Zoom Transcript for “Legislative Roundtable: Draft Regulation on the anonymization of personal information in Quebec”, held on 30 January 2024.

00:09:57.000 --> 00:10:09.000

There we go. Okay. Well, hello, everyone. Welcome to our roundtable discussion on Quebec’s draft anonymization regulation.

00:10:09.000 --> 00:10:21.000

This session today is being hosted jointly by Access Privacy, Osler’s Thought Leadership Forum, and the Canadian Anonymization Network or, as we call ourselves, CANON.

00:10:21.000 --> 00:10:30.000

CANON is a not for profit. Its members consist of large data custodians across the private, health and public sectors.

00:10:30.000 --> 00:10:39.000

And the stated objectives of CANON are set out on the website. For those of you who have not been, we encourage you to go to www.deidentify.ca.

00:10:39.000 --> 00:11:11.000

We love that URL. But those objectives are, among others, sharing and exchanging information about internationally evolving legal policy and technical standards on anonymization, developing a Canadian community practice on effective anonymization and, particularly germane for this session, advocacy for balanced legislative and policy standards for anonymization for 2 fundamental purposes.

00:11:11.000 --> 00:12:17.000

One, to reasonably protect against foreseeable privacy risks. And critically also, to enable innovative and beneficial uses of data. Here at Osler, our privacy team has been fielding calls and having extensive discussions internally about the draft anonymization regulations. We have over 700 registrants - folks that have registered for today’s session. We have folks that are continuing to join as we speak, and this is reflective of the significant interest and the certain challenges raised about the draft regulations and the content of the draft regulations put forth by the Quebec government. And more broadly it’s really yet another example of the expanding and increasingly intense focus of interest amongst the stakeholders in all sectors about the concept of de-identification and anonymization.

00:12:17.000 --> 00:13:00.000

Today’s session is structured similarly to workshops that Access Privacy has run as part of governmental and regulatory authority consultations such as the ones we did for the ISED code of practice on AI and the Quebec privacy regulatory authority’s draft consent guidance. In essence, we’re effectively running this discussion for the next hour and a half to 2 hours as part of the Quebec government’s consultation process. Structurally we’ll begin the session with a panel discussion. And we have an excellent panel consisting of members of the CANON steering group, specifically Khaled El Emam

00:13:00.000 --> 00:13:01.000

No sound.

00:13:01.000 --> 00:13:05.000

Who is a globally recognized expert in de-identification, anonymization and the current - I'm sorry if everyone could just go on mute if you aren't.

00:13:05.000 --> 00:13:10.000

Sound.

00:13:10.000 --> 00:13:36.000

Thank you. I'll just introduce the panel again. Members of the CANON steering group, specifically Khaled El Emam, a globally recognized expert in de-identification and anonymization and the current Canada research chair in Medical AI at the University of Ottawa, and co-founder and CEO of Replica Analytics. Pam Snively, who's the chief data and trust officer at TELUS Communications and TELUS health.

00:13:36.000 --> 00:13:45.000

Suzanne Morin. A VP Enterprise of Conduct, Data Ethics, and the Chief Privacy Officer at Sun Life. And last but definitely not least,

00:13:45.000 --> 00:13:52.000

Keren Groll, who is the Senior Special Counsel, Privacy and Data Innovation at TD Bank.

00:13:52.000 --> 00:14:02.000

Our session today will be recorded and a copy will be sent to the Quebec government for their consideration as part of the consultation process, which ends on February 3rd.

00:14:02.000 --> 00:14:12.000

We're going to begin, as I mentioned. with the panel discussion and then after the panel discussion, we're going to open up the floor for comments.

00:14:12.000 --> 00:14:29.000

We're encouraging live comments or questions, but of course feel free to make comments in writing on the chat feature in the Zoom Platform and to do so, we encourage you to make those comments as the panel discussion is ongoing.

00:14:29.000 --> 00:14:34.000

If you wish, given that the session will be recorded, the zoom feature will allow you to change your handle or the profile

00:14:34.000 --> 00:14:47.000

so that your comments can be made without attribution to you or your company. So. Let's begin.

00:14:47.000 --> 00:14:54.000

Catherine, can you just put the document up on the screen?

00:14:54.000 --> 00:15:05.000

So, for the purposes of level setting for the session, I'm just going to make a few comments

00:15:05.000 --> 00:15:18.000

about the anonymization provisions within the statute before we dive into the discussion with the panelists about the content of the draft regulations.

00:15:18.000 --> 00:15:39.000

So first, you'll see in section 23, the concept of anonymization is captured within that second paragraph where, by virtue of the provisions in law 25, which amended Quebec's private sector privacy law.

00:15:39.000 --> 00:15:51.000

There are corresponding amendments to the public sector privacy law. We're going to be focusing on the private sector piece for this particular call.

00:15:51.000 --> 00:16:17.000

Law 25 introduced changes, the vast majority of which came into effect this past September. One of them was these anonymization provisions and the second paragraph basically sets out that information concerning a natural person is anonymized if it's reasonably foreseeable in the circumstances. That's one condition.

00:16:17.000 --> 00:16:50.000

That it "irreversibly no longer allows the person to be identified directly or indirectly". So basically, there's a contextual provision within the definition of anonymization – it has to be reasonably foreseeable in the circumstances and we've had discussions amongst CANON and that was reflected in comments CANON made to the federal government or INDU specifically as part of C 27 on this exact point. And specifically, the second aspect of this is in the third paragraph:

00:16:50.000 --> 00:17:16.000

Information is anonymized under the statute. It has to be anonymized in accordance with generally accepted best practices. Therefore, by implication, by reference, in a non-specific way, incorporating by reference the best practices that would appear in well-established instruments outside the statutory framework.

00:17:16.000 --> 00:17:29.000

And then it goes on to say, and "according to the criteria and terms determined by regulation". And if you look under section 90,

00:17:29.000 --> 00:18:41.000

the regulation basically says, in section 90 for the purposes of this section, regulations may be made with respect to the criteria in terms applicable to the anonymization of personal information, and that is what is leading to the draft regulations there. So, the second piece to mention just before we move on is that the anonymization provisions don't appear in a vacuum, the definitions are not within the other defined terms, a list of the defined terms, but rather the reference to the anonymization concept is within section 23 as you see on the screen and specifically the destruction provisions, which provide that, where the purposes for which personal information was collected or used are achieved, the person carrying on the enterprise must destroy or, by implication as an alternative to destruction, anonymize it.

00:18:41.000 --> 00:18:58.000

And then that leads us to a phrase that really has been subject to considerable discussion. It's anonymizing it, not in a vacuum, but it's stated to use it for serious and legitimate purposes. It's worth making a couple of comments about this.

00:18:58.000 --> 00:19:12.000

So, Law 25 introduced, as many folks on this call are aware, a number of provisions that were novel.

00:19:12.000 --> 00:19:45.000

Distinct from many if not any other statute globally. And while they're similar thematically, they certainly, I can speak with respect to client mandates, have been the subject and remain the subject of a lot of discussion. This is section 8(1), which is the profiling provision. Section 9(1) is confidentiality by default, and the prescriptiveness of some of the language in the consent provisions, etc.

00:19:45.000 --> 00:20:01.000

And these are discussion points that we continue to have in terms of operationalizing the provisions and, in particular, concepts relating to interoperability of this statutory regime with those other statutory instruments.

00:20:01.000 --> 00:20:13.000

This provision right here in that first paragraph, which says "or anonymize it to use it for serious legitimate purposes".

00:20:13.000 --> 00:20:25.000

is novel and distinct, and we'd be interested in comments from folks on this, but, to our knowledge and we've looked at multiple other statutory regimes,

00:20:25.000 --> 00:20:29.000

there is not another Privacy statute that has this qualification of the purpose for anonymizing data.

00:20:29.000 --> 00:20:45.000

This seems unique and therefore raises a number of different questions as to operationalizing it.

00:20:45.000 --> 00:20:55.000

We're going to be discussing that in the panel. And the final point, I just want to scroll down, if you just go to the penalty provisions in section 91.

00:20:55.000 --> 00:21:11.000

It's an offense under the statute to attempt to identify a natural person using de-identified information or using anonymized information.

00:21:11.000 --> 00:21:29.000

So basically, a re-identification prohibition once data has been anonymized. Penalties are potentially quite severe for a contravention of this particular statute and notably this is not the only statute that has this.

00:21:29.000 --> 00:21:46.000

There's a prohibition on reidentification in multiple statutory instruments. PHIPA is one example in Ontario domestically.

00:21:46.000 --> 00:21:51.000

There's different wording, but similar provisions in Singapore, under the CCPA in California, in Japan's statute, etc.

00:21:51.000 --> 00:21:57.000

So, this is a prohibition on anonymized data, but it is in effect and this is an important point -

00:21:57.000 --> 00:22:00.000

That's attempt to inter. Okay.

00:22:00.000 --> 00:22:12.000

I'm sorry if everyone can go on mute. It is in effect a provision that is actually regulating the use of anonymized data.

00:22:12.000 --> 00:22:19.000

In other words, you can't use anonymized data for this reidentification purpose. Another point just to highlight.

00:22:19.000 --> 00:22:25.000

So, let's turn now with that background. We just wanted to level set for those of you who haven't spent time with the anonymization provisions.

00:22:25.000 --> 00:22:38.000

And also, to level set for the purposes of the conversation. Let's turn to the panel and I'd like to begin the first with 3 questions.

00:22:38.000 --> 00:22:42.000

We'll start with the first one.

00:22:42.000 --> 00:23:00.000

And I'm going to begin with Khaled. Khaled, in your view, given the statutory definition of anonymization - and Catherine can you go back to section 23

00:23:00.000 --> 00:23:08.000

and the reference to, in particular, best practices and this concept of reasonably foreseeable in the circumstances, etc.

00:23:08.000 --> 00:23:49.000

Just from a public policy perspective, number one: Are regulations even necessary from a practical perspective in order for companies to engage in an effective anonymization practice? And I note this, in particular in the context that the CAI, the Quebec Privacy Regulatory Authority, made a public statement that, given the nuance of the anonymization process, the commission believed that government regulation was needed to clarify the situation and that pending indications from the government to this effect, that it was going to be extraordinarily difficult

00:23:53.000 --> 00:24:16.000

to actually anonymize data. So, Khaled, just to get your perspective on this: A. Are, in fact, these regulations even required and if they are not actually required, what are some of the beneficial aspects of the proposed regs that you think are worth highlighting?

00:24:16.000 --> 00:24:27.000

So, I'll start with some general statements and then I'll talk about the specifics in these regulations.

00:24:27.000 --> 00:24:35.000

So, as a general statement, we've observed over many years that uncertainty is not beneficial. Uncertainty around what are acceptable anonymization practices.

00:24:35.000 --> 00:24:52.000

It either results in organizations doing nothing because they're afraid of taking steps in an uncertain environment – an uncertain regulatory environment,

00:24:52.000 --> 00:25:15.000

which means that potentially beneficial uses of data are not happening. Or, organizations and individuals in those organizations take big risks - big corporate risks or individual risks - to put in place activities around anonymization in an uncertain regulatory environment.

00:25:15.000 --> 00:25:36.000

So, uncertainty in general is not beneficial and removing that uncertainty is desirable. The regulations mentioned following generally accepted best practices which is good because there are a lot of good practices out there.

00:25:36.000 --> 00:25:41.000

And I'll mention 2. One is the recently published ISO standard, 27599,

00:25:41.000 --> 00:25:46.000

which is the identification standard that reflects good practices that have been in use for some time.

00:25:46.000 --> 00:25:58.000

And then of course there are the Ontario de-identification guidelines as well, which have won awards – they are very well written guidelines.

00:25:58.000 --> 00:26:10.000

So those are 2 obvious documents describing good anonymization practices that one can refer to, an international one and the Canadian one.

00:26:10.000 --> 00:26:42.000

With respect to the regulations, they have many good things. So, if we take the best principles from statutes and regulations around the world – there are some very good things in the US HIPAA privacy rule around de-identification and in PHIPA - and if you take the union of those and map them to the Quebec regulations, there's a big overlap

00:26:42.000 --> 00:26:52.000

in the sense that there's a requirement for the person to be qualified, which is a very good requirement.

