcement is going to go up. It's no secret that the OPC felt that they needed these powers because you indicated in the opening, it's an open question whether or not they really do.

But if they're passed, I doubt the OPC is just going to leave those powers on the shelf, rather they will use them to aggressively pursue their mandate under the act. And there's been a bit of a jurisdictional rivalry that's already out there, the Competition Bureau has already gone after a number of significant companies for false and misleading representations relating to privacy.

And I think the OPC is going to use these powers to try to get that jurisdiction back. But at the same time, as I highlighted, there's some institutional design issues here, maybe some constitutional issues, certainly some fairness issues, as well as some statutory interpretation issues relating to loss or injury and other terms of the act.

So I think there's going to be a wave of litigation interpreting this but overall, I think more public enforcement and perhaps, an increase in private enforcement as well, but we already have plenty of that.

ADAM KARDASH: Céline, five years. What's the Quebec data litigation landscape going to look like?

CÉLINE LEGENDRE: It's going to look very similar to the rest of Canada for all the reasons mentioned by Mark and Chris. And we have Bill 64 in Quebec that's presently being studied by the committee, and we'll have some developments with regard to that draft bill in 2021.

So similar landscape, whether you're at the federal level or provincial level here in Quebec, and maybe, the only thing I would add is that as a whole, this is just another indication for organizations to review their policies and practices and align in order to face that wave of enforcement inquiry and ensuing litigation.

ADAM KARDASH: And Evan, last but not least, your thoughts.

EVAN THOMAS: Well, Adam, I'm picking up on some of my comments earlier because of the importance of inquiries, I think upstream of that, really from the initiation of investigations or some sort of contact with the OPC that suggests that an investigation or some other enforcement action is forthcoming.

Organizations are going to have litigators involved in the process because of the downstream effects of what happens in the investigation. So I think in terms of a change, not just in terms of the volume of litigation, I absolutely agree we'll see more of this

But I also think the role of data litigators working closely will change and that they'll be working closely with substantive privacy, counsel and other privacy experts from an earlier stage once there's the specter of enforcement action in the air.

ADAM KARDASH: Well, thank you, and Mark, Chris, Céline and Evan, thank you all for your insight, very interesting discussion. Excellent comments, and we're going to continue this, of course, in the new year. In the interim, I encourage all call attendees to take advantage of the growing wealth of resources we have on the CPPA, legislative reform more generally on our subscription service.

We've just posted the first iteration, it's being posted in waves of an interactive clause by clause annotation of the CPPA and it's designed as a knowledge portal to assist stakeholders in preparation for submissions for the upcoming testimony before the ethics committee, again, which is anticipated now to take place either end of January, or early February.

And also just more broadly, to inform the consideration of chief privacy officers, in house privacy counsel and compliance specialists about the steps and resources necessary to comply with, and to mitigate the significant financial and of course reputational risk arising from the proposed changes in the federal statutory private sector, privacy statutory realm.

But most importantly, I want to thank you all for joining us today, and for throughout the year, we hope you found the call very helpful. And from all of us here at Osler, we wish you all the best for the holiday season and we look forward to speaking with you in 2021, thank you.

Transcript

AccessPrivacy Podcast: Canadian Privacy Legislative Reform – Key Issues and Considerations arising from the proposed *Consumer Privacy Protection Act*

ADAM KARDASH: Hello, everyone, and welcome to our January monthly privacy call. We're pleased to welcome you back after the holidays with a fresh new platform. For colleagues unable to join us today, note that all previous AccessPrivacy calls are incorporated under the Resources tap of our online platform for subscribers to listen to it any time at their convenience. And while we don't have an opportunity to answer questions during the call, subscribers can find more information on today's topics and many others in this monthly scan, also available under the Resources tab of our subscription platform.

The scan is intended to provide subscribers with a convenient one-page snapshot to consolidate a list of hyperlinks to recent decisions, guidance documents, and other notable developments that have occurred in the privacy arena together with easily accessible links all in one place to help keep you in the know and hopefully save your valuable time. For more information how to subscribe to our knowledge portal, click the red Subscribe Now button on the left-hand side of your screen. And just below that button on our resources list, you can access a complimentary copy of our jurisprudence report, privacy in the courts, and check out in our What's New page.

So let's begin our call. Today's session will be the latest in our continuing series of calls on Canadian Privacy Legislative Reform. In the course of our continued consideration of the new proposed Privacy Legislative Reform Act, specifically the Consumer Privacy Protection Act, or the CPPA in short, we're addressing a steady and growing number of client queries. We're working on developing comments and suggested revisions to the proposed statute in anticipation of potential parliamentary hearings. And we're continuing to work on the clause by clause annotation of the CPPA that we posted on our access privacy website.

In the course of all of this, we're fielding a steady stream of some common queries, queries that are consistent user theme and substance. And we're going to explore a subset of these queries over the next hour or so. And consistent with the format of the last monthly call in December, we're privileged to be joined by Osler subject matter experts to consider and discuss a fairly broad range of issues that the CPPA is raising here for us at the firm, and for our clients, and other stakeholders in the privacy arena.

