A Discussion with Éloïse Gratton
Introduction by Ian Rae

Even in the Cloud, Jurisdiction Matters

Updated 2017

Even in the Cloud, Jurisdiction Matters

Introduction—Data Governance in the Age of Artificial Intelligence

by Ian Rae

We live in the age of data, and if "data is the new oil" then the cloud is the refinery. But data, unlike oil, is not necessarily a commodity. Its value can be highly differentiated - consider top secret information or confidential financial, legal and health records. In many cases, the value of such data and the associated liabilities are dependent on the methods of governance and the legal jurisdiction governing the owner of the data, as well as the location of the data. But because data can transit networks and be in multiple locations, jurisdictions are frequently in conflict regarding how they treat the same data (see Microsoft vs US government).

What is clear is that it is early days in our understanding of data and its governance. Legally, data is treated as a "thing" that can be possessed. But unlike physical objects "information wants to be free". While the value of data in the market is increasing, the cost and efficiency of the technology to copy, share and even doctor the data has outstripped our capabilities to control it (ref: Panama papers, Wikileaks, Snowden), and the legal situations arising are without precedent, which can stress or break existing frameworks.

The explosion of the internet, the web, encryption (that is cheap, accessible and powerful), smartphones, and cloud computing has all happened in the last two decades and policy makers have struggled to keep up. The InfoSec industry has failed in "prevention" and few technology firms have the vision or capital to create products that are secure by design. Small armies of hackers scour the internet in a jurisdictional grey zone, collecting valuable data for a variety of uses. Most organizations have been infiltrated. "There are two types of companies in the world: those that know they've been hacked, and those that don't." (Misha Glenny)

The legal frameworks governing data are evolving rapidly, which is why we are updating this white paper and expect to do so regularly. Recently, the US government has tried to revoke data privacy protections for non-US citizens and has moved to allow ISPs to sell data about their users. The EU is deeply concerned about the data privacy and governance practices of Google and Facebook in particular, and Canada seems to be paying attention with recent decisions by the Supreme Court of Canada against both (see Facebook Privacy class action and Equustek vs Google). As these legal challenges escalate there will likely be watershed moments that will get broad attention from society and force us to make significant decisions about the balance between privacy and convenience.

The recent rise of AI seems likely to trigger just such a moment. We are experiencing a resurgence of AI approaches developed in academia decades ago, including neural networks, deep learning and reinforcement learning. These have been recently unleashed by the utility of cloud computing and the power of modern Graphical Processing Units (GPUs), that are almost accidentally useful at training models that, once built, can then be run on cheap modern consumer grade technology such as smartphones and IoT devices. Machine learning requires huge amounts of data; in many cases having data has been shown to be more important that having sophisticated algorithms. As a result, there is a battle for control of and access to valuable "big data". The UK National Health Service controversially agreed to share data on 1.6 million patients in a partnership with Google's "DeepMind". We expect rapidly escalating investments in striking such agreements as AI allows industry to "mine" valuable results from industrial data. As the value of such data sets escalates, we expect data governance and jurisdiction to be pushed to the forefront of the conversation, and have significant impact on decisions of where to store, process and secure data.

cloud.ca has a clear vision of a future where there is a need for cloud services that can comply completely with regional governance, minimizing inter-regional conflicts in laws or norms, while providing standardized and open compute services. We expect regional, secure, open source based cloud services to be complementary to the proprietary globalized platform services offered by Amazon, Microsoft and Google. The evolution of norms and laws in the coming decades will provide a tug of war between the two models of commodity cloud infrastructure vs differentiated cloud platforms and we expect each approach will be a good fit for different use cases. The key will be achieving the right balance and reserving the right to change that when laws and norms change.

Even in the Cloud, Jurisdiction Matters

A Discussion

with Éloïse Gratton

Éloïse is a partner at Borden Ladner Gervais LLP (BLG) and National Co-Leader of the Privacy and Data Security Practice Group, based in Montreal. Éloïse is one of Canada's foremost experts in the field of privacy and is recognized as the "go to" person, relied upon nationally (by both federal and provincial privacy commissioners, as well as by the federal government) as well as internationally. Read Eloïse's full bio here.

1 Why does jurisdiction matter for cloud? How does this impact data storage and processing?

A jurisdiction is an area within which a particular system of laws is used (e.g. Canada, US, EU). Jurisdiction arises regularly as a concern in cloud computing, because cloud computing is borderless, potentially involving several parties in different countries. For instance, a company could be established in France, and have its data centers and cloud services run from Canada, but its customers mainly located in Brazil, meaning the data potentially transits across three jurisdictions and the cloud service provider has potential links with all three. Data may fall under the jurisdiction of any country to which the service provider or data is connected; this means that it is important to consider where the cloud computing service provider is based, where the client is located, the citizenship of the persons whose data is being uploaded to the cloud, etc.