00:26:52.000 --> 00:27:12.000

Talks about removing directly identifying variables first. So, talking about pseudonymization, very good; generally accepted practices, very good; establish the protection and security measures – so, essentially other controls to manage the risk consistent with best practices; reasonably foreseeable in the circumstances -

00:27:12.000 --> 00:27:19.000

so, reasonableness criterion; no zero risk - that's really important

00:27:19.000 --> 00:27:28.000

and it's written in there, which is fantastic; and then there's the requirement to do reanalysis over time.

00:27:28.000 --> 00:27:34.000

I think we'll come back to that later on, but that's consistent with best practices. How you define it, of course, is important.

00:27:34.000 --> 00:28:03.000

And then there are things in there that I think are not consistent with best practices, at least that exist today. One of them is one you mentioned about the purposes have to be defined a priori for which the

purposes for the anonymized data. And then there are 3 criteria that are correlation, interference and individualization, which are consistent with the European Article 29

00:28:03.000 --> 00:28:14.000

Working Party opinion on anonymization techniques, linkability, inferences, and singling out.

00:28:14.000 --> 00:28:27.000

And those are problematic because even under the context of GDPR and the implementation of these criteria, we just don't know how to do it.

00:28:27.000 --> 00:28:33.000

I mean they came out in 2014 so basically 10 years later we still don't know what they mean.

00:28:33.000 --> 00:28:39.000

And we still have discussions about what these things mean and how to interpret them. Academics are writing about them.

00:28:39.000 --> 00:28:49.000

People are struggling to interpret them. So, the fact that these 3 criteria showed up in 2024, I think increases uncertainty.

00:28:49.000 --> 00:28:50.000

And then the -

00:28:50.000 --> 00:28:57.000

And Khaled, just so we're helping folks along the line - Catherine, can you just scroll down?

00:28:57.000 --> 00:29:14.000

Just to catch up before your next point. So, first of all, Khaled was just mentioning here these definitions: correlation, individualization, and inference. And Khaled, we're going to get to the challenges in the second question but I just want to highlight a couple of particular points.

00:29:14.000 --> 00:29:25.000

If you go to section 7, I want to highlight the point that Khaled mentioned. Go down, Catherine, to section 7.

00:29:25.000 --> 00:29:38.000

Here is this reference to the zero risk piece. And for the purposes, look at the third paragraph.

00:29:38.000 --> 00:29:58.000

For the purposes of the second paragraph here in section 7 it is not necessary to demonstrate that zero risk exists, however taking into account the following elements. I don't want to put words in your

mouth, Khaled, but I think this is what you were highlighting that was beneficial of the proposed regs. Am I correct?

00:29:58.000 --> 00:30:10.000

Absolutely. I mean, it says irreversibly no longer allowed the person to be identified. So, the word irreversible kind of implies zero risk, but then subsequently it says not zero risk.

00:30:10.000 --> 00:30:23.000

So, that's good. However, you know, if the word irreversible is removed, that would make it more consistent with the concept of zero risk because generally irreversible is interpreted as zero risk.

00:30:23.000 --> 00:30:33.000

But the last 2 things I would say is the things that are missing. Under the US HIPAA, we talk about how you evaluate the risk from the perspective of the anticipated recipient.

00:30:33.000 --> 00:30:51.000

And there are various court cases from in the European context that have essentially reached the same conclusion - that the same data may have different risk levels depending on who is processing the data. So really, you measure the risk from the perspective of the anticipated recipient.

00:30:51.000 --> 00:30:57.000

This is a really important concept. So, that's missing. And then another big one is consent for anonymization,

00:30:57.000 --> 00:31:04.000

which is very clear under HIPAA. But that's not mentioned here in terms of whether you require consent for anonymization or not.

00:31:04.000 --> 00:31:09.000

So, all that to say, to summarize, I know it's a long answer, but it's kind of an opening statement.

00:31:09.000 --> 00:31:22.000

So, the reduction of risk is important. There are a lot of good things here, some things that I think will be harder to operationalize, some things that are missing.

00:31:22.000 --> 00:31:27.000

Having guardrails is good. They're good practices. We can just say use good practices.

00:31:27.000 --> 00:31:38.000

But if a regulation is going to be written then they should be consistent with good practices and so all the points I raise are trying to make it consistent with those good practices.

00:31:38.000 --> 00:32:17.000

Right, and so just to even further give a summary of your summary at the end: What you're saying is just with the definition of anonymization, which expressly contemplates best practices, while it might not be critical for the purposes of the operationalization and organizations engaging in the anonymization practice, there's beneficial aspects. Especially - let's go back to number 7 of this reg - because of that statement that it doesn't have to be zero risk which is very important.

00:32:17.000 --> 00:32:31.000

And there seems to be other aspects of this draft regulation that overlap with well established standards or other principles for effective de identification.

00:32:31.000 --> 00:32:33.000

Am I summarizing that correct? Go ahead.

00:32:33.000 --> 00:32:35.000

That's right. Yes, absolutely.

00:32:35.000 --> 00:33:04.000

Okay, well thank you and Pam let's turn it to you to build upon or have your own additional comments with respect to the 2 questions of: are these regs even necessary? And even if they're not necessary, what are the beneficial aspects that you see of having regulations relating to anonymization process.

00:33:04.000 --> 00:33:13.000

Thanks, Adam. I'm not sure that they are necessary. I mean, I don't think that they are.

00:33:13.000 --> 00:33:30.000

I think you could just go with the best practices reference and you know, Khaled, very eloquently kind of laid out a lot of the really good best practices that exist today and that could be all that's required and that would be a very fulsome law.

00:33:30.000 --> 00:33:40.000

But that said, I do believe that consistent with what Khaled said, good laws and clear regs can be very beneficial.

00:33:40.000 --> 00:33:50.000

They provide that clarity to organizations as they conduct their business. So, it prevents that reticence risk that we might have if we don't have clarity.

00:33:50.000 --> 00:34:05.000

And it can also provide confidence to individuals. In this case, what we hope for is the clarity to allow innovation in a privacy respectful manner and then we hope to generate consumer trust in the digital or data ecosystem.

00:34:05.000 --> 00:34:24.000

I'm going to ground my comments about why I think this is beneficial in an actual fact situation. Some of the people on this call will be familiar with what happened with TELUS and our data for good program.

00:34:24.000 --> 00:34:26.000

But I'll just kind of briefly go through it to highlight where I think these could be beneficial, and why.

00:34:26.000 --> 00:34:40.000

So about 8 years ago, TELUS began building what we called our insights platform, and it was designed to generate insights from de-identified network mobility location data.

00:34:40.000 --> 00:34:55.000

So that's data generated from cell tower pings as devices move about our network. Now when we use the term de-identified and when I use it in my remarks today, we intended to convey the idea that it could not reasonably be traced back to an identifiable individual.

00:34:55.000 --> 00:35:03.000

It wasn't personal information. For clarity, maybe under law 25, that would be considered anonymized data.

00:35:03.000 --> 00:35:07.000

But I'm just going to continue to say de-identify today because that's the term that we have always used.

00:35:07.000 --> 00:35:18.000

No longer identifiable to an individual. So, we did spend years focused on how to do this in a privacy preserving way.

00:35:18.000 --> 00:35:35.000

And we consulted experts on our methodology, and then early 2019, TELUS had a new platform containing de-identified network mobility data that researchers could come on to and look for insights and it was certified for privacy by design.

00:35:35.000 --> 00:35:47.000

Immediately following that, the COVID-19 pandemic hit, and we realize that this de-identified data could benefit policy makers, epidemiologists, health researchers, governments, etc.

00:35:47.000 --> 00:35:58.000

We embarked on a pretty robust transparency campaign, talking to regulators, the media and some privacy advocates to ensure that they understood how this data and the insights could be shared in a privacy-preserving way.

00:35:58.000 --> 00:36:13.000

And then we launched our data for good program which made this de-identified mobility data available free of charge for government researchers and health authorities working on reducing the impact of COVID-19 and it all worked. The platform worked. Our comms worked. There was no backlash, the program worked, people seemed to understand and appreciate it.

00:36:13.000 --> 00:36:26.000

We even won privacy awards for it and got some international accolades for the program and its impact.

00:36:26.000 --> 00:36:43.000

Then again, fast forward to the end of 2021 and the environment had changed significantly and I think it's important to note how political environment and social environments can actually impact the way we look at these things and that's again another reason why clarity is really important.

00:36:43.000 --> 00:37:05.000

So, at this point, the pandemic had transitioned from a galvanizing to a polarizing issue. And fighting the pandemic is not necessarily seen as an all good thing, maybe, as certain media outlets began to put a negative spin on our data for good program as did some politicians. So, there was a new level of scrutiny, which was fed by a tremendous amount of misinformation.

00:37:05.000 --> 00:37:16.000

The Public Health Authority of Canada, many of you will remember, used our platform and allegations were made that they had been tracking Canadians using mobility data that we had provided.

00:37:16.000 --> 00:37:31.000

It was usually only implied, but sometimes stated outright that this was personal information. I found it really difficult at that time to have fact driven discussions in defense of our program, especially about the de-identification.

00:37:31.000 --> 00:37:41.000

We couldn't anchor our best practices in any clear standard, in regulatory guidance, or legislation. So, it was hard to give comfort to anyone or to the media.

00:37:41.000 --> 00:37:51.000

I had to give testimony in front of the Ethics Committee of Parliament explaining how the data for good program was leveraging only strongly de-identified data, not personal information of Canadians.

00:37:51.000 --> 00:37:56.000

And we were grateful that in the end the ethics report came out and found that we hadn't done anything wrong.

00:37:56.000 --> 00:38:11.000

But the overall experience left me acutely aware that using de-identified data requires, what I sometimes refer to as, a degree of bravery which it should not, and I think that's what Khaled was also referring to.

00:38:11.000 --> 00:38:16.000

And then the OPC launched an investigation into PHAC collection and use of data for good.

00:38:16.000 --> 00:38:21.000

And at its core, their investigation turned on whether the data was in fact de-identified such that it was no longer personal information, subject to the Privacy Act.

00:38:21.000 --> 00:38:36.000

So, it really did turn on our de-identification methodology. If the data we provided was not personal information, then the Privacy Act would not apply and it would not be a well-founded complaint to the OPC.

00:38:36.000 --> 00:38:50.000

So, they did find in the end that the complaints under the Privacy Act were not well founded. That was the OPC's finding and more specifically they concluded that this was due to the de-identification of the data and the suite of protections used in this case.

00:38:50.000 --> 00:38:57.000

I think the OPC decision is really important, and I've said that before because it lays out what we see as best practices for de-identification,

00:38:57.000 --> 00:39:03.000

a lot of which are very consistent with what Khalid talked about - all of which, I think really. There's a lot of detail in that decision and I really recommend reading it and studying it.

00:39:03.000 --> 00:39:29.000

But what we see overall is a focus on the identification technique: how the data is stripped and encrypted or otherwise transformed, appropriate aggregation if that fits, access and release model, and the contractual controls in place. I've often said that the decision makes it less necessary to be brave now when using data.

00:39:29.000 --> 00:39:42.000

It provides more clarity and similarly I find that these new regs under Quebec's law do provide more clarity and while different terms are used, the concepts are for the most part fairly consistent.

00:39:42.000 --> 00:39:50.000

I try to look at this and say, okay, well, would it have applied? Could we have done what we did under these regs? And I believe that for the most part we could.

00:39:50.000 --> 00:39:58.000

So, section 4 references the need for expertise. Khaled mentioned that as well. That's consistent with what we did.

00:39:58.000 --> 00:40:21.000

Section 5 outlines the need to start by removing direct identifiers, as we did. It goes on to talk about that it's necessary to then conduct a preliminary analysis of reidentification risk, taking into consideration what they call, and Khaled mentioned, these individualization, correlation, and inference criteria. So, as Khaled mentioned, these are not

00:40:21.000 --> 00:40:36.000

clear and they haven't been made clear in other jurisdictions. Frankly, I just choose to believe that the intention behind them is consistent with the concepts that we are a little bit more familiar with and consistent with our methodology.

