As cloud computing comes of age, a confluence of events has placed real enterprise concerns around data security, data privacy and how organizations can ensure that sensitive information is protected at all times.

How Private Is Your Data? A North American Perspective

As cloud computing comes of age, a confluence of events has placed real enterprise concerns around data security, data privacy and how organizations can ensure that sensitive information is protected at all times.
Jim Love, CIO, ITWC and his special guests Ben Young, Vice President, General Counsel, Cogeco Peer 1 and Sheila FitzPatrick, World Wide Data Governance and Privacy Counsel/Chief Privacy Officer, NetApp, discuss managed services and data sovereignty. With the release of the Panama papers and the FBI - Apple wrangling over iPhone security as a backdrop, the panel explores the differences between privacy and security, the often-confusing layers of international warrants and surveillance policies, and the discussions customers should be having with their cloud providers.

**Setting the scene**

The ground around data privacy and data sovereignty is shifting and CIOs tasked to understand the latest legislative changes, or the consequences of the latest high profile data breach, are struggling to make sense of the landscape.

As an example of the rapidly changing regulatory environment, NetApp’s World Wide Data Governance Officer Sheila FitzPatrick, says the new EU data protection regulation that goes into effect in early 2018 will fundamentally change data privacy laws, impacting the way any company does business in Europe, regardless of whether they have a physical presence there. If a company processes personal data of any EU citizen, she says, they will be impacted.

Difficult negotiations between the EU and the U.S. on Privacy Shield regulations will also have implications; the way new privacy laws unfold in Latin America and the Asia Pacific region will need to be understood; and Canada’s embedding of the world’s most restrictive data sovereignty provisions into already strict data privacy legislation, will demand attention.
Why the sudden urgency?
Data privacy laws have been around for more than 30 years, but the urgency of issue is now palpable.

“You can’t pick up the newspaper, or read something on the Internet, or hear something in the business world and not understand there are laws out there that are protecting personal data - meaning what can and cannot be done with data, what companies can collect and what they can share,” says FitzPatrick.

High profile breaches and ramped up media attention fueled by social channels focus the spotlight on the issue, but FitzPatrick points to the development of technology-driven business models like the cloud, and the proliferation of data on any device, as the more foundational reasons.

“The proliferation of information is expanding. Big data is everywhere. You can acquire it in any location, on any type of device and people are increasingly concerned about how the data is being gathered and how it’s being used,” she says.

Ben Young, Cogeco Peer 1’s Vice President and General Counsel, says growing awareness of the issue is morphing into action. Recently, he said there were demonstrations in 15 different U.S. cities, backlash against the FBI for asking Apple to breach iPhone security protocols.

“People are taking control of the issue... and customers are finally asking the right questions around data and security,” he said.

Different jurisdictions, different rules
FitzPatrick estimates about 80 per cent of the countries in the world have data protection laws that cover the fundamental issues of how personal data can be collected, how it can be used or shared, how consent must be obtained and the processes involved for the transfer of information to jurisdictions with inadequate data protection laws. She says there is a clear understanding that individuals are the owners of the data, companies are simply the stewards.
Young agrees, but notes there are variations within the 80 per cent. Some countries like Canada, Germany and Hong Kong use data security and privacy legislation “as a bit of a marketing tool” to turn their strong privacy laws into a key differentiator and a competitive advantage on the world stage.

But they both agree the United States takes a dramatically different view of the matter, noting the most powerful nation on the planet has the least restrictive data privacy laws in the world – looser than the Middle East or most third world nations.

In the U.S., Young explains, legislative and constitutional priorities focus on freedom of information. In the rest of the world, legislation is focused on the protection of privacy. American businesses may be serious about security, but privacy is a customer’s responsibility - and certainly not the government’s.

“The Americans really only have quasi-privacy laws,” agrees FitzPatrick. “There are exceptions to every law, and there is a loophole in every law.”

Young said the lack of any fundamental privacy legislation in the U.S. makes it hard to compare the relative effectiveness of the U.S. position to other countries. “All jurisdictions are not created equal and it behooves any user of the Internet to take a close look at that. It is especially important for a company choosing a service provider or other technology company that may handle your personal data.”

