


Cutting Through the Noise and Clutter

Getting ahead of Canadian legislative and regulatory rule changes by shifting focus and using the right technologies



Security has changed enormously since the days when a lock on your company's front door was sufficient. Things are now far more complicated. It's not enough anymore to just *protect* our data – we now must also look at how we gather and use it, and what we do with it when we suspect it has been accessed

It's complicated enough that all this is covered by a jumble of legislative rules in our provinces, from Ottawa, and even on an international level. Unfortunately, this legislation and regulation is about to get even more complicated as Canada works to play catch-up with the rest of the world.

ITWC CIO **Jim Love** had a conversation with **Sean Lynch**, Director, Client Strategy - Legal Services, Ricoh, and **Imran Ahmad**, Partner and Head of Technology, Co-Chair Data Protection, Privacy and Cybersecurity, Norton Rose Fulbright. The discussion opened on the question of why legislation and regulation is *everyone's* concern.

Everyone's Concern

Lynch said the reputational and financial risk that comes out of data breaches affects entire organizations.

"There is tremendous ... risk associated with poorly managing your data, and ... data management, information governance, and compliance with legislation span the entirety of the business and legal environment. It's important for *all members* of an organization to be mindful of how they're managing, storing, and collecting their data as it has a direct impact on the financial and reputational risk for the entire corporation."

Every organization is now a data company, said Ahmad.

“Data is the oil that keeps things going. Even auto parts manufacturers and law firms are collecting data. The big challenge I’m seeing amongst clients is this realization that they have a lot of data. [They want to know] how to sort that data ... and what their responsibilities are versus those that belong to their clients.”

Indeed, the complexity around data brings complexity to partnerships.

“We see a lot more contracting between law firms and their clients where the clients are saying, ‘I’m going to give you this information, but I want to make sure you’re securing it right, that you have the most cutting-edge information and security in place.’”

Changes Afoot

When it comes to security and privacy, things are complex enough as it is. Unfortunately for fans of the status quo, Canada’s legislative framework is set to change dramatically – something Ahmad traces back to the EU’s adoption of [GDPR](#) in 2016, and then “what the Americans did with [each of their] 50 states having data breach legislation.”

“Canada found itself ... behind the curve,” said Ahmad, who described the country’s legal and regulatory landscape, featuring 24 different privacy data protection laws, as a “patchwork” of laws.

Canada, he explained, was built on an ombudsman model, which flowed from the 1990s, when ecommerce businesses popping up for the first time were being asked as consumers to provide credit card information.

“So [government] adopted a code of conduct ... which became our federal legislation. When the Personal Information Protection and Electronic Documents Act ([PIPEDA](#)) came in, the model was not one of harsh enforcement [but] of an ombudsman one.”

But that is changing, said Ahmad.

“Quebec adopted Bill 64, which is now known as Law 25, which for the first time imposes very significant fines – a percentage of global turnover – if you get it wrong, if you are offsite.” There is a similar shift toward enforcement in other parts of Canada, particularly in Alberta and British Columbia.

“ Prior to the Quebec bill being tabled, Canadian legislation lacked teeth.

IMRAN AHMAD, Partner and Head of Technology, Co-Chair Data Protection, Privacy and Cybersecurity, Norton Rose Fulbright

While Imran didn't champion the idea of harsher rules, he allowed that *something* had to be done. “Prior to the Quebec bill being tabled, Canadian legislation lacked teeth.”

The change brings cold realities: “A percentage [penalty], even if it's as high as five per cent of your global turnover, is for many organizations going to be significant. It moves things from being a nice-to-have best practice to a pure compliance requirement.”

Balancing Act

However, Ahmad said change cannot come full-bore, as some carbon copy of the EU model.

“The European legislation is much more restrictive – the [regulatory] gold standard globally. Canada, being a G7 country and a net recipient of foreign direct investment, cannot be too strict or too conservative in its interpretation of privacy legislation. [It must] strike a balance between what Europe is doing and what would fly in the Canadian marketplace without [there being any loss of] Canadian distinctiveness.”

Consistent Message

Ahmad offered sage advice to anyone in Canada confused as to what legislation, foreign or Canadian, applies to them.

“You have to have a link to the jurisdiction. Typically,” he said, “it’s not [about] citizenship or residency but where you are domiciled. So if ... you are based in Europe for whatever period of time, and you go to a hotel and give your information, including your passport ... and then, after moving back to Canada that hotel chain has a breach, you would be entitled, under European law, to say ‘You should have notified me.’”

While Lynch knows the regulatory sands are shifting beneath Canadians’ feet, and potential complications abound, he said he doesn’t think his approach, or the advice he gives clients, has changed.

“It’s not [about] citizenship or residency but where you are domiciled.

SEAN LYNCH, Director, Client Strategy - Legal Services, Ricoh

“[The advice we give] has evolved ... as the consequences [of noncompliance] have grown. The advisory services we provide around information governance, data management, and data analysis have risen to the challenge of the pressure organizations are under. But broadly speaking our position

[is still] that you need to know what data you have and where it resides, and how it is accessed, and [by whom].”