00:40:36.000 --> 00:40:51.000

I think the idea of not being able to identify an individual within the data set, that just kind of almost goes to the definition of de-identified or anonymized data, the idea that you cannot correlate that data set with another data set and that you can't make inferences from other data sets about personal information.

00:40:51.000 --> 00:41:06.000

So, I'm just choosing to interpret those as being fairly consistent with what we've already seen as best practices, but I fully agree that it's proven a little bit problematic.

00:41:06.000 --> 00:41:19.000

And then finally, in the regs there's this concept of an overall reidentification risk assessment that uses techniques consistent with and it quotes "best practices".

00:41:19.000 --> 00:41:28.000

And I think it's really important to say that well, having a reg that says "consistent with best practices" doesn't sound like it's adding a lot of clarity.

00:41:28.000 --> 00:41:36.000

We had used best practices for our data for good program. But it wasn't clear to me that would help us in front of the ethics committee or the OPC

00:41:36.000 --> 00:41:44.000

because nowhere was there an indication that was what made it good enough. You didn't know what good enough was.

00:41:44.000 --> 00:42:00.000

And so regs like this, if by saying you can do this, if you do it in accordance with best practices, I would have so appreciated that clarity at that time because I didn't have it and I couldn't say to the ethics

committee, you can be comfortable that we did the right thing because this is what the law requires of us.

00:42:00.000 --> 00:42:07.000

And so, I think this clarity is really, really important. And then finally, and Khaled touched on this as well,

00:42:07.000 --> 00:42:09.000

I think the clarity around the final threshold of not zero risk, but very low risk is really helpful.

00:42:09.000 --> 00:42:19.000

And, particularly as it does include some criteria for assessing that risk, I think that would also be done in accordance with best practices.

00:42:19.000 --> 00:42:30.000

I do say that the comments about the consecutive nature of the analysis set out in the regs is maybe a little bit artificial.

00:42:30.000 --> 00:42:39.000

The idea of saying you strip it out and then you consider whether or not this, and then you do it, and analysis of that, and then you apply these controls, and then you do your final analysis.

00:42:39.000 --> 00:42:48.000

I'm not sure that's actually what happens in real life and in the way it plays out in terms of that consecutive nature of your order of operations.

00:42:48.000 --> 00:42:59.000

But I think it's consistent in concept with what would be a best practice today. And as I said, I really appreciate that clarity.

00:42:59.000 --> 00:43:07.000

In fairness, when I look back, I think the members of the ethics committee who were expected to assess whether or not following best practices was sufficient

00:43:07.000 --> 00:43:23.000

were left with kind of little to go on and it was hard to give them confidence as I said. In summary, I think regs like these can help so that is the good news, Adam. I think that there can be something really beneficial in clarity like this.

00:43:23.000 --> 00:43:24.000

That's the good news.

00:43:24.000 --> 00:43:45.000

Excellent comments. So just to summarize your comments. Not strictly required by the reading of the actual statute, especially with the cross reference, the inclusion of the reference to best practices, but nevertheless helpful because to the extent that it aligns that the provisions in the draft regs, which we're going to talk to because there's some challenges,

00:43:45.000 --> 00:43:54.000

with some of the detail you highlighted like in section 5, for instance: the order - we'd flag that internally.

00:43:54.000 --> 00:44:01.000

The order actually often makes no sense. The first thing you do is conduct the analysis. You wouldn't start the anonymization process.

00:44:01.000 --> 00:44:38.000

So, I understand what you mean, artificial and there's other examples. But conceptually as long as the regs encapsulate the core elements or base elements of what would be those best or very good practices, then it's beneficial because it anchors, it provides some clarity, and it would rely on organizations like TELUS. Like if you had that these were the regs that we were talking about in the ideal form into the Privacy Act, it would have been a completely different experience, maybe not eliminating it, but it would have been a different experience for TELUS.

00:44:38.000 --> 00:44:42.000

Am I encapsulating your comments correctly?

00:44:42.000 --> 00:44:44.000

Yeah, I think so.

00:44:44.000 --> 00:44:51.000

Those were very, very helpful. And Suzanne, any additional comments?

00:44:51.000 --> 00:45:07.000

Sure, thanks, Adam. You know, anybody who knows me, I think I would tend to agree with Pam that I'm not sure regs, technically speaking, are necessary given the clear reference to the generally accepted best practices in law 25.

00:45:07.000 --> 00:45:18.000

However, because, you know, I often believe that less is more and provides sufficient flexibility for organizations to tailor different circumstances.

00:45:18.000 --> 00:45:36.000

But you know, maybe just briefly before we sort of move on to some of the challenges in a little bit more detail, but sort of at a high level, some of the positives definitely in this version of the draft regs, some of this has been mentioned already, but the standard was zero risk on re-identification.

00:45:36.000 --> 00:45:58.000

Now we're not looking for that any longer. Concepts of reasonability have been added. There was something in there before that biometrics could not be anonymized. That language is not there any longer. They've also removed the prohibition on selling of anonymized data.

00:45:58.000 --> 00:46:21.000

And then, remove that steps need to be taken to make sure that anonymized data is only used for the original purpose kind of went counter to what law 25 says about anonymizing it for serious and legitimate purposes. And then the last one maybe, that I'll just mention here is, there was some language before about having to publish your governance steps on your website.

00:46:21.000 --> 00:46:52.000

There's no doubt in a world of increased transparency, organizations are doing more and more of that. I know at Sun Life we're trying to do that as well. But you don't want to be putting too much information up on your website that way. So you know, organizations will definitely, just generally speaking as part of their openness and transparency obligations under the private sector privacy law, will be doing that. But that was of some concern.

00:46:52.000 --> 00:46:53.000

So, I'll stop with that.

00:46:53.000 --> 00:46:58.000

Yeah, perfect. It segues, and even the beginning of your remarks segues to what really is going to be the guts of this conversation, some of the challenges or concerns with the draft reg.

00:46:58.000 --> 00:47:27.000

So why don't we begin with you, Suzanne, on that. As you read the proposed text, and separate of course from the beneficial aspects of this that you and Pam and Khaled have talked about, what are some of the challenges or concerns you have with respect to it?

00:47:27.000 --> 00:47:35.000

So, I really start with one fundamental one, and sort of let others speak to some of the other ones.

00:47:35.000 --> 00:47:51.000

But fundamentally speaking, I think if you think about the scope, just like with the statute, it needs to be clear what the scope for the regulations refers to and you know I'm going to pick up a little bit on part of your introduction, Adam, but maybe just outline it a little bit differently

00:47:51.000 --> 00:48:27.000

so folks can follow. So, Law 25 clearly mentions anonymization regards to really a single place, a single requirement. Rather than destroying personal information after business purposes have been completed, you're allowed to anonymize the information for a serious and legitimate purpose and I saw

Holly's comment in the chat there about how serious would be considered and thoughtful and not just sort of willy-nilly right. So that's one thing that's been added.

00:48:27.000 --> 00:48:54.000

The second thing is, Law 25 and section 23 is actually reflecting a current practice by many organizations in specific circumstances to use an anonymization rather than destruction once those business purposes have been passed, when there's still additional value in the data when it's anonymized, and that's been going on for a very long time.

00:48:54.000 --> 00:49:05.000

This is not a new flexibility that's being given to organizations, but rather it's carrying forward, if you like, current practice.

00:49:05.000 --> 00:49:14.000

And again, we're talking about end of life, for purposes that have been identified to individuals. Now what do you do?

00:49:14.000 --> 00:49:21.000

Do you delete it, or do you hang on to it? And so now clearly it says you're allowed to hang on to it and anonymize it

00:49:21.000 --> 00:49:36.000

for serious and legitimate purposes. And you did refer to the regulation making power in section 90 and it's clear it is "may" pass regulations. If they were required, I think it would say "must". And sometimes provisions don't come into force until then necessary regulations that accompany them are in force.

00:49:36.000 --> 00:50:00.000

But they do refer to section 23 like for purposes of section 23 any criterion terms applicable to the anonymization of personal information, so again making sure that those regs point directly to those criteria and terms.

00:50:00.000 --> 00:50:06.000

And then in the draft regs, section 3 of the draft regs refers to where?

00:50:06.000 --> 00:50:21.000

Section 23 of law 25 obviously, right. So, a reasonable read of the draft regulations as they are right now is that they are to law 25 and that they're limited to anonymization in the context of section 23 only.

00:50:21.000 --> 00:50:43.000

It doesn't mean that if an organization anonymizes data in another context and does it poorly that they may not still be subject to requirements under the private sector statute. But again, these regs were intended to focus on section 23 requirements to destroy or anonymize.

00:50:43.000 --> 00:50:54.000

But we wouldn't be here if there wasn't some uncertainty as to that scope. And it's not just the scope in and of itself

00:50:54.000 --> 00:51:02.000

that's the problem. But there are, Adam pointed to them, penal provisions related to that scope, right?

00:51:02.000 --> 00:51:23.000

And so, the fact that there is this uncertainty and some concerns - and I'm going to pass it over to Keren maybe to delve into a little bit more detail around why that scope could be problematic in this context, right? And then obviously, you know, you tag on the penal provisions there and that makes it even more relevant and real for organizations.

00:51:23.000 --> 00:51:24.000

So, I'll stop there and pass it over to you, Keren.

00:51:24.000 --> 00:51:25.000

Yeah.

00:51:25.000 --> 00:51:59.000

Yeah, yeah, I'll turn it to Keren, just to highlight one point you were mentioning, but just to put a punctuation on it, this is a statute that is designed to protect personal information. If you've effectively anonymized it then you would by implication address the privacy risk associated there. Again, even with that zero risk context.

00:51:59.000 --> 00:52:10.000

And so, this by implication is a provision that speaks to a post-anonymization contact.

00:52:10.000 --> 00:52:38.000

So, I think your points are critical. It's in the statute now. It's passed. But tying it to section 23, it's interesting and a comment we've heard from others, the critical nature of that. But Keren, your comments on Suzanne's points, but also more generally other concerns or challenges you have with the text of the draft regs?

00:52:38.000 --> 00:52:55.000

Thank you. Yeah, I just want to layer on and go a little bit deeper into some of the points that Suzanne made, for context, anonymization as Suzanne said has always been available as an option and that is codified especially in PIPEDA.

00:52:55.000 --> 00:53:17.000

So, when you take a look specifically at principal 4.5 in PIPEDA, 4.5.3, says that personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous.

00:53:17.000 --> 00:53:24.000

And it also goes on to say organizations shall develop guidelines and implement procedures to govern this. And so, you know, to me that's very similar to what Quebec codified.

00:53:24.000 --> 00:53:56.000

And again, at the beginning of this session when Adam looked at law 25 directly, the requirement for this regulation came from section 23. That again talks about when purposes for which the PI was collected are achieved that the organization should then either delete or alternatively can anonymize the data for serious and legitimate purposes.

00:53:56.000 --> 00:54:03.000

So unfortunately, the serious legitimate purpose requirement is baked into the law. So that's where that comes from.

00:54:03.000 --> 00:54:12.000

But to Suzanne's point, the entire basis for regulation comes out of section 23.

00:54:12.000 --> 00:54:26.000

And then if you think about maybe why that is, arguably when you're in this scenario, you have finished using the data for your original purpose, your consent to use that data has ended.

00:54:26.000 --> 00:54:32.000

Either the client has left or the specified purpose that they gave the consent for has come to an end.

00:54:32.000 --> 00:54:38.000

And so, you're just outside of the permissible uses under the consent regime that you originally had.

00:54:38.000 --> 00:54:50.000

So, when you're faced with that end of life moment, that is where you really should destroy the data or, as Suzanne said, there's a lot of value in the data that has nothing to do with the PI or alternatively sometimes it's just difficult to actually physically destroy data

00:54:50.000 --> 00:55:15.000

and it is just easier to anonymize it as just a methodology. And so, for that purpose, I guess they said you can destroy it or anonymize it for a legitimate purpose. So, in other words, if you're going to choose the route of anonymization, there needs to be, I guess, a reason why and that reason needs to be legitimate.