Specifically, with me, I have, from our technology group, I have Wendy Gross, the partner, and Michael Fekete, a partner. And what's very valuable here is Wendy, leading national recognized expert in the technology space and has deep expertise and advising on large entities who are engaging service providers in various arrangements that involve information sharing, information processing. And correspondingly, we have Mike Fekete, a partner in our technology group, who has deep experience, nationally recognized as an expert. And Mike has specific expertise advising service providers in that context. So there's some interesting views that they both share.

We also have Elizabeth Sale, a partner in our corporate group and an expert in financial services regulatory area, Chris Naudie, a partner in our litigation group with deep expertise and regular diet of competition law mandates, and last but not least, we have Andrew MacDougall, partner in our corporate group and one of Canada's leading experts on corporate governance. So thank you all for joining us.

And let's just dive in. And I'm going to begin with Wendy and Mike. There's a set of questions we'll ask. And I'll start with you, Wendy. We're receiving, and as you know, we're talking about regularly now, queries from clients in the context feeling one way or another with service provider arrangements and the prospective impact of the CCPA. So let's start off with a snapshot query.

What do you feel that the impact of CPPA's enforcement regime, which, callers all know, severe penalty provision provisions including penalties of up to even 5% of global annual revenues, private right of action, order-making power, et cetera? What is the impact do you feel of the CPPA's enforcement regime on the risk profile for service provider arrangements involving personal information?

WENDY GROSS: So this is the issue that I think is garnering the most attention in terms of the substantive and significant differences between PIPEDA and the CPPA in the context of service provider arrangements, and for good reason, I think. The fact that there are now express penalties and there's a real enforcement regime that gives the CPA teeth where

historically PIPEDA hasn't really had, much of that, if any, is really going to change the landscape. And while I don't think the discussions are necessarily going to become any different in the nature and the substance of the risk allocation discussions, it's definitely going to make them much more difficult.

Over the years, when PIPEDA first came into force back in 2000, I think, it was, it was almost not a point of discussion that liability for privacy breaches would attract unlimited liability for providers. And over the last 20 years, that trend has shifted significantly to the point where many agreements between sophisticated service providers would include caps on liability for various types of privacy breaches. It's not an unlimited strict liability regime. There will be liability only for breaches or failures of security safeguards. And then the discussion often revolves around the categories of damages and the quantum of those damages.

And in the context of PIPEDA, customers were taking the lack of the enforcement teeth in PIPEDA into account in getting themselves to a place where they would feel comfortable agreeing to stretch caps or typically separate caps on liability for privacy breaches. And then in the quantum of those breaches was tied to an analysis of what the likelihood of damage would really be.

And now, we're in a scenario where the potential exposure for a service provider's breach is exponentially different than it used to be in terms of the quantum. So I think from a customer perspective, customers are going to want to revisit whether the caps that they previously got comfortable with from a risk allocation perspective will continue to be reasonable and acceptable in terms of shifting, adopting, or accepting some of the risk of their service provider's failure.

And I think Mike will have his own view on this. I think for the exact same reason, service providers are going to have to revisit those risks in the same way and are going to equally be concerned about the increased likelihood of exposure. And so I think in both cases, you're going to have customers looking to revisit those stretch caps and look for higher stretch caps. And you're going to have service providers potentially looking at those caps and fearing that they are too high.

I don't know, Mike, if you want to express your view on that. But that's my expectation about what's going to happen with these discussions.

ADAM KARDASH: Yeah, Mike, you're on.

MICHAEL FEKETE: For sure. So absolutely, Wendy, I agree with what you said. I mean, the stakes are clearly much higher. And the caps on liability will be one element that the parties absolutely will be focused on. But I think we will also see an increased focus by service providers on looking for contractual limits on what personal information is transferred to them for processing.

The more personal information that's transferred to them for processing, the greater the risks. And service providers will often want to place contractual limits on what they receive. And if they do receive information, have in place clear safeguards and controls to ensure that the shared responsibility for data security is reflected in the contractual documents in the operational practices.

Ultimately, service providers will continue to remind their customers that there are risks inherent in managing data that customers assume day to day. And that they aren't, as the service providers, there to be an insurer. I think the good news from it is that there's going to be an increased focus on data security. And ultimately, that is what the legislation is trying to drive out. And we can see that as perhaps a benefit. But from the standpoint of contracting

and from the standpoint of costs of delivering services, there will absolutely be impacts.

ADAM KARDASH: When the CPPA clarifies the scope of the definition of a service provider under the Act and correspondingly the limited obligations of organizations acting as a pure service provider, at the same time, crystallizes when a service provider would or could become an accountable entity. So what's your sense of how these concepts will be reflected in contractual arrangements?

