Barclay Damon Live Presents: The Cyber Sip Podcast™
Episode 23: "Oh Canada? How to Comply With Canadian Law as a US Business," With Ruth Promislow"

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Ruth Promislow**, Bennett Jones LLP

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: She is a partner in the Toronto office of Bennett Jones, and Chambers-ranked in privacy and data—Ruth Promislow has been 20 years a commercial litigator, extensive experience in the data protection, privacy, and security space, and she is a thought leader in all of these critical areas. Ruth, thank you so much for joining us today.

[Ruth]: Thank you for having me.

[Kevin]: So I thought we'd start with a little reflection that leads into what I think is an important topic: US businesses doing business in Canada. So I don't know about you, but I grew up 15 minutes from the Canadian border, so we were in Canada all the time. And I remember hearing that it was a thing to visit Niagara Falls, like a bucket list thing.

[Ruth]: We have the better side of the falls, as you know.

[Kevin]: Right? Right. And it was incredible to me because we were Niagara Falls 10 times a year. So there was this seamlessness to traveling between US and Canada. But that, of course, masks very different legislative and legal structures. So if I'm a US business and I have either operations or customers or employees in Canada, what do I need to do to figure out how to comply with Canadian law?

[Ruth]: It is a very different structure, as you've noted. So there's several, but I'll just sort of focus on high level. You know, first we have sort of a unique structure in that we have federal and provincial legislation in certain provinces, both of which could apply in certain circumstances. Or it could be the case that only one of the federal provincial legislation applies. Thankfully, on a principle basis, they're pretty much aligned. But in terms of US organizations doing business in Canada, a key difference between the US and Canada is that we don't have this concept of PII. We have the concept of personal information, which is any information about an identifiable individual. So when we look at obligation under privacy legislation and we think about the obligation to safeguard and to develop policies and practices and to report breaches, that's all sort of a contextual analysis that includes a risk of harm assessment.

[Kevin]: So when you say there's no PII, it's just the concept is "personal information." Does that mean any identifier—is a name or an email address sufficient to trigger the law?

[Ruth]: Well, it could. So, for example, a list of customer names associated with a convenience store or, you know, or BestBuy may not be particularly sensitive, but a list of customer names with an organization like an addiction organization could be quite sensitive in that it's disclosing some personal information

about the individuals that could give rise to some level of harm. And our definition of harm is quite broad that it would include embarrassment, emotional distress, and things of that nature. So it really does require a contextual analysis where you look at, well, what is the harm that could come from the compromise of this list of names? And you can see how in one scenario, there would be no obvious harm, like the Best Buy, and in the other, there could be. And so when we talk about safeguarding and reporting breaches, you do have to be mindful of the context and that assessment has to be undertaken. So we certainly do have a concept of more highly sensitive information in that, yes, what we call social insurance number, your Social Security number and income tax returns and driver's licenses and things like that will be deemed and considered in almost all circumstances to be highly sensitive. But our concept of information to be protected is just any information about an identifiable individual.

[Kevin]: Right. That is definitely more strict than in the States. So what is it that triggers the application of Canadian law? Is it...you have to be doing business in Canada or is it enough, for example, to have one or a few employees that live in Canada, even if they travel to the US to do their work?

[Ruth]: So I'll answer the employee question first, because the federal legislation only covers employee information for those undertakings that are within the federal jurisdiction and...such as oversight, such as banks and airlines and things of that nature. So at a high level, that's generally speaking, employee data isn't covered by the federal legislation. But for the provinces, certain provinces, that have privacy legislation that has been deemed substantially similar to the federal legislation, which just in short terms, it means it applies. We have three provinces where that's the case, and that legislation does cover employee information. And there's no...this is another distinction between, I think, certain states and Canada. There's no special number, right? So if you have an employee who resides in the province of Alberta, then quite arguably you have obligations under the Alberta privacy legislation to safeguard...to afford the same level of transparency that you are required to do so and to notify of any breach involving their information that meets the threshold of notification. In the same...so then turning to sort of customers which would be covered under the federal legislation, if you're a US based organization, you have customers in Canada. I quite arguably...that would be considered doing business in Canada. I think it would be a hard argument to say you're not doing business in Canada if you make your products or services available to people residing in Canada and you know that they're ordering those products and services and you deliver it to them, I think that would be it would be a fair argument that that is doing business in Canada. So to the extent that is that organization that's US–based does have customers or employees in Canada, that it does have to look at what regulatory obligations it may have. Because they are they're quite different and they're changing. But we'll come to that. That's the big news from Canada.