00:55:15.000 --> 00:55:20.000

I'm just trying to understand why that's there. That's, I guess, my working theory.

00:55:20.000 --> 00:55:28.000

But then, when you go to section 90 that speaks to the regs, the regs are tied again for the purposes of section 23.

00:55:28.000 --> 00:55:37.000

So, I think what the regs are lacking, but what is imperative, is that these regs should really only apply to anonymization

00:55:37.000 --> 00:55:49.000

when anonymization is being used at the end of life of the data. There are lots of other examples where organizations have lawful bases for creating anonymized data outside of an alternative to a destruction.

00:55:49.000 --> 00:55:55.000

It could be a method of safeguarding.

00:55:55.000 --> 00:56:01.000

It could be a method of using it for analysis or modeling.

00:56:01.000 --> 00:56:18.000

Or maybe, to Pam's point as part of a data for social good, which also is reflected in the new CPPA provisions that talks about de-identifying data in the context of sharing that data externally to your organization for a socially beneficial purpose.

00:56:18.000 --> 00:56:36.000

And even in the Quebec Law 25 there's a section 12 that has a consent exception for using data for study or research or to produce statistics if that data is de-identified.

00:56:36.000 --> 00:56:45.000

So, as I'm trying to say, there are lots of bases where you'd want to use anonymized data outside of an alternative to destruction.

00:56:45.000 --> 00:56:56.000

And why is this important? Some of the provisions of this regulation are quite onerous and wouldn't equally apply to those other scenarios nor should they.

00:56:56.000 --> 00:57:38.000

In that section 12 example, for study research or producing statistics, it uses the term de-identified, which is something that TELUS was also using which might be a slightly lower threshold than anonymization, but perhaps not. That ISO standard that Khaled was referring to out of Europe - I think its outside of Europe - that standard also refers to de-identified information, but I believe it's clearly talking about something more akin to anonymized. And maybe that's just a term of art because of the zero risk possibility that it's nearly impossible to get to zero risk and so it's difficult to call something anonymized.

00:57:38.000 --> 00:57:50.000

So, I really struggle with a lack of clear application to this regulation and a potential suggestion that it would apply across the board to any scenario of anonymization.

00:57:50.000 --> 00:58:01.000

And then also, separately from that, the concept of anonymization transforms the data in a way that makes it no longer PI.

00:58:01.000 --> 00:58:13.000

Once that data is no longer PI, there is no basis in law 25, PIPEDA or any other personal information protection law to regulate that data that is no longer personal information and that's gone to court before.

00:58:13.000 --> 00:58:23.000

There's the Gordon case, there's lots of cases that have gone to court to say this information is outside of the scope of privacy laws.

00:58:23.000 --> 00:58:59.000

And why that's problematic is that there are certain sections of the draft regulation that almost purport to regulate the data once it's already been anonymized. So, by way of example, I believe section 23.... Sorry, section 3 yeah, there it is. There's 2 parts to section 3. So, the first part says that before you begin the process of anonymization, you have to establish the purpose, which I think just ties back to the wording of the act that says you can choose to anonymize it

00:58:59.000 --> 00:59:08.000

as an alternative to destruction if there's a serious purpose for that. A serious and legitimate purpose. Okay, so we're going to choose to anonymize it and we're going to have a serious and legitimate purpose.

00:59:08.000 --> 00:59:26.000

Perhaps there's great value in the data with no risk to the individual that can be used. Some form of, let's say a credit model or something that can help prevent fraud or there's a serious need to keep the data and just strip it in a way that reduces the very likelihood of it being reidentified.

00:59:26.000 --> 00:59:37.000

But then the second half of section 3 goes on to say, but then if you want to use that data for another purpose, you have to go back and make sure that this new purpose is consistent.

00:59:37.000 --> 01:00:01.000

But I find this whole paragraph to be slightly problematic because arguably the data is now anonymized and has met the requirements in section 7 where we've done the analysis to ensure that we've taken into consideration the 5 elements to ensure that the re-identification risk is very low.

01:00:01.000 --> 01:00:11.000

So, if the data is already anonymized, it's outside of the scope of the act. So, if we've all of a sudden determined another purpose, why do we need to go back and make sure that purpose is consistent?

01:00:11.000 --> 01:00:21.000

I'm not sure what's the regulatory intent here. I understand the initial purpose, you need to have a valid purpose otherwise you should just destroy it. That was baked into the law. The information is now anonymized.

01:00:21.000 --> 01:00:32.000

It's a bit confusing. Now that it's anonymized, why do we need another valid purpose to use the data?

01:00:32.000 --> 01:00:43.000

If you think about, the TELUS example, if they put it on the platform, different researchers that are coming in that have already passed the legitimate test – they're in health care,

01:00:43.000 --> 01:00:55.000

the data is anonymized - does every specific use case need to be vetted? I mean, maybe, but to me, I'm just not sure what the basis for that is because we're outside of the scope of privacy laws.

01:00:55.000 --> 01:01:06.000

So, there might be ethical considerations and I'm not denying that. I just don't think that it should be grounded in a regulation associated with privacy laws.

01:01:06.000 --> 01:01:13.000

So, I'm really struggling with that. I'm also struggling with section 8

01:01:13.000 --> 01:01:16.000

in the regulation that talks about a regular reassessment of the information that's out there to make sure that it remains anonymous.

01:01:16.000 --> 01:01:22.000

So again, once the information has been anonymized, you're outside of the scope of the act.

01:01:22.000 --> 01:01:48.000

So, it's difficult to see how this applies and I don't dispute the fact that there might be a technological advance that might render an anonymization technique no longer valid, and I think that that's a real concern. But you can't judge us on 20/20 hindsight.

01:01:48.000 --> 01:01:57.000

You can't say, well today the information that you anonymized 10, 15, 20 years ago, is no longer anonymous and poses a risk, but that might actually be true.

01:01:57.000 --> 01:02:05.000

But that information, if it's been disseminated or has left the control of the organization, the reality is there's very little that can be done now.

01:02:05.000 --> 01:02:28.000

If the information remains in the organization's control or perhaps if the organization is embarking on a new set of data that they intend to anonymize, they can't use an old technique that is now no longer considered best practice. And I feel like it would be caught in that regard that when you start on a new journey of anonymization, you'd have to use then current best practice standards.

01:02:28.000 --> 01:02:47.000

And so perhaps what you did 10 years ago is no longer sufficient. But to suggest that you need to go back, and there's no endgame in sight, to look at data you might have anonymized in 10, 15, 20 years ago, to continuously regularly assess it to ensure that it remains anonymous when you might have lost control of that information…

01:02:47.000 --> 01:03:06.000

I think section 8 could be cleaned up a little. It's drafted in a way that's inoperable, ambiguous, and potentially out of scope of edited law. So again, I just think there are scenarios where section 8 wouldn't be able to work.

01:03:06.000 --> 01:03:14.000

And again, those are the scenarios where the information is perhaps in the public domain, or it's been there for many years.

01:03:14.000 --> 01:03:25.000

You know perhaps there's some tweaking we could do. I'm not saying it should be wholly struck out, that the whole reg should be struck out, but there's definitely room for improvement.

01:03:25.000 --> 01:03:45.000

So, before we go down that path of the discussion, I did want to say my main concern is the scope of the regulation and some of the sections of the regulation that are purporting to apply to information that should now technically be out of scope of the act.

01:03:45.000 --> 01:03:47.000

So, I'll pause there Adam just to see if there's more that needs to be added.

01:03:47.000 --> 01:04:02.000

Excellent comments and they align and dive deeper into comments we've heard from clients and other stakeholders.

01:04:02.000 --> 01:04:15.000

Khaled, you've listened to the conversation thus far. You also raised a couple of concerns and challenges in your initial comments. Can you share with us your perspective on some of the challenges or concerns with the draft regs?

01:04:15.000 --> 01:04:39.000

Yes, thanks, Adam. So, as I mentioned before, there are a number of things that are difficult to interpret in the current drafting. So, as I mentioned, the correlation, inference, and individualization criteria have been difficult to operationalize the way they're defined.

01:04:39.000 --> 01:04:59.000

If you narrow the definition and read into them a narrow scope, then they're workable, but not everybody has read into those criteria, at least the ones from the Article 29 working party document, not everyone has read into them in narrow scope.

01:04:59.000 --> 01:05:21.000

So those have been confusing in practice and including them just perpetuates that confusion I think unless, like I said, you deliberately narrow the scope in your reading of them. And then the two things that would be helpful to include are this anticipated recipient and consent for anonymization.

01:05:21.000 --> 01:05:24.000

But there are two other points which I think would be really helpful. And that kind of came out in the discussions we've had so far.

01:05:24.000 --> 01:05:35.000

One is to make a distinction between public and non-public data sharing or data releases or data disclosures.

01:05:35.000 --> 01:05:56.000

If an organization is sharing data publicly where they really can't control and have no oversight on who has the data and what they do with it, that there's a set of risks there, and a set of techniques that can be used to manage those risks. And then if you are sharing data with known entities, with business partners, with consultants, with researchers, etc.,

01:05:56.000 --> 01:06:04.000

but that's a non-public data disclosure, there's a whole set of other ways to manage that risk.

01:06:04.000 --> 01:06:17.000

And the methods you would use are not the same. So the idea of having additional controls, security controls, privacy controls, etc.,

01:06:17.000 --> 01:06:25.000

you can't really do that in a public data release. With the public data release, you put the data out there and it's gone, and you can't control who gets it and what they do with it.

01:06:25.000 --> 01:06:29.000

So, the whole idea of open data, open science, etc.

01:06:29.000 --> 01:06:44.000

That is different and the way you manage the risk there is different than if you are sharing data with a partner where you have a contract and you can impose controls and monitor and so on.

01:06:44.000 --> 01:06:49.000

So, when you think about anonymization, it's helpful to make a distinction between those two.

01:06:49.000 --> 01:07:05.000

Sometimes, not making that distinction can make it unclear what to do, what the practice should be, And then the other thing that would be helpful to make a distinction about is static versus dynamic data releases.

01:07:05.000 --> 01:07:12.000

So, if you have a static data set you disclose it once, it goes online, it's public or you share it and it's not public.

01:07:12.000 --> 01:07:20.000

That's a different scenario and a different set of concerns than if it's dynamic. If data is continuously being updated

01:07:20.000 --> 01:07:35.000

and potentially every update is being shared with different group of entities, different recipients. The process you put in place to manage that risk would also be different than for static data.

01:07:35.000 --> 01:07:58.000

So, if we're going to have regs that define guardrails in a way that ensures that they are applied consistently, then adding those clarifications would be helpful. Now, adding in all these clarifications means that we're going to get a more complicated set of regulations with more detail in them and so on,

01:07:58.000 --> 01:08:11.000

which goes back to the earlier point: well, if you're going to go into that much detail, why don't you just refer to best practices. But if you're going to write the regs, then it's helpful to put these guardrails in place and make those distinctions so that it's clear

01:08:11.000 --> 01:08:21.000

to the stakeholders what has to be done and what are the practices that are expected? So, if there's an auditor investigation,

01:08:21.000 --> 01:08:28.000

it's known what the criteria for evaluation or criteria that would be used are going to be. So those are the two additional things I will add:

01:08:28.000 --> 01:08:33.000

Public and non-public, and static versus dynamic distinctions.

01:08:33.000 --> 01:08:54.000

Alright, thank you. Pam, you as well mentioned in your earlier remarks at least a couple of the challenges or concerns, but can you share with us comments you have about what others have said and any additional concerns that you may have about this.

01:08:54.000 --> 01:09:12.000

Yeah, thanks, Adam. So, I think that what Khaled just said and those two additions are so important, because I think that level of nuance or granularity needs to be there if we're going to have rules like this because right now, as Keren put it, these are inoperable.

01:09:12.000 --> 01:09:33.000

And I think what happens is the rules have been made with a specific paradigm in mind, like either the static data set or the dynamic data set or the public release or private release and we haven't acknowledged the distinctions that are really important.