WENDY GROSS: So it's interesting. I think we were all happy to see that this was to some extent codified because I think it was always assumed at some level that the transfer for processing was not on disclosure, and that the service provider was not the accountable entity to the extent that the use was limited to providing the services back to the customer and purely for that purpose.

Where the discussions have historically have been challenged and increasingly more challenged, and I think with this new change that crystallizes or draws this clear distinction between service provider and accountable entity, is going to shine a microscope on the articulation in the contract of the scope of the data use and what's permitted and the definitions of the scope of what is and what is not customer data.

And service providers are typically looking for rights to use customer data that go beyond simply using it for the purposes of delivering the service, particularly in the cloud context. Cloud service providers will be looking to use that data, sometimes in identifiable form, sometimes not an identifiable form, for their own purposes to whether it's to improve the services or for other administrative and back office purposes relating to the service providers business for, in the financial services space, fraud prevention.

There are a number of uses that we will typically negotiate. What this changes will do is make it abundantly clear that to the extent that use strays outside of what's strictly required to provide the service, that the service provider is becoming the accountable entity with respect to those uses. And while that may have been the case before, I think it's now going to be exceptionally clear.

And that poses a real challenge because it's not clear how the service provider will have valid consent in order to make those additional uses that are outside of the scope of merely performing the service providers obligations for those services.

ADAM KARDASH: Yeah. It could be challenging that if they don't have consent, they'll have to rely on one of the exceptions to consent. Mike, your thoughts?

MICHAEL FEKETE: Well, first off, I would like to just highlight that there are ancillary uses of customer data that are integral to the delivery of online services, cloud services, using data to prevent, detect, repair problems, troubleshooting that is for the benefit of the platform, not just for an individual customer, is just an integral part of keeping the lights on and keeping the service operational. And it's for everybody's benefit. Same for fighting fraud or cyber security uses.

And increasingly, these platforms are being viewed as more secure traditional on-premise processing of data or traditional dedicated managed services because they're able to leverage the high volume of data and the high volume of threats that they see to make a more secure platform. And so from a privacy standpoint, placing limitations on what can be done vis-a-vis, that data doesn't seem to be advantageous from a privacy standpoint.

Now, of course, limits are needed, but it's a question of what the right balance is. And I think this is also perhaps an opportune time to point out that what CPPA does not include is new

authorities for processing information similar to what we see under GDPR. CPPA remains a consent regime with prescribed rule-based exceptions. And it's when you start applying this type of dichotomy, this binary approach to your service provider an accountable entity, and if you're accountable entity, you need valid consent, that you can see some of the limitations with remaining a consent regime. It doesn't necessarily reflect the reality of the marketplace, where the market is driving more secure solutions.

So I think this is an area that perhaps the regulator– sorry, perhaps the parliamentarians will want to take a look and see if, in fact there's a way of addressing this dichotomy in a way that is more beneficial from a privacy standpoint.

ADAM KARDASH: Now, Mike, the right of disposal in this [? CPPA, ?] as you and I have discussed at length already, raises some thorny practical issues. That the concept of a term "disposal" establish effectively establishes a very high standard for the deletion of data. In essence, a disposal is a permanent and irreversible deletion of personal information. And this corresponds with a very broad disposal right. And some observers are saying, the exemptions to it aren't sufficiently broad. What's your feeling about how this manifests itself in service provider arrangements?

MICHAEL FEKETE: Well, in the context of service provider arrangements, I think it's clear that the disposable standard is unrealistic because it fails to take into account the basic elements of digital services and cloud infrastructure. Data is often destroyed by overwriting it over time. It's not something that is destroyed on request. It's something that happens as part of the controls you build into your platform.

And it's also important to keep in mind that cloud service providers often don't have the ability to identify the information of individuals whose data may be included in their cloud platform by their customer. So perhaps, a financial institution using a cloud service to process information about their customers is cloud service provider won't be able to go into that platform because of the controls in place to identify that individual user.

So when CCPA requires an accountable organization to obtain a commitment from its service provider to delete specific data that's been requested by an individual for deletion, and then confirm that it's been deleted, it actually just can't be done in the cloud context. I don't know that that was an intentional disconnect or not, but clearly something that really needs to be addressed.

When you also think about how CPPA compares to GDPR, it's I think very relevant to point out that the disposable standard under the GDPR recognizes that it's not always possible to delete or erase all traces of data. That's not the legal standard as it may seem to be on the face of it under CPPA. And as well, there's no requirement in GDPR that a service provider provide confirmation of deletion. So a couple more examples where we can see inspiration perhaps from GDPR in terms of CPPA requirements, but there is a lack of interoperability, which we think is very important from the standpoint of having a Canadian privacy regime that really does work in the global context.

ADAM KARDASH: Wendy, your thoughts?