Young said if the U.S. wants to be seen as a viable location to host data and a place where technology can thrive, “it will need to proclaim that it cares about these issues.”

**Data privacy versus data security**

The confusion between data security and data privacy is still commonplace in the industry, but as FitzPatrick points out, you can have the best security in the world, “but that does not mean you have any privacy.”
“If you think about data privacy as a wheel, data security is just one spoke on the wheel. It’s important because it is the fortress around protecting the data from unauthorized access and use, but data privacy is the whole fundamental aspect of legal and regulatory framework around the data you are allowed to have.”

Issues like security and encryption are important, but she says they follow privacy considerations and whether a company should have the information in the first place.

Security is a tool that can get you to privacy, says Young.

Moving to the cloud
Asked to identify the privacy and security issues companies must tackle if they move toward the cloud, the panel had several suggestions:

• Make sure your cloud service provider can pinpoint the location of your data. In countries like Canada with strict data sovereignty regulations, the answers are crucial. Just because a company can claim they offer data centers within a given jurisdiction, it’s important to know if the data may be backed up or replicated outside of the jurisdiction, or accessed by someone from outside the region.
• Understand where your provider stands on voluntary compliance.
• Ask whether your data management is outsourced to a third party.
• Conduct a privacy audit to determine which information is appropriate to put in the cloud. Remember that information that tracks to personal information can appear in different levels of information.

With rapid privacy and security changes, the pair agreed it is more important than ever before for a critical partnership to exist between the CIO and the corporate privacy officer. CIOs may not be responsible for privacy issues, but if they make technology decisions that put privacy data at risk, they could end up being responsible for the consequences.
Mitigating Risk

FitzPatrick says companies dealing with information management of any kind need to take a global approach. A country-centric approach, especially if based around the American model, will leave a company “dead in the water.” Better, she recommends, to develop a plan that deals with the most restrictive countries first, then there will be fewer problems as opportunities expand outward.

Other suggestions from FitzPatrick and Young include:
- Conducting privacy audits as well as security audits
- Know who can access your data
- Develop threat models that identify the threats to your data
- Be transparent. Don’t look for ways to get around legislation, learn how to work within it.

Show me the money

When people seem exclusively concerned about the cost and efficiency of moving into new technology, FitzPatrick says she doesn’t hesitate to point out that one major privacy violation can wipe out all the savings of a move to new technology.

“If your customers, or even your employees, look at you as a company and see that you don’t respect and comply with data protection regulations, you’re going to take a hit. Companies can recover from financial damage. It’s much harder to recover from reputational damage,” she says.
About Cogeco Peer 1
Cogeco Peer 1 is a wholly-owned subsidiary of Cogeco Communications Inc. (TSX:CCA) and is a global provider of essential business-to-business products and services, such as colocation, network connectivity, managed hosting, cloud services and managed IT services, that allow customers across Canada, the United States and Western Europe to focus on their core business. With 21 data centers, extensive FastFiber Network™ and more than 50 points-of-presence in North America and Europe combined, Cogeco Peer 1 is a trusted partner to businesses small, medium and large, providing the ability to access, move, manage and store mission-critical data worldwide, backed by superior customer support.

www.cogecopeer1.com

About ITBusiness.ca and ITWC
ITBusiness.ca is Canada’s leading information source for line-of-business professionals seeking to leverage technology to drive their business goals – from HR through to marketing and the C-Suite. Providing an overview of trends and technologies, ITBusiness.ca also offers insights into product availability, deployment challenges, and business outcomes within a Canadian context.

ITBusiness.ca is published by ITWC, a privately-owned digital media and content services company. Building on more than three decades of solid relationships with Canada’s technology decision-makers through award-winning excellence in journalism, ITWC delivers incisive, relevant information to executive and managerial audiences. It also provides leading, integrated marketing content strategies to clients, including more than 200 global Fortune 1000 companies.

ITWC is the exclusive Canadian affiliate of International Data Group (IDG) which publishes more than 300 publications worldwide.

www.itbusiness.ca | www.itwc.com