01:09:33.000 --> 01:09:57.000

And I just want to go back to the other thing that concerns me greatly - this concept of, to Keren's point, trying to govern data that is anonymized and that's no longer personal information. And I think again, if we were to try to do that, which in the context of a piece of privacy legislation is inapplicable

01:09:57.000 --> 01:10:36.000

but even so, it's incredibly challenging to start to say that rules can apply to anonymized data and things like having a register. Because I think when we get into the concept of taking what was originally personal information and then saying it's now anonymized, it can apply to a massive range of things, including, and I've said this before, for example, a hospital saying, well, there are 400 cases of COVID today. That came from personal information. Individuals with their personal health information that have been counted up and aggregated.

01:10:36.000 --> 01:10:50.000

That's a form of anonymization. That was personal information that has now been stripped of the identifiers and stripped of those aspects that make it traceable back to an individual and is a statistic that is super useful.

01:10:50.000 --> 01:10:57.000

So, does that now have to be governed under this legislation? Do they have to have a register? Do they have to go back and revisit that statistic

01:10:57.000 --> 01:11:04.000

at some regular period in the future? Do they have to document what the purpose is for it?

01:11:04.000 --> 01:11:06.000

If they're going to use it next month to figure out how much they're going to spend on hospital beds,

01:11:06.000 --> 01:11:17.000

does that have to have been implied in the original purpose for which they anonymized it when they were first releasing it to just tell people how many people have COVID??

01:11:17.000 --> 01:11:39.000

These are clearly kind of not the intention that anyone had when they developed the regs, but if we don't distinguish between full on data sets, which I think is the paradigm they have in their mind when they made the regs, versus other forms or pieces of data that we anonymize in other circumstances,

01:11:39.000 --> 01:11:42.000

then again, it becomes quite unworkable. So that worries me greatly.

01:11:42.000 --> 01:11:52.000

And for folks on the call, what you're referring to is on the screen, section 9 in particular sub 2,

01:11:52.000 --> 01:12:11.000

that once you've anonymized PI, you have got to have a register and what you're referring to is the statement that register has to be the purposes for which the body intends to use the anonymized personal information. You're giving a couple of just one of what would be an infinite number of use cases

01:12:11.000 --> 01:12:33.000

where that would be an administrative burden that is just certainly new, like novel, but otherwise might be extremely difficult if not impossible to actually adhere to. I don't want to put words in your mouth, but is that in essence the key point there?

01:12:33.000 --> 01:12:34.000

Okay.

01:12:34.000 --> 01:12:45.000

It is and I think it's not just section 9. It would also be section 8 which is the regularly reassess. I mean it clearly would be quite frankly kind of asinine to have to go back and say I've got to reassess when I said those 400 people today have COVID whether or not that now has to be treated differently, okay?

01:12:45.000 --> 01:12:53.000

Do I have to record that and document every time I've given out a statistic that came originally from personal information?

01:12:53.000 --> 01:13:04.000

It’s clearly not what anyone intends, but that’s what the words could be interpreted to say and if we’re going to make specific explicit rules like this

01:13:04.000 --> 01:13:13.000

that create administrative burden, then we need to be really explicit about the level of nuance and granularity about what exactly we’re talking about.

01:13:13.000 --> 01:13:25.000

Great comments. You’ve alluded to this already with your comments and I want to just turn to Khaled for our third question just before we open it up for comments.

01:13:25.000 --> 01:13:47.000

Khaled, you started by making a couple of suggestions. You’ve mentioned the challenges with the correlation, individualization, inference criteria. I don’t want to put words in your mouth, but it seems that you’re thinking those either have to be aligned, if not struck, because they might not be necessary.

01:13:47.000 --> 01:14:09.000

You spoke about the need to make a clear distinction between public disclosures, and we’ll call it nonpublic disclosures and the critical nature of making a distinction between static and dynamic data releases. And, if I’m getting this correct, by dynamic you mean data that’s continuously updated or sent to different recipients or a combination of that.

01:14:09.000 --> 01:14:26.000

First, I just want to clarify, am I accurately summarizing some of the suggestions you have, and separately would you have additional changes or amendments that you would recommend given the discussion that you’ve heard?

01:14:26.000 --> 01:15:20.000

I mean, I think the discussion we had around defining the purpose for using or processing anonymized data and updating that purpose over time, a number of questions have been raised about that, and I think that needs additional consideration and then the whole point of reanalysis over time. I mean current practice for static data, and this is for non-public static data, you share a data set and then the risk assessment to claim that the risk is very small or very low has a time limit on it - either 2 years, 3 years, so that can be determined and any of the assumptions that went into that analysis have changed during that period

01:15:20.000 --> 01:16:01.000

then you would redo the analysis to see if it changes the conclusion. Or, if nothing has changed, then after the period is expired, you would revisit the assumptions to see if the conclusion needs to be changed, that the risk is very small. So, that’s the current practice. Because you’re not really redoing the analysis every time, you’re just retesting the assumptions. And if you have many data sets, the assumptions are probably going to be the same across many of your datasets but if you have a dynamic data set…

01:16:01.000 --> 01:16:06.000

Oh, sorry, I think you just went on mute for 2 seconds.

01:16:06.000 --> 01:16:12.000

Okay. Sorry, my hand was moving. I must have pressed something by accident.

01:16:12.000 --> 01:16:24.000

In a dynamic context, this process may be harder to operationalize and you need a more efficient way of thinking about it.

01:16:24.000 --> 01:16:26.000

So, I think the idea of a reanalysis needs further consideration and maybe more nuanced to make it operational to get it to work in practice.

01:16:26.000 --> 01:16:48.000

So those would be the two other things that I think need to be looked at further from an operational perspective to see whether any additional nuance is needed to make them more scalable in practice.

01:16:48.000 --> 01:16:59.000

Just so we're keeping track: one is, at minimum, a refinement to the reference to the continual reassessment, right?

01:16:59.000 --> 01:17:12.000

That's section 8. Yeah.

01:17:01.000 --> 01:17:12.000

Assessment in section 8 and then what was the first, just as a high level, just as we keep up?

01:17:12.000 --> 01:17:22.000

Yeah.

01:17:22.000 --> 01:17:23.000

Okay.

01:17:23.000 --> 01:17:40.000

And then section 3, you establish the purposes for which it intends to use the anonymized personal information. If that purpose has changed it must be consistent with Section 23 and section 73, which implies if the purposes change you have to perform a reexamination which, as we discussed before, that essentially is regulating the anonymized data and that raises a whole set of other issues.

01:17:40.000 --> 01:17:48.000

Perfect. Keren, if you had to make 2 or 3 changes, what would you recommend of the revisions to the draft reg?

01:17:48.000 --> 01:18:15.000

Okay, I would ideally remove the entire second paragraph of Article 3 or alternatively just to ensure that if you want to use the anonymized data for a new purpose, just consider whether there's any material change to that circumstance and whether or not that impacts the anonymization as opposed to the purpose that you're trying to use it.

01:18:15.000 --> 01:18:20.000

Like maybe this new purpose somehow if you're marrying a data set with another data set, like maybe the anonymization risk is different.

01:18:20.000 --> 01:18:32.000

So maybe just assess the risk of anonymization to make sure that the data is still anonymized. Focus less on the new purpose itself.

01:18:32.000 --> 01:18:47.000

So, article 8, Khaled was talking about maybe limiting the time frame. I also think it should be limited to information that's still under the control of the organization.

01:18:47.000 --> 01:18:57.000

And it should be periodically and somehow connected to material events as opposed to just a routine regular assessment.

01:18:57.000 --> 01:19:28.000

I'm also struggling with article 4, the anonymization expert. I understand that TELUS consulted several. Sometimes organizations, especially smaller ones, so less Telcos and banks, but smaller organizations might not have a designated expert and may just relying on best practices would be sufficient or vetting those practices. So, I think that some smaller organizations might struggle with the requirement of having a dedicated supervised person.

01:19:28.000 --> 01:19:38.000

So, I see Khaled's hand is up, but perhaps there's another alternative to housing an individual in your organization that can do this.

01:19:38.000 --> 01:19:51.000

Sorry. I just want to present a counterpoint to that last one. I've seen a lot of organizations that try to do this without the expertise and it's a very risky thing.

01:19:51.000 --> 01:20:16.000

If you don't have the expertise, you shouldn't be doing this because chances are you're not going to do a good job. And I've seen that many times where we come in and try to rescue someone who has implemented anonymization practices and something happened, and they have to fix it. So, that's in the US HIPAA,

01:20:16.000 --> 01:20:23.000

and I think it's a really good requirement because it ensures a certain level of good practices are always implemented.

01:20:23.000 --> 01:20:45.000

I know it's hard for small organizations but...I guess this is where they can hire a consultant - they can bring someone in for a moment in time, as opposed to putting someone on the payroll. I just think some organizations might struggle with this requirement if it was someone that had to be a part of the organization.

01:20:45.000 --> 01:21:07.000

And then finally my big overarching comment is that the entire set of regs needs to have a preamble that limits the scope of the application of this section to anonymization under section 23 as an alternative to destruction as opposed to having just broad application.

01:21:07.000 --> 01:21:10.000

Thank you, Pam.

01:21:10.000 --> 01:21:11.000

Your suggestions.

01:21:11.000 --> 01:21:18.000

Well, I've already mentioned a couple that I think in terms of adding nuance if we're going to leave it the way it is.

01:21:18.000 --> 01:21:36.000

But I think there been a few comments back and forth around, and I think Khaled said, if we're going to have this in here, then we need to get the details of the nuance correct. And I think it might be better to just go with best practices

01:21:36.000 --> 01:21:49.000

when we're talking about these things, Also agree with all of the things that Keren just said. But I think if we just went to best practices and rather than trying to get specific and prescriptive because I do worry that we're going to go down a rabbit hole of needing to have a tremendous amount of detail and that gets worrisome,

01:21:49.000 --> 01:22:06.000

so, I think it's a bit of an Adam-ism but less is more here. And if we can stick with best practices, then that can shift over time in the same way that we have historically done that in the security context, security standards.

01:22:06.000 --> 01:22:23.000

What's acceptable from a security standard is different today than it was 3 years ago, even a year ago. We need to be able to stay up to date on what is the best practice and the more that we write in here, the more confusing it might be and the more likely we are to end up with a regulation that is actually self-defeating.

01:22:23.000 --> 01:22:33.000

So, I think the clarity is still there - if we talk about best practices and increasingly we have more best practices,

01:22:33.000 --> 01:22:56.000

we've got findings and decisions, we've got ISO standards, we've got more and more experts out there, but I think if we've got the clarity that that's the standard that's required in whatever the circumstances are, then I think that's sufficient and probably safer, and will result in a better more effective law that will protect privacy.

01:22:56.000 --> 01:23:06.000

Great comments and last but definitely not least, Suzanne, recommendations if any supplemental to the ones you've heard or anything you want to just reiterate.

01:23:06.000 --> 01:23:07.000

Okay.

01:23:07.000 --> 01:23:21.000

Yeah, so maybe just a few and I said it at the top of my comments too, less is more because we need to avoid being too prescriptive or else, we will fall prey to having regulations that will quickly fall behind.

01:23:21.000 --> 01:23:40.000

And so, we don't want to do anything in these regulations that chips away at the importance of generally accepted best practices. To go through the regs with a fine-tooth comb to make sure is there anything in here

01:23:40.000 --> 01:23:52.000

that would take away from an organization following generally accepted best practices. And some people look at generally accepted best practice and say, well, those are subjective.

01:23:52.000 --> 01:23:54.000

They are and they aren't. Courts hold organizations to generally accepted best practices for your industry all the time.

01:23:54.000 --> 01:24:07.000

So, this is not really a new concept. They are always relevant when it comes to the type of industry, the sensitivity of data.

01:24:07.000 --> 01:24:16.000

We talked about internal versus external use. So, anything that chips away at generally accepted best practices I think should be removed or adjusted.

01:24:16.000 --> 01:24:25.000

Resist attempts to repeat what we find in the law, in the regs, unless it's there to reinforce the importance of generally accepted best practices.

01:24:25.000 --> 01:24:40.000

Avoiding language like a register. You know, we updated the private sector law to get rid of some of that non-technology neutral, narrower type view, of how maybe a business run.