WENDY GROSS: I agree that this is going to be a challenge for service providers or for everybody really. A typical clause in the service provider agreement will provide for destruction sometimes on request. It will mandate certain practices in terms of the standards that are used for destruction. But often, there will be exceptions to that, just to that disposal, or destruction that will not typically be heavily negotiated because it will be acknowledged that there are limitations on the service providers ability to do so.

And often, there will be an accommodation to say that the destruction will happen in accordance with the service provider standard processes or policies, which might which might mean it's done on a 90-day window or something like that. And again, those are typically provisions that are not terribly contentious because as it's acknowledged that there's an operational necessity here. And as long as your service provider has suitably rigorous standards, it's OK for them to apply those standards.

And so with this new requirement, I think that potentially means that those types of provisions are not going to be sufficient anymore unless there is some acknowledgment that there needs to be some exceptions.

ADAM KARDASH: Let's turn now to the CPPA's safeguarding requirement. The wording that sets out the standard for which organizations have to protect information [INAUDIBLE]. PIPEDA, just by way of background, provided very basically that organizations have to protect information by security guards that are appropriate to the sensitivity of the information. The CPPA elaborates that the organization must protect personal information through physical organizational and technical service safeguards, but then uses different wording. It says that the level of protection, which effectively would be the standard, must be proportionate and appropriate, proportionate to the sensitivity information.

So one of the questions that many observers are asking is, is this even a meaningful distinction? Is this effectively the same requirement, just like slightly different words? Or is it something that's meaningful? Wendy, how do you feel this will impact, this change in wording will impact contracting?

WENDY GROSS: All those thorny questions of statutory interpretation, I suppose, whether proportionate is different from appropriate and whether it's a higher or lower standard. I think there is, although it would be nice if it were clearer, there is arguably the intention of proportionate has a quantity element to it, which maybe is intended to suggest that short-term arrangements or arrangements that engage sensitive information but in very small quantities, let's say, a short-term pilot or something like that, the security safeguards and the requirements for something like that can be more flexible than a longer term arrangement.

So I'm wondering if that's possibly what– if that's possibly what they're intended to– the distinction they're intending to draw here. To facilitate short-term pilot arrangements are continually a challenge the minute they engage sensitive information. And therefore, trigger all of the full range of privacy protections and agreements. And we end up with the challenge of trying not to find a way to negotiate something that is sensible and appropriate or Proportionate To the actual risk profile because it's something smaller. And perhaps, that is the reason for the change.

ADAM KARDASH: Yeah. I mean, we're all staring at the wording trying to come to a determination on this and other parts of the Act. There's another provision in the act where a concept of proportionality is a subset of what would be– or the concept of proportionality of something must be considered in terms of determining if it's appropriate, but that's not the wording here.

Mike, any additional comments on that front?

MICHAEL FEKETE: Well, the question that has me pondering is the proper interpretation of section 11, which refers to an organization that transfers personal information to a service provider must ensure that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide. And there's two ways of reading this. One is both the service provider and the accountable organization are subject to Section 57. And section 57 sets the standard for protecting information. And so

you could say an accountable organization needs that service provider to agree to comply with section 57.

Or you could read it as saying, no, the accountable organization needs the service provider to agree to substantially the same protections as which the accountable organization has implemented to protect the information. And if that's the case, we really again have a problem vis-a-vis cloud services because cloud services and other services that are provided on a one-to-many basis reflect a single standard or framework for protecting personal information. That applies to all customer data, regardless of the individual customer.

And the business model doesn't allow for customized security commitments for individual customers. The whole model is based on the economies of scale. And frankly, meeting internationally recognized standards, which are typically certified, and then audited against by independent third party auditors with reports issued. And so it seems like the language, although open to two interpretations, could be read by accountable organizations in a way that may really be inconsistent with their use of cloud services. And as a statute that is intending to advance Canada's position in the digital economy and Canada as an innovative economy, I'm certainly hoping that isn't the interpretation that would ultimately win the day.

ADAM KARDASH: Well, Mike, Wendy, thank you for that. The thing that strikes me from your comments is there's so much to unpack there, but you're seeing so many of those elements now, in one way or the other, starting to manifest themselves in draft comments that organizations are putting together for surgical fixes that address some of the uncertainties or ambiguities and some of the other concerns. I think for the most part, you would think it would be unintended by the drafters or the policy folks at [INAUDIBLE]. But thank you for that.

And I'd like to turn now to Elizabeth to address some financial services regulatory context related considerations. Elizabeth, before don't we specifically address the CPPA, can you provide a reflection on your experience and client mandates over the last few years in terms of how the focus of data is manifesting itself in the financial services regulatory context?

ELIZABETH SALE: Sure, Adam. So maybe because it's snowing a lot today where I am, but the metaphor that came to mind is that this is a snowball rolling down the hill. And a few years ago, we had a pretty small snowball and a kind of a gentle slope. And in those circumstances, we're seeing pretty straightforward relationship structures.