[Kevin]: Right. So it just strikes me that if you are a US business in that situation, you want to make sure that you go to your US lawyer and that your US lawyer hooks you up with an experienced Canadian practitioner like Ruth, like Bennett Jones, so that you get advice on how to follow Canadian law because Canadian law is a different animal, right, Ruth? I don't practice Canadian law. Do you practice US law?

[Ruth]: No.

[Kevin]: Right. So it's ... you're really getting two important but very different sides of the same coin. You want to talk to your US lawyers about data protection and privacy stateside, and your Canadian lawyers about those critical topics north of the border.

[Ruth]: Yeah.

[Kevin]: Okay. So you mentioned some statutes, and I know I wanted to talk to you about some hot topics in

Canadian privacy law. And I have a couple of places I want to go, but I want you to take us wherever you want to go. What are the hot topics? What's happening up there? I know that both here in the States and in Canada, the legislatures are working to try to enact new laws with varying degrees of success. What are the hot topics and trends out there now?

[Ruth]: So we are set to get new privacy legislation at the federal level. It's a complete overhaul of the existing regime. So our current structure is, you know, I'd say, the legislation in place at present is sort of a set of "motherhood statements" with...not...it's not very prescriptive in terms of where...

[Kevin]: Can I stop you there? When you say "motherhood," I think it sounds like what you mean is these are sort of broad, laudable principles with not a lot of meat on the bones.

[Ruth]: Reasonable steps to protect information, sort of that, sort of rights like, you know, things that you should do. The real...the precision about what the expectations are have come in the form of non-legally-binding guidance documents and in the course of investigation decisions from the privacy commissioner. So, if you ask me what does the privacy commissioner think of this particular issue, we can answer that. And that would be based on their guidance documents and their decisions, various investigations. So we do have insight into that. And the guidance we give clients is based on that, not simply on the plain wording of the legislation, but in terms of the changes coming. We are set to move toward a structure that's much more closely aligned with GDPR. It's still in draft form, but we have every expectation that the legislation...or that this bill will in, in a very similar form or precise form, become legislation particularly because Canada stands to lose its "adequacy decision"...and under EU law, if we don't reform our privacy legislation, our adequacy decision, which we have, is based on our existing legislation which is considered to be fairly outdated. So the new regime...No, go ahead...

[Kevin]: No, no. I was just going to say you mentioned GDPR. Tell us what that is and tell us why Canada was set to lose its adequacy designation. I'm gathering that's because in the opinions of those across the Atlantic, Canadian law was no longer adequate to protect the privacy of citizens and those whose data those citizens were collecting.

[Ruth]: Yeah. So the... well we do have inadequacy decision which says that the legislation is adequate and sufficient to protect data of EU residents, meaning so data of EU residents can be processed or stored in Canada currently. There is genuine fear that we will lose that with an impact on our economy.

[Kevin]: Ah I see.

[Ruth]: And so you can see that's a driver for the new federal regime. Another driver is there's a recognition that as we transition increasingly to the digital... in the digital economy, the privacy and information issues have increased significantly and there are opportunities are there as well, which we don't want to lose out on. So all to say that we expect this federal legislation...or this draft to become law soon. We don't we don't have insights only gone through the first reading, we don't have insight into precisely when. But the big changes are: we currently have essentially no penalties. We'll have a full penalty structure that involves 3% of gross global revenue or $10 million for administrative fines and up to 5% ($25 million) for intentional violations. So that's huge. There's also going to be a complete overhaul of the obligations in that currently, while there's an expectation that you develop a comprehensive information management program with all your policies and your protocols, there's no specific requirement that you do so in the legislation. The draft includes a very detailed requirement of what is expected or required, rather, of the set of policies and protocols that outline how you comply and that can be requested by the privacy commissioner without any basis to do so. And if the privacy commissioner doesn't like what he (it's currently a he) so what he sees, he can make specific recommendations for corrective measures. And if you under the current draft, if you do not follow those corrective measures, there's a risk the commissioner can then just start off an

audit or investigation. So there could be big repercussions if you don't have this whole documented management program in place, big changes as well to the whole consent structure in terms of express consent being the default in most situations other than there's sort of a carve-out for what we call business activity exception, you know, I order a book from you and you use my name and address to deliver the book. That's going to be covered by the exception. We don't need sort of the express consent. But if you want to keep a record of what books I like to order so that you can make some predictive analysis about what I like and what you may recommend, that's going to be a different ballgame. And you would need the express consent from me. You need to show that I understood it before you started the collection, and then it's all sort of documented in a compliant way.