01:24:40.000 --> 01:25:18.000

So, we should avoid language like that. And then maybe the last one and this goes to some of what Khaled mentioned before too is we should avoid the combination of words that create confusion. So, if you take the example of no longer requiring zero risk. Well, then don't put irreversible at the front end of that paragraph or sentence. Sort of the same thing, if you're going to require generally accepted best practices, don't throw something in there that causes confusion. And so, I think being really sort of cognizant of that would go a long way.

01:25:18.000 --> 01:25:20.000

And with that I'll stop.

01:25:20.000 --> 01:25:26.000

Great comments. Just before we turn to the floor, the one thing, and I think it came up implicit in some of the comments, but just go to section 3.

01:25:26.000 --> 01:25:49.000

Well, first, it's more of the regulation, Catherine, the regulation authority in the section just above. The regulations are determining the criteria applicable to the anonymization. This is the process one would think from the wording of that.

01:25:49.000 --> 01:25:54.000

Go to section 3 in the regs.

01:25:54.000 --> 01:26:01.000

One recommendation - I think this picks up and built upon Keren's comment - just remove section 3 altogether.

01:26:01.000 --> 01:26:13.000

That's not about the process for anonymization. That's about this purposes aspect, which as we've talked about and there were a number of excellent comments. is just challenging. Why do you even need that?

01:26:13.000 --> 01:26:19.000

This is about the process. Perhaps this is even *ultra vires* threat to the regulation authority. But that would be the case.

01:26:19.000 --> 01:26:30.000

And then flip to section 9. I want to pick up, Suzanne, on your points and then it was emphasized in particular by Pam.

01:26:30.000 --> 01:26:52.000

Let's not use the word register, but is really any of this section necessary? If you're going to do an appropriate assessment there will be documentation in respect of that. Why do you need this register? Especially number 2 which is the one that Pam very eloquently cited all sorts of challenges with.

01:26:52.000 --> 01:27:02.000

So, we're hopeful. I think you're hearing across the board, and I think this is a comment we've gotten from a lot of folks that, less is more.

01:27:02.000 --> 01:27:57.000

Don't make this unnecessarily complicated. This is an incredibly nuanced area. Start with, Khaled, a globally recognized expert, who could speak volumes about how nuanced this gets. Less is more - that will serve a lot of the benefits that folks have talked about but at the same time not create these operational challenges and arguably overreach at least, vis-à-vis the public policy purpose of what the statute is generally, as you mentioned a couple of times, Suzanne and others, as well, as what these regs really need to do, which is just give some baseline on what is simple elements of the best practices for the anonymization process aligned with what's already been out there, and in many cases, have been done for a while.

01:27:57.000 --> 01:28:03.000

So, I think those were excellent comments from folks on the panel.

01:28:03.000 --> 01:28:14.000

Let's open it up for comments. We're very interested in your comments on what you've heard or certainly questions for the panel, each of whom are tremendous experts in this area,

01:28:14.000 --> 01:28:25.000

and one or more of them may be able to respond to the particular question. There's options.

01:28:25.000 --> 01:28:32.000

We really welcome folks to raise their hand. Give some verbal comments. If you're so inclined that would be really, really helpful.

01:28:32.000 --> 01:28:44.000

And secondly, it would be otherwise helpful just if you put in comments, I know there's a number of comments already.

01:28:44.000 --> 01:28:55.000

I see close to 60 comments in the chat, and we could through, Katelyn, who's moderating those can share those comments and we can comment on those and any questions.

01:28:55.000 --> 01:29:07.000

So, I'll just turn it over to you, Katelyn, to moderate the next part and Catherine let's just leave this up on the screen because certain of the comments might focus on provision so we can have that in front of us for the discussion.

01:29:07.000 --> 01:29:15.000

So, Katelyn over to you. I don't know if anyone's hand is up for a comment.

01:29:15.000 --> 01:29:21.000

We do have a hand up if you'd like to start us off, I will unmute you.

01:29:21.000 --> 01:29:27.000

Great to have you, nice to hear from you. Very interested in your comments.

01:29:27.000 --> 01:29:31.000

You too, Adam and what a small world seeing people who I've worked with before.

01:29:31.000 --> 01:29:57.000

It's great. So, the first thing that I thought was why have regulations for something that under law is no longer personal information or requirements. And then, the second thing was about the register. I mean, that sort of strikes me as well. We have privacy impact assessments just for that purpose.

01:29:57.000 --> 01:30:06.000

So, we already have a register in a sense, but I don't think the formalization of one actually adds any value.

01:30:06.000 --> 01:30:16.000

And that actually is the question I have for a number of these provisions - what problem are they trying to solve or what value are they adding.

01:30:16.000 --> 01:30:23.000

And in a lot of the cases that were spoken of, especially some of the things that Keren talked about,

01:30:23.000 --> 01:30:34.000

I really question, where is that value? And then some of the requirements are going to be outlined in further guidance

01:30:34.000 --> 01:30:45.000

from the CAI, but then there becomes a conflict between what you have to comply with under the guidelines versus what's in the act.

01:30:45.000 --> 01:30:52.000

And that came up in the issue of the requirements for consent. And do we want to go down that rabbit hole?

01:30:52.000 --> 01:31:01.000

So, I think a lot of the comments that were made about Law 25 when it first came out you could apply to these ones.

01:31:01.000 --> 01:31:09.000

Thank you for that. I mean you are picking up on several themes. First less is more, at minimum,

01:31:09.000 --> 01:31:40.000

if I'm hearing you correct. Secondly, if you go to to the register, and to your point, I can tell you that in terms of comments we received at the firm and this is from clients, but also just with stakeholders, this is one that was problematic and perplexing operationally for many folks.

01:31:40.000 --> 01:31:41.000

Yeah.

01:31:41.000 --> 01:31:54.000

The word register was a little bit of a mini lightning rod like what do you mean? A register seems a little bit dated but as you mentioned when you do a PIA, you'll document the relevant things in there. Why do you need another administrative requirement separate and apart from those documents which are relevant?

01:31:54.000 --> 01:31:58.000

It's a great point and I don't think it's a small point.

01:31:58.000 --> 01:32:05.000

I think it's very significant. Every single provision I think you eloquently set it out.

01:32:05.000 --> 01:32:21.000

We're recommending, and again a recording of this is going to the Quebec government, we're recommending stick only with the bare minimum of which is required to provide the clarification that would be helpful as Pam very eloquently said it.

01:32:21.000 --> 01:32:39.000

Everything else is going to risk adding complexity, administrative burden and otherwise highlight the novelty or distinctiveness of Law 25 or the amendments brought in by Law 25 from many other statutory regimes.

01:32:39.000 --> 01:32:42.000

So, I think your points are just dead on and really picking up thematically on the comments we've received.

01:32:42.000 --> 01:32:53.000

Others want to comment?

01:32:53.000 --> 01:33:06.000

I think that's a valid implied assent to the value of your comment. Is there anyone else who has put their hands up?

01:33:06.000 --> 01:33:20.000

We did receive a question before the session, Adam, and I think it will help ground the comments as well and in practical examples just like Pam had given rather than keeping it esoteric, as one of your favorite words.

01:33:20.000 --> 01:33:31.000

What are the real pragmatic use cases of anonymization for organizations except as an alternative method to destruction, especially for the financial sector?

01:33:31.000 --> 01:33:40.000

In other words, does truly anonymized data retain any value for an organization and if so in which context and for what types of use cases?

01:33:40.000 --> 01:34:24.000

I mean, we have great panel on this, I mean, maybe we take it out, it's not really just banking, it's anything. Pam, maybe you could just build upon your point that you made about those use cases. You gave a couple, but certainly our clients across the board, there would be an infinite number of use cases where every day they're using data that is in anonymous form to achieve a myriad of business purposes, that by implication wouldn't have any privacy issue because the data has been anonymized. But Pam, I'll turn to you because you could speak from an organizational perspective and then the other panelists can weigh in.

01:34:24.000 --> 01:34:31.000

Yeah, absolutely. Honestly, the sky's the limit, as you say - an infinite number.

01:34:31.000 --> 01:34:41.000

So, in the context of the data for good program that I referred to with de-identified mobility data, we were able to see large-scale movement patterns.

01:34:41.000 --> 01:34:57.000

For example, during COVID, we were able to see were people responding to different policy decisions that were made. So, when the government came out and said, please don't go to your cottage this weekend, did people listen? We could see, did people go to their cottage that weekend?

01:34:57.000 --> 01:35:08.000

You know, did the emotional plea work? We could compare that to other jurisdictions where they may have made an absolute rule.

01:35:08.000 --> 01:35:16.000

Did that impact people differently? Was it more effective, less effective? So, you know, large scale patterns.

01:35:16.000 --> 01:35:35.000

But that's true in every possible area of a business or in trying to solve social problems. Health data, absolutely, like de-identified health data to understand: are people who are going to their doctors and getting prescriptions and filling those prescriptions getting better at a faster rate?

01:35:35.000 --> 01:35:45.000

These are big picture answers to questions. And when we're looking for patterns and trends, which is so much of what we are always looking for,

01:35:45.000 --> 01:35:51.000

we don't need identifiable data. De-identified data will do the trick.

01:35:51.000 --> 01:36:10.000

Absolutely, when we look at things like AI and the power of AI, which I don't think anyone is questioning these days, it comes from the power of being able to look at trends and patterns and we don't need identifiable data to create those trends and patterns.

01:36:10.000 --> 01:36:18.000

So, all of the things that you can do with AI, we can use de-identified data to do or almost all of them.

01:36:18.000 --> 01:37:03.000

But every day in the business, in terms of, how many people who use this product would like that product, this can be done with deidentified data so it's really the sky's the limit and there's so many more opportunities. I think businesses are often missing an opportunity to use de-identified data in certain circumstances where they could be doing so. And they're using personal information instead or they're simply not going through this process and are missing out on those big picture trends. But, at a government level, social level, health for sure, and business level, they're just endless opportunities to use it, I think.

01:37:03.000 --> 01:37:30.000

Yeah, and as you're talking, I was thinking for years this has been done with, actually 99.999% of the time, zero issue. Anonymized data used for business strategy, anonymized data used for improving products and services, or most critically the innovation that you're speaking about, AI just being yet the latest part of those innovative efforts.

01:37:30.000 --> 01:37:57.000

So huge things, which is why a set of rules that applies to anonymized data is inadvertently and has, in my view of this, and we've heard this from other folks, unintended consequences. So, this seemingly small on a requirement: Oh, just create a register and keep track of all these purposes.

01:37:57.000 --> 01:38:05.000

The burden on that, especially for larger organizations, would be beyond events. And, frankly, section 9, again, as we mentioned before, is it even necessary?

01:38:05.000 --> 01:38:25.000

Which leads to that. And really what value does it bring? I think it's a great point for each of these provisions to be highlighting. Katelyn, any other hands up for comments?

01:38:25.000 --> 01:38:27.000

Rosario just put her hand up, so we'll unmute you.

01:38:27.000 --> 01:38:31.000

Great.

01:38:31.000 --> 01:38:42.000

Hi there, just wanted to echo Adam, what you just said about the burden on smaller organizations or organizations perhaps that, have a high volume of work.

01:38:42.000 --> 01:38:52.000

And that's certainly the case in the health care industry as Pam mentioned where you have constant reporting and dashboards for evidence-based decision-making.

01:38:52.000 --> 01:38:59.000

So, dashboards are used by Toronto Public Health or public health units. They're used by the government at the ministry level.

01:38:59.000 --> 01:39:04.000

How many homeless shelters do we need to open up? What do we need to do about this?

01:39:04.000 --> 01:39:16.000

I mean every single decision-making that one would hope that is made by the government is based on data and internally certainly decisions are made using data

01:39:16.000 --> 01:39:52.000

that has been de-identified for whatever purposes or even included on websites. And even, you know, those individuals that conduct at least at the organization where I work, they do they do projects and then those get reported in presentations and in journals and manuscripts and lectures and a number of different dashboards. I mean, it's just, astronomical when you think about the number of instances once the data has been de-identified that it then gets leveraged and used for accurate decision-making.