When I was helping clients develop and launch new products or we were entering into arrangements for the provision of financial services, the privacy review was more limited, more basic concepts, ensuring there's appropriate consent. The information collected was reasonable, looking at the privacy policy. And that was a while ago. And that snowball has been rolling down the hill, and it's been getting bigger.

And now, we're much more likely to be advising on arrangements where there's multiple providers. There's a whole chain. You have a service provider. You have various subcontractor arrangements. And those are required because the services are much more data-rich.

Examples of these kind of services, which can be great. They can help combat money laundering. We've already talked earlier in the session about fraud detection services. They can allow consumers to have more insight on their spending habits, help prevent overdrafts and assess.

But these relatively simple sounding services, they require a lot of lift in terms of understanding the data flows at play, confirming the various responsibilities of the parties,

so that we can provide that overall regulatory advice on how to structure the product, how to put pen to paper on both the commercial arrangements and client facing terms, and identify and put her arms around the risks.

And I mean, Adam, you can attest to this. I'm on the phone with you or another member of the Osler privacy team several times a week because data is just an integral part of so many financial services products. And not only is it an integral part, but there's just more data that's available in a useful way. So maybe more established organizations had a lot of data, but it wasn't really at their fingertips. It wasn't organized in a usable manner. And now, that's changing course. And we've got a whole bunch of new providers on the horizon who've explicitly designed their products to be data-rich.

And of course, we've also layered on that. Our snowball is just rolling down that hill, we've got COVID, who's accelerated all these trends as more and more customers transition to being active participants in the digital economy. So it's really, really changed and accelerated over the past few years in terms of the type of products, the sophistication of the data arrangements that are at play here.

ADAM KARDASH: What's your impression of the most striking impact the CPPA will have through the lens of a financial services context?

ELIZABETH SALE: So for me, it's definitely the provisions on data mobility. And the first thing that popped into my head when you and I were speaking about this was, well, open banking. And you, Adam, you've had confirmation of this in terms of the regs, right?

ADAM KARDASH: Yeah. Well, at least there seems to be an indication that the regs that will be set out under the data mobility provisions and all the detail for the data mobility provisions is right of data mobility. It's all going to be set out in regulations. And at least the initial indications are that, yes, open banking would be the first use case. Well, it remains to be seen if that's the case, but that appears to be the case.

ELIZABETH SALE: Exactly. And just to put this into perspective, we, in Canada, have been talking about open banking for a very long time now. There have been consultations reports, et cetera. But it's a pretty thorny issue. And there are some pretty significant key issues that need to be considered. Privacy of course, being one of them, security, having common standards and allocation of liability.

And because of these thorny issues and because there's a lot of players who have different stakes and different interests at play, we really weren't seeing anything concrete. And particularly, when COVID first hit, there was some hand wringing from some corners when the industry consultations that were supposed to happen in the spring of 2020 on open banking were postponed with no set date, although there was some engagement this past fall.

But this past year, we've had two concrete steps that were taken. The first was that the major banks interact with payments Canada, among others, joined FDX Canada to drive common standards for data sharing. FDX being an organization where they've already established an API in the United States. So the industry started moving towards that path of the common standards. But with the CPPA here, this is the first legislative step in the direction of open banking.

So it's a pretty big deal and the implications of course can be far reaching. There's a lot of discussion of course on the possible impact on the new players, such as fintech, the possibility for more consumer-centric services, and the financial services space, which is a part of a broader discussion that's not just open banking. It's also just that focus on the

consumer. It's not silos of wealth management and insurance and basic banking.

There's an understanding that even though for historical reasons, these have all been separate, consumers don't appreciate necessarily those legislative constraints or why things appear different from the same enterprise when they go for an application for one type of product have to do the same application for a very different product. So that consumer-centric discussion has been in place for a while. And that'll be accelerated with open banking.

But there's also some other implications. And one that came to mind for me, Adam, as I was thinking about this session, was one of those traditional informational divides, which is that between insurance companies and banks. And there's provisions under the federal banking laws that prohibit banks from sharing customer information with insurance companies. It's been around for a long time. [INAUDIBLE] was a result of lobbying efforts and concerns about market dominance.

And so over the years organizations, particularly those that have had both a bank and insurance company in their corporate structure, have gone to great lengths to ensure that they don't run afoul of these provisions. But those kinds of things aren't going to make as much sense when we're looking at a true consumer-centric data world, where the consumers are in control of who has their data, who they can share their data with.

And I'm sure there's going to be other examples that come to light as we think through the implications of the CPPA. And it's going to be very, very interesting to see how some of these long-standing roles and legal obligations changed to reflect that new reality should the CPPA come into force in the way that it's currently contemplated.

ADAM KARDASH: Right. And beyond the data mobility provisions, that's essentially what you're articulating there or there are other broader impacts you're seeing? For instance, you and I have been dealing with just this increasingly interconnected web of statutory frameworks or regulatory frameworks that are governing data arrangements. But is that what you're expecting?