[Kevin]: We're talking about some emerging legislation. And I was just thinking about—because you and I were talking offline about Bill C 26, which is more of a security for critical infrastructure-based law than the privacy law you're talking about now. And I know C 26 is meant to apply to certain industries. It's broad, but it's not all-inclusive. Is the privacy legislation that you're talking about now; changes that you're discussing is...does that apply across the board to all businesses.

[Ruth]: Any organization that collects personal information in the course of a commercial activity?

[Kevin]: Yeah.

[Ruth]: So that's basically across the board and even nonprofit organizations can fall under that to the extent that they're fundraising to that collection of your fundraising list would be subject to that. So that is across the board. And you're right. C 26 it had...the scope of it hasn't been clearly defined because there's just been the first draft that was tabled in the spring in what organizations will be defined to come under the umbrella of critical infrastructure remains. But you know the obvious ones and then are even identified in some of the wording like financial institutions, critical infrastructure will be sort of...telecom, airlines, you know, they're sort of the obvious ones that will be subject to those requirements. You'll financial institutions already have sort of a separate set of obligations that are detailed by our Office of the Superintendent of financial institutions. They're already subject to certain requirements when it comes to security, not just privacy.

[Kevin]: Right. So we talked about privacy earlier and now we're talking about Bill C 26, which has not been adopted. But I wanted to ask you a question about it. This is the...an act respecting cybersecurity or ARCs, and this is an act designed to require federally regulated, organized nations to take steps to protect their cyber infrastructure. And if something in the draft dovetails with something you said earlier, and I wanted to read it to you and ask about it. So one of the things that part two of ARCs would require is the "protection"...an organization has to protect "critical cyber systems from being compromised." So that when I read that, I thought about something you said earlier, that sounds more like a motherhood-type requirement, and you referred to these broad requirements and then guidance when you were talking earlier about the proposed legislation. So where is it? I take it it's not in the act, or maybe it is. How does an organization subject to Canadian law know what steps it needs to take to protect its critical systems from compromise? Can they find that anywhere in regulation or regulatory guidance?

[Ruth]: Not yet. And I'd expect that with this legislation, there will be some regulations issued under it that would give a little bit more precision. I mean, as you know, it's hard to be too prescriptive when it comes to security because it's a moving target.

[Kevin]: And it really is.

[Ruth]: And I, I would think it's fair, you know, in the absence of any particulars about what's expected, we would typically look to well-regarded frameworks like NIST or things like that for an approach

to security. A lot of the industries that will be covered by this legislation are probably the more sophisticated level of security, but certainly not all. And that, of course, is the concern for Canada, is that it's one weak link in our security, in our economy, and that could pose problems for many. So I do think there'll be guidance documents. That would be the expectation. I would expect there'll be some more particulars in regulation. And in the absence of anything, the experts will turn to what is industry standard and what are well-regarded frameworks for approaching security risk.

[Kevin]: It's interesting you mentioned if it is a highly regulated industry like banks or financial institutions, those organizations have well-tested cyber protocols, privacy policies—small businesses, manufacturing, and others doing business cross-border may not have those things in place. I know we have one more topic, but I wonder, do you have a horror story, if you will, you could share with us about something from your experience of a US business finding out too late that it was not in compliance with Canadian privacy or data security law. I know it happens, but can you to talk to us about one of your experiences?

[Ruth]: I don't have any sort of one horror story, but what I will say is this: that it's quite frequent, that there's an assumption that the regime north of the border is the same as in the US. And when it comes...the matter may come to us one way or the other through a breach or in the course of some questions that arise, but, you know, it's evident that there hasn't been an accounting for the types of regulatory issues that you have in Canada. So, for example, just a data mapping, you know, that would be...it's not currently prescribed in our privacy legislation, but that would be, in my assessment, first critical step in both privacy and security. How do you protect what you...if you don't know what you have, how are you protecting it? So very rarely do we see that proper kind of data mapping. And I think that is sometimes comes from the US approach of, well, we don't have any driver's licenses, we don't have any Social Security numbers, so we're okay. But you do have a lot more than that, that together can be quite sensitive. And so generally I think in terms of compliance, you know, it's so much easier to build from the ground up. It's very hard to sort of plop compliance from top of existing operations and policies and protocols. And when it's an afterthought, then it becomes much more expensive to deal with.

[Kevin]: Right. But we'll come we'll come back to this at the end. I just think the takeaway here is if you're a US business working in any form or fashion north of the border, you've really got to get on top of this early and often through US counsel coordinating with Canadian counsel and I guess, Ruth, that leads me to one last topic I wanted to ask you about. If there were two or three things that you had to tell every US business with operations in Canada, they need to be mindful of what would those things be?