01:39:52.000 --> 01:39:59.000

So, it does seem unwieldy to me to have that section 9 in there.

01:39:59.000 --> 01:40:00.000

So, just a comment on my end, Adam.

01:40:00.000 --> 01:40:08.000

Okay. That's great because you're looking at it and I think it was mentioned a couple of times now, but I think it's a very helpful prism to look at these things.

01:40:08.000 --> 01:40:22.000

What's the value? Keeping in mind not just the specific words, it'd be good to have these things, but even given the burden

01:40:22.000 --> 01:40:33.000

that would be placed and we've had discussions in a number of different contexts that there is a freight train of regulatory burden coming down

01:40:33.000 --> 01:40:46.000

nationally - Law 25 in particular, but nationally on companies across the board, and it's imperative from our view, from a public policy perspective, that governmental authorities who are creating these instruments really bear down and include what is going to be helpful.

01:40:46.000 --> 01:41:11.000

Aligning for the overall purpose, consistent with the spirit and intent of the act and just absolutely remove any unnecessary administrative element that's not going to serve a valuable purpose. And we've had a number of comments, eloquently supplemented by yourself, Rosario, that highlight section 9 - the suggestion, but why require it?

01:41:11.000 --> 01:41:20.000

Just doesn't seem necessary at all. Anybody else have their hand up, Katelyn?

01:41:20.000 --> 01:41:21.000

Khaled does.

01:41:21.000 --> 01:41:23.000

Oh great.

01:41:23.000 --> 01:41:26.000

I just have a comment in defense of section 9?

01:41:26.000 --> 01:41:27.000

Okay.

01:41:27.000 --> 01:42:00.000

Well, as you comment, I just have a question for you. Assuming, and you might be getting to this, but assuming you have performed an appropriately - that would be tailored for the circumstance – appropriately rigorous deidentification assessment, risk re-identification, etc. and you've documented that, and it's there, what is the value of section 9? That would be really helpful to hear.

01:42:00.000 --> 01:42:22.000

Well, it's to make sure that it's documented because when things go wrong the first thing you bring out is the documentation and it may happen 2, 3 years, 5 years after the fact, and having that clear documentation would be very important in those cases, if there's an investigation or an audit of some sort.

01:42:22.000 --> 01:42:41.000

And the question I get asked often is what should be in that documentation? Give me the table of contents so that I can make sure that I cover everything that needs to be covered. So, in that sense, section 9 is helpful because it gives you a little bit of that table of contents.

01:42:41.000 --> 01:42:45.000

But I think the documentation is important. I don't think it's complete, but it's a start.

01:42:45.000 --> 01:43:04.000

It covers some of the important things. But nevertheless, having the documentation is important because when things go wrong, you will rely on that documentation to explain what you did, the rationale for the decisions and the process that was followed, etc.

01:43:04.000 --> 01:43:25.000

Right, so go to section 5. I think we should bear down on this because I think there would be alignment that, first of all, best practice, I mean, best standard practice that you conduct an appropriate analysis of the re-identification risk.

01:43:25.000 --> 01:43:36.000

And when you do that analysis, Khaled, I'm assuming the organization will document and keep relevant documentation in connection with that.

01:43:36.000 --> 01:43:42.000

If you have it there, if you have documentation - no one's doubting the value of documentation -

01:43:42.000 --> 01:43:50.000

why would you need to separate register? Or is your point that it's not necessarily the register, it's the documentation?

01:43:50.000 --> 01:43:51.000

Okay.

01:43:51.000 --> 01:43:55.000

It's the documentation. You need to put it somewhere. It's important. If you can make it explicit, that's better just to make sure it gets done.

01:43:55.000 --> 01:44:05.000

But removing a documentation requirement completely, I think, will result in lack of documentation, which can be problematic in practice.

01:44:05.000 --> 01:44:11.000

Yeah, because the comments we've heard, and go back to section 9, Catherine, with respect to this is number one,

01:44:11.000 --> 01:44:14.000

and I like the comment today, like this register term itself seems a little bit dated, but that's the most minor of points.

01:44:14.000 --> 01:44:37.000

The number 2 is problematic for all sorts of different reasons, and then the comment that I've received, that we've discussed offline with several clients and other stakeholders, is why do you even need this IF there's appropriate documentation in connection with the risk assessment?

01:44:37.000 --> 01:44:54.000

If you do a PIA, a documentation, you don't need a separate register to deal with it thereafter. So, I think there's alignment, a common ground - it's the documentation piece. Let's not have any extra burden. Is that fair?

01:44:54.000 --> 01:44:58.000

Yes, yeah, that's fair.

01:44:58.000 --> 01:45:04.000

Are there other questions or comments? Just mindful of time.

01:45:04.000 --> 01:45:05.000

Yeah.

01:45:05.000 --> 01:45:40.000

Adam, I was just going to just add one little teeny piece to that and that's I don't think it's the documentation that's the issue and I think you've highlighted that. I think it's the scope of what is being documented and I saw in the in the chat, Rhonda Wing has put a great comment in there about how important it is to stress test section 9 with real life scenarios and to understand what a hurdle it risks constituting to essential decision-making and information dissemination.

01:45:40.000 --> 01:45:41.000

Yeah.

01:45:41.000 --> 01:45:43.000

So again, back to the, well, there are 400 beds filled with COVID patients. Does that have to be documented because that was a stat that was derived originally from personal information?

01:45:43.000 --> 01:46:00.000

Like that clearly can't be what is contemplated here, but it's not excluded. So, that's my concern with section 9 - it's the scope of its application more so than the concept of documentation.

01:46:00.000 --> 01:46:01.000

Yeah.

01:46:01.000 --> 01:46:03.000

I mean, I'm all for documentation. We documented everything we did do, and we do big important de-identifications.

01:46:03.000 --> 01:46:10.000

I think that's a great point to like punctuate. It's the scope issue. And then especially with two and one.

01:46:10.000 --> 01:46:37.000

But 3 and 4 and 5 would seem to be replication of what you would have otherwise typically done and certainly all of them, each of these elements should, if you're going to even keep section 9, needs to be carefully viewed with a very practical lens and I think Rhonda's point is excellent.

01:46:37.000 --> 01:46:46.000

So, there's a comment here. Section 9 is in order. Can you read that? Because I want to make sure there's common ground. I think there is.

01:46:46.000 --> 01:46:49.000

The latest comment. Katelyn, could you read that?

01:46:49.000 --> 01:47:10.000

Okay. In my opinion, section 9 is in order. Privacy legislation is big on transparency. I understand that a PIA would likely have been completed before the latter anonymization. However, the anonymization

increases the use of this information, which by the way is no longer personal information, but was derived from personal information, which is the point that Pam has made.

01:47:10.000 --> 01:47:18.000

In my opinion, it provides individuals the ability to provide an informed consent when initially providing their personal information.

01:47:18.000 --> 01:47:31.000

Right, I think that point, which I understand, I think it's really important. And several of the panelists, mentioned this and it's critical.

01:47:31.000 --> 01:47:40.000

The legislation applies to the protection of personal information - the collection, use, and disclosure of personal information.

01:47:40.000 --> 01:47:16.000

This legislative scheme, the proposed legislative scheme, that's replacing PIPEDA, the CPPA, other legislative schemes globally, has a scope limitation where the data is personal information and therefore, there's a privacy interest, of course that would vary with the sensitivity of the data. Once the data is effectively anonymized, you've effectively addressed that privacy interest. At least that would be the starting proposition and what section 9 goes to was not necessarily transparency.

01:48:16.000 --> 01:48:37.000

It sets out 5 things, at least, several elements of which would be already documented in the context of performing just the risk assessment, which would be consistent with best practice.

01:48:37.000 --> 01:48:48.000

In other words, if you remove 9, but follow best practice, there would be adherence to certain aspects of this.

01:48:48.000 --> 01:49:16.000

But critically, there's a couple of aspects of this that at least clients are telling us and you're hearing on this call that would be potentially a minimum hugely challenging, if not almost practically not feasible to keep track of purposes of non-identifiable data. Doing it and for all the reasons that are there.

01:49:16.000 --> 01:49:18.000

So, I think there's common ground, but I wanted to highlight my reading of this. This isn't a transparency provision.

01:49:18.000 --> 01:49:32.000

This is read as a supplemental administrative obligation on organizations to create a register distinct from the assessment that would typically contain the relevant aspects of this.

01:49:32.000 --> 01:49:46.000

I'm interested in other panelists comments on that.

01:49:46.000 --> 01:49:51.000

Again, will I assume. Well, let's turn Katelyn to, are there any other?

01:49:51.000 --> 01:49:55.000

Sorry, Adam. I think, just to your point, that I would agree. I think I'm struggling with the word register

01:49:55.000 --> 01:50:19.000

and the prescriptive nature of this requirement. If anything, I would think you could just simplify to say that organizations have to be able to demonstrate accountability or compliance with this regulation should they be called upon to do so or should maintain a record demonstrating their compliance. Like, something a lot simpler

01:50:19.000 --> 01:50:35.000

and less prescriptive. I'm not disputing that we should do what this says and be able to demonstrate our accountability and compliance, but that's what we have to do across the board with all privacy requirements, being able to demonstrate that we've met this requirement and that requirement.

01:50:35.000 --> 01:50:41.000

So, this is the first time that I'm seeing such a prescriptive way of doing that.

01:50:41.000 --> 01:50:48.000

Yeah, it's interesting and it's generating a lot of comment. Your suggestion, Keren

01:50:48.000 --> 01:51:07.000

would align with the spirit and intent. I don't want to put words in folks mouth because there's folks making comments on this, by dealing with, we'll call it demonstrable accountability, at least vis-à-vis this, at the same time without the prescriptiveness, aspects of which would be almost impossible to implement.

01:51:07.000 --> 01:51:19.000

We have scores of clients that would find it exceptionally difficult to adhere, at least to this purposes piece.

01:51:19.000 --> 01:51:26.000

Like I'm not even sure when we factor this number two, I'm not sure of the purpose or the value of it but, even if you were aligned on there, it's just not going to be feasible.

01:51:26.000 --> 01:51:35.000

Larger enterprises would have like multiple staff doing this. That's all they'd be doing

01:51:35.000 --> 01:51:41.000

one would think to operationalize.

01:51:41.000 --> 01:51:44.000

I'm interested in comments on that, but that was our view and that is the comment -

01:51:44.000 --> 01:51:46.000

I'm just reflecting - multiple comments we have received from

01:51:46.000 --> 01:51:54.000

clients who've actually looked and meditated on some of these provisions. Any other comments? Katelyn?

01:51:54.000 --> 01:51:55.000

Yes.

01:51:55.000 --> 01:52:04.000

Wait, sorry, Adam. Just before we leave that, don't forget section 3 requires that before you anonymize the data, you have to first establish the purpose that you're intending to use it for.

01:52:04.000 --> 01:52:10.000

So again, as long as you can demonstrate compliance, then establishing one purpose, the initial purpose for anonymization, is very different than what's required under section 2 of section 9,

01:52:10.000 --> 01:52:23.000

which is all the purposes that you intend to use it. Really as long as you've got the one that you initially anonymized it for, you can demonstrate compliance.

01:52:23.000 --> 01:52:34.000

Yeah. Yeah, look, there's great comments we're receiving upon this. It's certainly an interesting discussion, comments are worthwhile considering.

01:52:34.000 --> 01:52:40.000

Katelyn, any other comments? I'm just, mindful of time we just have a few minutes.

01:52:40.000 --> 01:52:41.000

Yeah.

01:52:41.000 --> 01:52:45.000

We said 2 hours, we meant this to go about an hour and 45 min max.

01:52:45.000 --> 01:52:49.000

For sure. So, there is a written comment that I would like to get to on section 8, but just to make sure that I'm not cutting anyone off on their ideas on section 9,

01:52:49.000 --> 01:52:56.000

I'll call on David Elder and then to Surtinder Bal also has comments.

01:52:56.000 --> 01:53:07.000

Great. David, nice to hear from you. Thank you.

01:53:07.000 --> 01:53:17.000

David, I've unmuted you, you should be able to make your comments.

01:53:17.000 --> 01:53:22.000

All right, I'll pass it over to Surtinder. David, if you're okay.