ELIZABETH SALE: Absolutely. The web of regulation that is imposed on financial services providers is just getting more complex. There's more and more layers. And so that's snowball that I was talking about at the beginning, Adam, the hill is just getting steeper, and the snowball is just coming faster. I think that if this goes as expected, there's going to be more process depends on the ecosystem, in particular an area that can be uplifted through data rich and innovative services like payments.

And the issues that you and I are dealing today, they're just going to intensify, things like transparency considerations. You and I have had intense discussions about service providers versus controller issues. We're going to be looking more, and we're going to be bumping up against other types of regulatory regimes like the consumer reporting laws. That comes into play already given the broad definitions of what a consumer report is and with all these new use cases for data. We're just going to be having those discussions more and more frequently.

And I think it's just navigating those different rules, the layers of the different rules. And so because of this we, as a financial services advisor and privacy advisor, our conversations are only going to continue so that we can provide practical, agile advice and a clear sense of the potential risk to businesses, who are operating on increasingly shorter timelines as they are launching new products and trying to stay ahead of this ever-changing environment

ADAM KARDASH: Yeah. That word agility is key because the expectation, there's development of products and services in a highly agile way. There's an emerging concept of agile impact

assessments. And corresponding with that, there's that agility to the advice. Really, it's almost real time.

ELIZABETH SALE: Almost real time.

ADAM KARDASH: It's challenging. But thank you, Elizabeth. And I think is it to pick up from where Elizabeth left off, I want to turn to Chris. And just before we dive in, Chris, on the specifics of the impact of this CPPA, can you provide a reflection on your experience and client mandates relating to the competition law context over the last few years of how the focus of data is manifesting itself in this regard?

CHRIS NAUDIE: Sure. Thanks, Adam. And it's great to be here. So over the past few years, we have seen privacy and competition regulators ramp up their enforcement of the protection of privacy rights. And many of our client mandates on the competition and litigation side had been representing companies and responding to those enforcement actions. And this enforcement trend has been driven by a number of factors, including increasing societal recognition of the importance of privacy rights, increasing number of incidents involving large companies that have experienced unauthorized disclosure of consumer information, and of course the political reality that the federal government and its regulators want to be at the front end of protecting the privacy interests of consumers across Canada.

Now, much of this enforcement activity has been focused on holding companies responsible for data breach incidents as well as the unauthorized collection, use, and disclosure of consumer information. But there's been a separate stream of enforcement that has focused on, what I call, deceptive practices relating to privacy, namely alleged false and misleading representations to consumers regarding the collection, use, and disclosure of their personal data.

And in this respect, both the Office of the Privacy Commissioner and our federal competition regulator, the Competition Bureau, have both been jockeying for a role, even sometimes in the same enforcement cases. The OPC has been exercising its traditional ombudsman powers as the lead privacy regulator in Canada. And the Bureau has been exercising its powers as the federal regulator responsible for taking enforcement action in respect of false and misleading representations to the public. And to use Elizabeth's winter metaphor, they have been throwing snowballs at each other to determine who is going to be really the lead regulator of deceptive practices relating to use of consumers data.

But for years, the OPC has been hindered by some limits on its investigation powers and its inability to seek and impose fines. And that's led to a significant push to gain new enforcement powers. And the CPPA has been a product of that process.

We've also seen one other enforcement trend in this area. Over the past several years, the Bureau has placed a significant policy focus on studying the impact of big data on competition in the Canadian economy. And as part of that policy focus, the Bureau has expressed concern about how the collection of data network effects can contribute to the enhancement of market power in various sectors of the economy and could create barriers to entry for new entrants in important markets.

As a result, in the exercise of the Bureau's review of mergers, monopolistic practices, and other reviewable practices, the Bureau has increased their scrutiny of these practices relating to the collection of consumer data and whether that collection can undermine the ability of consumers to switch to competitors and interests. And as we'll talk about, the introduction of the new data mobility right could mitigate some of these concerns and is going to be an important part of the competition analysis going forward.

ADAM KARDASH: And what is your impression of the most striking impact that the CPPA will have in the competition law sector?

CHRIS NAUDIE: Sure. Well, there's really two features that come to mind. The first is the expansion of the OPC's enforcement powers that overlap with the Bureau. And second is the creation of this new data mobility right.

So under the CCPA, the OPC will have a host of new powers to conduct inquiries and issue orders, including interim orders and compliance orders and preservation laws. In addition, the OPC will have new powers to recommend significant fines. And the new maximum fine for a breach of the act is $10 million or 3% of a company's global revenues.

And there's even higher fines and penalties where an offense is being committed involving knowing and willful conduct that results in breaches of the act. So this is a clear transition to a full enforcement model. And we will now have two federal regulators armed with compulsive powers and fine powers that are policing representation to consumers regarding the use of their data.

Secondly, the new data mobility right is a real game changer. It will facilitate, if implemented, the ability of consumers to take possession of their own personal data and to switch to competitors. But it also creates a host of challenges for organizations to accommodate this right, particularly where data sets are structured in a way that incorporate the company's proprietary and confidential information.