Lynch repeatedly stressed the importance of the point that organizations must know what data they have and where it is.

“Let’s say your information goes to Germany, where they [might not] have the same concept of [legal] privilege protections. At this point it becomes very complex for clients and organizations involved in international legal disputes. It becomes complicated when you’re an international law firm that might be exchanging information to support litigation in multiple jurisdictions. [It is very important now to] have a handle on where your data is ... domiciled ... and who has access to it from which jurisdiction.”

Contract Caution

With all the buzz around legislative changes and privacy laws, and whatever changes are to come, contractual complexities are often overlooked. As Ahmad explained it:

“Contracts stipulate unique provisions. You may be a law firm advising a company doing business with a government [organization]. A department or Crown Corporation might say ‘You cannot take [the data from the transactions between us] outside of the country. Not only that – you also cannot take the metadata out of the country.’ [According to contract terms], in the case of a breach and resulting doc review, it may be that servers must be located in Canada, and in some cases the reviewers also based in Canada.”

Ahmad reiterated that while people should be ever mindful of legislation, the piece that gives the most headaches in breach situations is actually contracts.

Lynch confirmed that contracts can be a major sticking point.

“Certainly when it comes to Ricoh addressing contractual issues with our clients, this comes up on a regular basis. If you’re contracting, where are your contractors going to be based? Where are your servers based? Can non-Canadians access data that is physically resident in Canada? There’s [even] the question of whether viewing a document constitutes the document and the information leaving [its home] jurisdiction.”

“Same thing when it comes to security. What security provisions are in place? What security are you utilizing to ensure data is not going to get breached? This level of complexity has not really been appreciated yet by organizations around the world, [with the exception of certain] European corporations who have been steeped in GDPR.”

“ We have artificial intelligence and machine learning tools that make the process [of managing data] significantly easier than ever before.

SEAN LYNCH, Director, Client Strategy - Legal Services, Ricoh

Organizations, said Lynch, are going to be “in for a surprise, a shock perhaps, when they really start getting confronted with the challenges of this legislation. The ease of access through a tribunal rather than needing to go through a court means companies are going to be faced with challenges on a regular basis, much more so than they are now. And I think that’s really going to affect the way they structure their data, the types of data they’re willing to collect, and how frequently they delete their data.”


Tech Solution

Despite all the issues and complexities in a country (Canada) in which huge legal and regulatory changes are afoot, Lynch holds an optimistic viewpoint. He said he sees technology as a solution and way forward.

“We have artificial intelligence and machine learning tools that make the process [of managing data] significantly easier than ever before. What we really want to know is: what data is held and who has access to it. Data analysis can give you that information. Where is the data held? Is it on a server? In the cloud? *What* is that data? Is it personal information? Is it someone’s passport? Credit card information? Cancelled checks?”

Technology, said Lynch, is now able to do all that – to untangle the spaghetti mess.

“We can use technology that crawls over entire networks, identifying the type of information that’s there, and when it was last accessed. What we’re really looking for when we run these types of data analysis projects is ROT, which stands for ‘Redundant, Obsolete, Trivial’ data.”



There are tools available right now, said Lynch, that can suss data as it comes in and determine whether or not it's information that should be retained or deleted. Getting sharp on this aspect has implications even beyond legal and regulatory compliance.

"No one really likes [deleting data], but it must be done. We've come across this in organizations going through a lift-and-shift process. These businesses want to move to the cloud because it's less expensive, more robust, and security is better. [However,] they [generally] don't want to lift and shift everything to the cloud."

The "Let's keep everything we possibly can because we might need it down the road" mindset needs to be broken, said Lynch. "All that it's doing is creating a risk for you and your organization if you're holding onto data you don't [and likely *won't* ever] need."

First Steps

Lynch said Canadian companies have a long road to travel, but offered solid advice as to first steps in a new direction.

"The first step is to find out what you have and where it is," he said. "Once you have an understanding of what you need to [retain], you can build an information governance policy. From there, you can build a breach response strategy. And then, once you have a breach response plan in place, [you can] better deal with the regulatory framework."

Ricoh Canada

At Ricoh, we're empowering our customers to respond to our changing world with actionable insights. We believe having access to the right information translates to better business agility, more human experiences, and the ability to thrive in today's age of hybrid and borderless work. Through our people, experience, and solutions, we create competitive advantage every day for over 1.4 million businesses around the globe. To us, there's no such thing as too much information.

www.ricoh.ca

About ITWC

ITWC is the Canadian AI-enabled digital media and marketing platform reaching Canada's most influential, engaged and targeted technology decision-makers. Using first-party data, the science of demand generation and industry knowledge, we create value for both our community of participants of over 280,000 CASL-compliant subscribers and our leading vendor customers.

www.itwc.ca