[Ruth]: You know, in large part, we've covered them, because it's in terms of the new legislation which we expect, it's such a drastic change from our existing structure that it will take a very significant amount of time to build a proper compliance program. And, you know, we saw in the EU how long it took for organizations to do that. They had the grace period and they were still struggling to do it properly. So I would say, given that we know that change is coming, organizations would be wise to start that process now of asking those questions internally, to start pulling together the information they will definitely need under the new legislation. And quite arguably, according to certain privacy commissioner positions that you do need right now, that's number one. Number two, a point that I didn't highlight and I'll highlight now in the draft legislation is "service provider exposure." So under the draft, service providers to organizations that collect or direct the collection of personal information will have direct obligations under that legislation to safeguard and to report breaches to the organization, not directly to the individuals or the commissioner. But there's also...

[Kevin]: Can I jump in and just ask you to define for us when we're talking about service providers, some of us may know, others may not. These are vendors of what different types, Ruth? Lawyers?

[Ruth]: Well, any organizations. Well that's an interesting...it hasn't been defined or I don't...in the definition I don't know that that has been that issues been thought through. But any organization that would offer or deliver services to process or store information. So I don't know that lawyers would be captured because we're not offering that service. It's not it's not part of what we do. We may come into custody of information through the course of delivering our legal services. But to the extent you're an organization that just stores information or it goes over to the US, to an affiliate organization or a stranger organization to process for the purposes of marketing information, those entities will have direct obligations and direct exposure to those penalties I spoke of, and that is a huge difference. So currently service providers would only have contractual obligations to the extent they were subject to any and maybe some common law obligations to protect the information. So that will be something new for US-based organizations to consider because they may be thinking, well, I'm not even captured under this because I'm not...I don't collect information directly from customers. So not my issue, but it could very well be my data. Yeah.

[Kevin]: It's not my data...Ruth, when are these changes, if it's known, when are these changes likely to take effect? And will there be a period of time after they become effective for organizations to come into compliance?

[Ruth]: So there's sort of a very odd background. Not very odd, but there's a bit of a background to this bill in that it was initially introduced by the federal government in 2020, our prime minister called an election. By doing so the bill died on the order paper and then following his reelection they then reintroduced it. So had already gone through committee readings. There's already been a lot of input, even though technically speaking, C 27 has only gone through one reading. That's sort of a long way of saying, I think it's going to be passed this fall and I expect there'll be a grace period. There's no way they would just...you can't implement legislation refined of that nature without a grace period. I would guess there could be a year to 18 months and maybe they'll do a phased approach, which just as a side note, it's a whole different podcast discussion. The Quebec legislation that was that...part of which comes into effect September 22 of this year, the other part of which comes into effect in 2023, is quite significant in that it takes Quebec much closer to a GDPR-type structure, quite prescriptive, with significant penalties. So we're already looking at that. And I just heard from somebody in the Alberta Privacy Commissioner office that they're also undertaking a review. Their legislation expectation is they're going to try and sort of move it toward that model, more prescription and penalties built in. And I wouldn't be surprised to see other provinces follow suit.

[Kevin]: So to sort of sum up here, Ruth, what I'm hearing is that sometime in the next few months, there are going to be some dramatic changes in Canadian privacy law. There could well be an explosion or great expansion of liability on the part of service providers. And the long-term trend is for Canada to come more in line with Europe and the general data privacy regulation than perhaps the United States, which has 50 different sovereigns, each of which imposes its own law.

[Ruth]: Yes, although with the qualifier that we do have, that provincial/federal structure. So as these things move, there could be some inconsistencies as between the provincial and federal regimes and at the same time you could be subject to both. I don't expect any significant inconsistencies. But it's just that it's this odd scenario. There are certain scenarios where there can be concurrent jurisdiction at both levels.

[Kevin]: It sounds like that's all the more reason for an organization to start today thinking about what steps it needs to take to bring itself into compliance with Canadian privacy law. Be mindful of the changes and be prepared to upgrade in order to meet the new legislation.

[Ruth]: Yeah, think that's fair.

[Kevin]: All right. Well, Ruth Promislow, thank you so much for joining us. It's been great talking to you. And as you said, we'll have to come back and do another episode on some of those ideas that we didn't have time to address today.

[Ruth]: That's great. Thank you.

[Kevin]: Thanks again to you, Ruth, and thanks to all of you. We're back soon with another episode.

[Kevin]: The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.