Now, there are general provisions of the proposed legislation that try to accommodate a company's protection of its proprietary information. But there's no detail as of yet. And all that detail will be set out in the regulations. And this is an area where, again, the OPC and the Bureau may not be fully aligned and federal policy they have to be worked out. Fully expect that the OPC is going to be a strong advocate for data mobility and portability.

And that the Bureau will be an advocate as well. But by contrast, the Bureau will want to ensure that competitors are not exchanging competitively sensitive information as part of the implementation of this right, particularly information relating to consumer choices, prices, transactions that may facilitate the ability of competitors to align their business practices, their business models to the detriment of competition in the Canadian economy.

So with those two significant trends, we certainly see a lot of challenges around the corner.

ADAM KARDASH: Chris, thank you. And with respect to that mobility rights as mentioned earlier, all the details are going to be in the ranks. It'll be interesting to gauge your thoughts once we have draft regs for consideration. Thank you for your comments. Let's turn now to Andrew on corporate governance-related matters. Andrew, thank you for joining us.

Before specifically addressing the CPPA, I thought it might be interesting for attendees to hear your reflections over the last 10, actually 15 years, as to the nature and themes of when and how boards of directors have been focusing on data and particular personal information?

ANDREW MACDOUGALL: That's a great question, Adam. I always love starting with a bit of a retro look at things. And it's very interesting because a decade ago, or so even 15 years ago, data issues rarely made their way to the board at all. Some of the early discussions that we would have with companies about how to bring this issue to the board were focused on why would you even take data issues up to the board level. And we began with some disclosure guidance from the SEC in 2011, followed by some Canadian securities administrators staff notice with guidance in 2013.

But when you think about it, all of that was focused on cybersecurity. And it really wasn't until 2012 that that cybersecurity was identified by the World Economic Forum as one of the global risks, one of the top five ones in terms of likelihood. So it was really very much a cybersecurity and a risk focus. And so the discussions that would be had at the board level were all focused on what were the risk implications looking at, for example, operational issues, such as disruption to business operations, loss of proprietary information, reputational concerns about the loss of trust from customers in the event of a data breach or a loss of data, the potential that you'd lose some commercial relationships with some of the other parties within the chain of commercial contracts that you might have.

There were body regulatory concerns. I think some of those we've talked about it already on the session. But they were relatively light. So we were focused mostly on disclosure controls and the start of reporting requirements. And litigation was very much focused on, for public companies, securities class actions as a basis with the theoretical possibility of derivative actions being relevant. So it was very much a risk focused. It was very much initial. And over time, that grew.

And as companies began experiencing data breaches, it became far more significant to the point where boards became educated on the issue. There may have even been a sense of giving up that everybody is going to experience a data breach at some point in time. So what can you do about it? But very much so focused on having to address it and find the right standard to apply for your organization. And it was right for the directors to focus on data. It was a valuable asset. And directors have a fiduciary duty to safeguard the assets of the corporation. So the focus on security initially is a quite natural extension of all of that.

The part that wasn't as well understood is really how valuable the corporation's data can be, especially the personal data that's in the corporation's possession. And I know you're very aware of all of this, but in a sense, we're still really only beginning to unlock the value of that data. We've moved from tracking a customer demands that we can improve our inventory management to using data to deliver a more personalized experience for individuals. And now, looking towards using that to start to predict customer needs in advance.

But we're really only beginning that journey at the board level and trying to understand data from a strategic perspective and the opportunities that it presents. And we don't know how to deal with the fact that data actually is a very valuable asset. We certainly don't know how to account for it on the balance sheet, for example.

But now that we're starting to look at that is as valuable at the board level, it's really looking at those concepts of how you're going to use the data and recognizing its value that I think is really what is of interest at the board level and is probably a large part of the motivation for CPPA.

ADAM KARDASH: Let's turn now to the CPPA. You've heard it over the course of the call several references to the CPPA's enforcement regime, severe penalty provisions, private rights of action, et cetera. And then what we haven't talked about on this call yet, there's accountability obligations which, in essence, require organizations to develop and implement a privacy management program. That in essence, is a suite of policies, practices, and procedures to fulfill their obligations under the statute.

And when you look at these two sort of core features of the statutory framework of the CPPA, how do you feel that that will impact corporate governance?

ANDREW MACDOUGALL: So when I look at what's happened with the CPPA, to me the sense is that there was a view that there needs to be minimum standards for data collection, use. And this is very much a remedial piece of legislation. Looking at the prescriptive nature of the

proposed legislation, the potentially enormous penalties that are there for noncompliance, you really do get the sense that the drafters believe that minimum standards were just not being met, and that privacy and data issues were just not receiving the attention that they deserve, including at the board level.

And I really like looking at sort of the penalty limits and sort of comparing them to what we might see, for example, in the statutory civil liability regime for public companies when you have misleading or untimely disclosure. Because a limit of 3% or in some cases 5% of global remedies is a very substantial penalty.