01:53:22.000 --> 01:53:23.000

Okay, there we go.

01:53:23.000 --> 01:53:29.000

Alright. I'm here. I'm speaking away and I've got my actual mic on mute as opposed to the zoom.

01:53:29.000 --> 01:53:30.000

Right.

01:53:30.000 --> 01:53:35.000

Sorry about that. I apologize in advance if I missed part of this. So maybe you covered it.

01:53:35.000 --> 01:53:53.000

But to what extent, legally speaking, do these regulations apply to anonymization done for the purpose of taking something, a data set, outside of the scope of the act versus anonymization done

01:53:53.000 --> 01:54:01.000

as an alternative to destruction, following the purposes for use of the personal information being fulfilled.

01:54:01.000 --> 01:54:10.000

Cause as I read it, section 23 is very much founded on when you get to the end of the lifecycle for data,

01:54:10.000 --> 01:54:30.000

this is the procedure, and these are the regulations. So, if you do it for some other reason, there's nothing that says you can't anonymize and create an anonymized data set during the currency of the information. But I'm wondering if legally speaking we think these regs would apply.

01:54:30.000 --> 01:54:42.000

David, you just reiterated comments from several of the panelists about the scope and the necessity to look at these provisions.

01:54:42.000 --> 01:55:04.000

Can you go to the statutory provisions right at the top? You're highlighting one of the things that has come up several times, which is these anonymization provisions are set out not generally. They're set out under the destruction provision - when you're finished, end of life, as was articulated by a couple of the panelists.

01:55:04.000 --> 01:55:13.000

So, you're just reiterating a view that we've received, and we discussed earlier, but also outside the context of this discussion today.

01:55:13.000 --> 01:55:20.000

A lot of people are expressing it as well. It's a scope consideration. So, point very well taken.

01:55:20.000 --> 01:55:25.000

Alright.

01:55:25.000 --> 01:55:27.000

Sorry for raising it again. Sorry. Good for emphasis. Yeah.

01:55:27.000 --> 01:55:35.000

No, it's excellent. This is a critical point

01:55:35.000 --> 01:55:42.000

that I think has been raised by a number of stakeholders across different sectors. So, thank you for raising it again.

01:55:42.000 --> 01:55:47.000

It's helpful to reemphasize.

01:55:47.000 --> 01:55:50.000

There was someone else who had put up their hand.

01:55:50.000 --> 01:56:05.000

Yes, Surtinder, I'll take you off mute now if you'd like to provide your comments.

01:56:05.000 --> 01:56:06.000

Yeah.

01:56:06.000 --> 01:56:26.000

Hello, thank you. Good afternoon. I just want to go back to section 9. So, the reason we anonymize data in the first place is there has to be a serious and legitimate reason for doing so, otherwise we should be destroying it. Now section 9, I believe, is asking what are you anonymizing and why are you anonymizing it and ensuring that you're using the right best practices for anonymizing it.

01:56:26.000 --> 01:56:30.000

So, I don't have an issue with section 9, so I don't see why the panel has such a concern with it.

01:56:30.000 --> 01:56:39.000

I think it's a fair question when you're coming to audit and assess how well a company is meeting that part of the law.

01:56:39.000 --> 01:57:29.000

So, first of all, thank you for that comment. I guess the question for you, Keren Groll had suggested an approach that, for the purposes of demonstrable accountability, which is a new theme in multiple different statutory frameworks, necessary for folks to have evidence - organizations to have evidence of compliance. So, I think there's common ground there. Assuming that an organization has engaged in the assessment that's expressly contemplated in above sections, number one, and otherwise it is just a core feature of

01:57:29.000 --> 01:57:30.000

Okay.

01:57:30.000 --> 01:57:49.000

best practices which have to be followed. That's the statutory requirement. If you had no regs, you have to follow statutory best practices - that's basically in there – and that undergoing the relevant applicable and appropriately rigorous process of de-identification or anonymization, you would have a documentation of that. So, we're aligned on that.

01:57:49.000 --> 01:57:55.000

Okay.

01:57:55.000 --> 01:57:56.000

Yeah.

01:57:56.000 --> 01:58:02.000

If you have that documentation, do you still feel that a separate requirement, in section 9, is still required?

01:58:02.000 --> 01:58:08.000

Yes, for accountability to the Act. And if you're not accountable, there are significant fines.

01:58:08.000 --> 01:58:09.000

Right.

01:58:09.000 --> 01:58:13.000

So, you could have best practices, but they're outside of the act.

01:58:13.000 --> 01:58:18.000

And I think this forces companies to comply with the act.

01:58:18.000 --> 01:58:32.000

Right, so I just want to make sure, cause I want to make sure I'm understanding. So, there's common ground and you have on the panel folks that have spent like an immeasurable amount of time with their accountability frameworks,

01:58:32.000 --> 01:58:43.000

no one will doubt or shed any type of issue with your point that accountability is critical – it is a fundamental feature of the statutory regime.

01:58:43.000 --> 01:58:44.000

Okay.

01:58:44.000 --> 01:59:03.000

Assuming that it's an obligation, let's say there was an investigation, and an organization had the documentation - just forget about section 9 for now - had the relevant requisite documentation to show that they've complied

01:59:03.000 --> 01:59:06.000

Okay.

01:59:06.000 --> 01:59:15.000

with the section 23 requirement and even complied with the regs above, the provisions above, that relate to the assessment,

01:59:15.000 --> 01:59:19.000

so we're agreeing with everything aspect,

01:59:19.000 --> 01:59:31.000

they have that documentation for accountability - demonstrable accountability. What is the value then of an additional requirement for a register?

01:59:31.000 --> 01:59:40.000

So, I think this comes back to specifically the case with anonymization, serious and legitimate. I also agree, you're not going to reinvent the wheel, something you already do.

01:59:40.000 --> 01:59:46.000

So, if you have a PIA which meets these requirements in section 9, you're good to go.

01:59:46.000 --> 01:59:55.000

You're ready. But those who don't need to comply with this, they need to have these features in their data practices.

01:59:55.000 --> 02:00:01.000

Right, I see. So, in other words, you're saying at least elements of section 9, cause there's a second level to this.

02:00:01.000 --> 02:00:16.000

You're saying as long as folks have that for accountability, you would satisfy or otherwise, I mean, I think the comments we're getting is 2 aspects.

02:00:16.000 --> 02:00:23.000

One, you're already satisfying when you conduct the assessment, because that would be the case.

02:00:23.000 --> 02:00:53.000

You would be documenting that. You're saying clarify that. That's number one. And the second point, which I think is a point that certainly as I've mentioned a couple of times, we've received from a number of clients and you've got this on the call from the panelists as well, there's aspects of section 9 that are prescriptive beyond what is, perhaps, even practical or even feasible and perhaps even unnecessary for the purposes of what you're referring to.

02:00:53.000 --> 02:00:54.000

Per second.

02:00:54.000 --> 02:00:55.000

I.

02:00:55.000 --> 02:00:57.000

02:00:57.000 --> 02:01:04.000

Oh, I agree, and I did have some conversation with Pam on this. I think it's also up to interpretation.

02:01:04.000 --> 02:01:07.000

So, Pam's interpretation of section 9 was different to mine. So, Pam said, well, this was also for grouping of data, etc.

02:01:07.000 --> 02:01:19.000

My interpretation of this is for an instance of a specific individual's data that has been anonymized.

02:01:19.000 --> 02:01:29.000

So, Adam, your data has been anonymized. But once you group data from several individuals into another setting, then is that really at a PI level?

02:01:29.000 --> 02:01:35.000

So, I think, and I think someone else put a comment that this would be something that would be taken to the courts.

02:01:35.000 --> 02:01:41.000

But, just the section 9, I know there's talk about going back and saying, get this removed.

02:01:41.000 --> 02:01:56.000

I would not be comfortable getting this removed because for those people don't have mature PIA practices, this is something that would need to be following or implemented.

02:01:56.000 --> 02:02:07.000

Got it. Well, like again, it's helpful to have these discussions and comments. And again this session just for clarity is being recorded and the entire session is being put forward.

02:02:07.000 --> 02:02:24.000

The recording of it's being put forth to the Quebec government. So, your comments will be received by the government officials who are responsible for the draft reg.

02:02:24.000 --> 02:02:29.000

Okay, thank you. Thank you for allowing me the time to speak.

02:02:29.000 --> 02:02:34.000

Thank you for the comment and Katelyn just in the interest of time, we have time for one more comment.

02:02:34.000 --> 02:02:39.000

Yeah, there's a really great one here. Bear with me. It is a bit lengthy, but it's worthwhile, I promise.

02:02:39.000 --> 02:03:31.000

And this is related to section 8. If we take a step back and look at what appears to be an underlying concern that in X years there would be a new technological advance that would permit someone a higher probability of being able to link between data sets to re-identify someone, would that mean that the data sets that have been anonymized in the past may no longer meet the very low risk threshold and therefore would be reconsidered as personal information. Or if the circumstances change, the information that had a very low risk of reidentification when kept internally with safeguards would now

be made public where there are fewer safeguards. In those cases, wouldn't it make more sense to monitor the environment and the circumstances for material changes to reidentification risk instead of requiring organizations to regularly reassess the information itself.

02:03:31.000 --> 02:03:44.000

Great comment. Khaled, interested in your comments on this because we've had a lot of conversations about this, interested in your comment on that thoughtful comment we just heard.

02:03:44.000 --> 02:03:55.000

So, by analogy and in the security world, we deal with risks in a similar way in the sense that in the context of encryption

02:03:55.000 --> 02:04:09.000

we know when certain key lengths are no longer going to be acceptable. Actually, NIST publishes a schedule that says in X number of years, key lengths have to be increased from X to Y.

02:04:09.000 --> 02:04:16.000

And at that point in time, you have to use stronger, essentially stronger encryption.

02:04:16.000 --> 02:04:17.000

And we have a schedule for that. I mean, it's an approximation, but it's a schedule.

02:04:17.000 --> 02:04:53.000

But it doesn't mean we don't encrypt today because we know in 5 years that the standard will no longer be acceptable or will no longer be strong enough. We still have to use the best methods and the best technologies available today to protect information knowing that in X number of years that that risk will go up. So, we already operate in that environment where we know technology will move forward

02:04:53.000 --> 02:05:01.000

and we even have a schedule to tell us when. It's not as uncertain as you know we're talking about now with anonymization.

02:05:01.000 --> 02:05:28.000

With respect to what you should do, that's an interesting question. I mean, if you know that the environment has changed, I think that the recommended practice would be to recall the dataset, if it's possible, because sometimes it's not possible to do that. But if you're sharing data or making that available to a partner, you'd have a provision in your contract saying that if the risk ever changes, we may have to recall the data set and replace it.

02:05:28.000 --> 02:05:39.000

And you'd have that provision, and you'd recall the data set or replace it so that you're still sharing data that's deemed to have a very low risk.

02:05:39.000 --> 02:05:46.000

If it's a public release, there's nothing you can do about it. That is always going to be the risk with public releases.

02:05:46.000 --> 02:06:00.000

And you know, the first case, what does a recall mean? That's a process issue that has to be kind of determined on a case by case basis, I think.

02:06:00.000 --> 02:06:08.000

Well, on that note, we're just about at time now and we're going to end the session.

02:06:08.000 --> 02:06:49.000

First of all, I want to thank you Khaled, Keren, Pam and Suzanne for extremely thoughtful comments and the time that each of you put in for the preparation of this and thank you to Katelyn and Catherine, on our Osler team for helping to prepare for the session and moderate it today. And most importantly thank you very much to everyone who attended, really appreciate the attendance and a lot of thoughtful comments. Again, this recording is going to be submitted with your thoughtful comments.

02:06:49.000 --> 02:07:11.000

We're looking to process it and then we're going to send it in, on or before February 3rd, and we'll make sure that all attendees or registrants - as I mentioned, there were over 700 registrants for this - all registrants will receive a copy of the recording for your future reference and consideration. So, thank you very much.

02:07:11.000 --> 02:07:26.000

Thanks, and we'll hope to see everyone soon. Bye.