And just out of fun, I went and took a look at Royal Bank with its 2019 revenues of $46 billion. 3% of those revenues is a penalty potentially of up to $1.4 billion. That's a very significant penalty. And it's not far off of the very significant penalties that would exist if there was a material misrepresentation in their continuous disclosure because there, it's a statutory civil liability cap of 5% of market cap. And with $150 billion market cap, that gets you to 7 and 1/2 billion as a penalty.

And what does this tell me? It tells me that this is being given, at least from the penalty side of things, a liability issue that is very similar to what we're facing under a statutory civil liability. We have responsibilities for directors who might authorize acquiesce to permit the non-compliance by the organization with a due diligence defense, just as we do under statutory civil liability.

And all of that means with these big numbers that the materiality of the consequences here of not only the data breach but of any improper use of data will limit in your enterprise risk framework. Data management and protection issues are going to be elevated far more because they're much more of a material number in terms of a risk. And so a lot more attention needs to be paid.

And when you think about what happens from a disclosure perspective for a public company in terms of the processes that you put in place to provide comfort that what you've disclosed is accurate, that you haven't left out something, is a very involved process. And we're going to be replicating much of the process over here on the data side in order to be able to ensure that there is comfort that the standards that are being articulated in the legislation are being met, and not only by the organization, but also with respect to the organizations subcontractors or service providers as well.

ADAM KARDASH: What's the snapshot of what boards of directors have to do to attain this comfort to address those risks? What do they have to do?

ANDREW MACDOUGALL: Stepping back, fundamentally the board's role is a stewardship role of active oversight of the strategies and the risks of the business and the delegates day to day decision-making to management. And if there's an appropriate compliance framework in place, the board can rely on management to do its job within the framework until it knows of some sort of flaw in the compliance framework.

And court cases have concluded that directors can be liable for failure to exercise appropriate oversight if they don't have an appropriate framework in place with appropriate reporting and information systems and controls. Or having implemented such a framework, they failed to monitor it and oversee it with the result that they don't become informed of subsequent risks or potential issues that might require their attention.

So what I think this actually means for a board of directors is they're going to need to understand the implications of the legislation for the organization, what needs to change in order to comply, the cost for doing so, the time frame for doing so, and what sort of

guardrails need to be put in place. And that discussion needs to happen with the directors ahead of time. And may even prompt some additional educational discussions at the board level to understand exactly where data is coming into the organization and where it's being used.

And that will prompt, putting in place a new regime, some updated corporate policies will be necessary, potentially capital investments, certainly new trading and personnel, enhancements to internal whistleblower policies, and practices, and training. All of that will be something that the board of directors will want to know as being looked at by the organization. They'll have some views on how effective it's being done. And then they're going to need to take a look at what are the controls that the organization is putting in place to ensure that the system is working and that red flags of indicative of potential problems are being raised internally.

And they just need to have an understanding that management's approach is rigorous enough. And that there is reporting at some level to the board to give the board some sort of assurance that management is paying attention, that issues are being raised and are being addressed. And so while this legislation is also remedial, I think it's actually just the first step in many respects because you do have a bit of a gap between individual expectations and the potentially broad permitted uses of personal information even under a consent.

So I think, to me, directors are going to be very much focused on ensuring that we've got the standards to satisfy what's necessary right now and that management has it underway. But they're also going to be very alert to the possibility that those standards will change over time and likely increase over time as people realize the value of the data that they generate individually and decide to take ownership of their own personal data.

And just because you have personal data doesn't mean that an organization should use it in a particular fashion. And there will be some instances where the board is going to need to chime in on just exactly what uses of data are appropriate for the organization, whether due to reputational concerns, or in order to differentiate themselves from competitors, or whether just to reflect the values that the organization holds dear.

I think we've got a two-step process here very much, Adam, where it's additionally going to be very much a compliance focus. But then there's I think a second stage that will evolve out of that and looking more strategically at how the organization wants to position itself in a new data-centric world.

ADAM KARDASH: Well, Andrew, thank you for the time. And thank you to all of my colleagues here at Osler for their insights and for the very interesting discussion and their reflections over the course of the call. I encourage all call attendees to take advantage of the growing resources we have on the CPPA and legislative reform generally on our subscription service.

We're continually updating our interactive clause by clause annotation. It is just in the last business days. We have updates on comments on the day identification provisions, the provisions relating to publicly available information, and the provisions relating to the penalties and enforcement, some of the stuff that is discussed on this call. And we also have a broader– if you get access to the site, there's also a wealth of other resources regarding current requirements. And we're just about to post a detailed hub on biometric information, as well as for those of you in Ontario, a very, very detailed provision on the very complex data integration unit provisions that were recently put into force.

So again, thank you very much for joining us. Again, we hope you found the call very helpful. And we look forward to speaking with all of you again in February.