For each additional jurisdiction that comes into play, it is necessary to consider whether it introduces any meaningful risk to the data in respect of applicable privacy, data security and other relevant laws. Indeed, jurisdiction matters because once an organization uses cloud services in another jurisdiction, the data transferred to that foreign jurisdiction becomes subject to its local laws, regardless of the terms of an outsourcing contract. In fact, data privacy and security obligations, which are the main concerns when it comes to cloud computing, can to a certain extent be set out contractually to ensure compliance with laws or help protect against potential liability towards clients. For this reason, we emphasize that the minimum concerns in the choice of a cloud provider in respect to jurisdiction pertain to the enforceability of the relevant contract and the existence of a fair and mature legal system within that country. Many if not most developed countries will meet this basic requirement.

Beyond applicable local laws and the ability to enforce contractual obligations negotiated with a cloud service provider, jurisdiction matters in the particular context of the EU, whose privacy laws prohibit the transfer of personal information to another jurisdiction unless the European Commission has determined that the other jurisdiction offers "adequate" legislative protection for personal information. Jurisdiction is therefore an important concern for European clients, as illustrated by the recent Safe Harbour ruling by the European Commission, declaring that the United States offers inadequate protection to personal information (which we discuss in greater detail below), but this concern is limited to ensuring that the foreign jurisdiction has been deemed "adequate" by the European Commission.

2 What types of data does Canadian regional jurisdiction have a notable impact on?

Given that Canadian privacy laws regulate all data that qualifies as "personal information", Canadian jurisdiction has a notable impact on this type of information, usually defined as *information about an identifiable individual*, a notion interpreted extremely broadly throughout Canada. The Office of the Privacy Commissioner has even taken the position that information collected for the purpose of Online Behavioral Advertising to be "personal information", even if the name or the contact information of the individual behind the marketing profile is unknown, given, among other things, the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals.

Moreover, under Canadian privacy laws, personal information that is considered *sensitive* must be safeguarded with more stringent security measures and therefore, Canadian jurisdiction may also have a notable impact on categories of data considered as sensitive information.

Even in the Cloud, Jurisdiction Matters

According to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), any information can be sensitive, depending on the context.

Information may, for instance, be sensitive because it is the type of information which may be used to commit fraud against an individual. This would include information such as financial records and other financial information associated with a financial account, balances, date of birth, unique numbers such as SINs, driver's' license numbers, etc. Information may also be considered as sensitive when it is inherently intimate by nature, for instance information relating to medical and health conditions (PIPEDA states that some information "such as medical records" are almost always considered to be sensitive, and specific health data protection laws have also been adopted in certain Canadian jurisdictions.), things relating to private, family life and one's home (information concerning a person's behavior or conduct at home) and information concerning a person's sexual life or sexual activities. Moreover, matters relating to an individual's religious beliefs, political and philosophical opinions, as well as information pertaining to an individual's race or ethnicity are often considered as sensitive.

New types of information such as biometric information, facial recognition and geo-location information may also be considered as sensitive.

People's private communications are also usually considered to be of sensitive nature. For instance, the Criminal Code of Canada under articles 183 and 184 prohibits the interception of private communications, given the sensitivity and private nature of this type of information. In Quebec, the Civil Code, art 36 (2), states that intentionally intercepting or using "someone's private communications" is considered as an invasion of privacy.

Another type of information usually considered sensitive is information which tends to reveal intimate details of the lifestyle and personal choices of the individual. Under section 8 of the Canadian Charter of Rights and Freedoms, information receives constitutional protection if it forms part of a "biographical core" of intimate details or lifestyle choices.

3 Which industries does Canadian regional jurisdiction have a notable impact on?

Given its broad reaching data protection / privacy laws, Canadian jurisdiction has an impact on any organization that manages personal information—either a high volume of personal information (customers' or employees' information) or that manages sensitive information. Such industries may include public sector organizations as well as private sector organizations involved in health services, financial services, consumer credit, information technology, security and technology, retail (as well as any business operating a reward or loyalty programs), etc. Certain of these industries, such as the ones involved in health, finance and consumer credit, are highly regulated and must respect additional provisions regarding compliance, privacy and data security.

4 What types of legislation should be considered when choosing a region outside Canada for cloud?

National security and law enforcement legislation are often cited as the biggest concerns when it comes to choosing a region outside Canada for cloud. In the US, the USA Patriot Act has given far-reaching search and surveillance powers to the US government, including over foreign-owned data located within the US. For example, the Canadian federal government, when outsourcing its email systems to the cloud, has required that the email system databases be hosted in Canada because of privacy concerns stemming from this USA Patriot Act. Many European countries permit even broader law enforcement and national security access to information than the US. If an organization chooses to outsource its data outside of Canada, it must be conscious of the fact that the data can arguably be accessed more easily by a foreign government. For this very reason, having a jurisdiction where laws are similar to the ones in Canada is useful, because clients have an expectation that their information will be protected in the same or at least in a similar manner even when

Even in the Cloud, Jurisdiction Matters

outsourced. Doing so may address some of the privacy and data concerns from clients, as well concerns relating to intellectual property or trade secrets protection.

5 What does the recent Safe Harbour ruling mean for Canada?—Updated 2017

The recent Safe Harbour ruling is a judgment issued by the Court of Justice of the European Union ("CJEU") on October 6, 2015, invalidating an important Commission Decision 2000/520 which was validating the EU-US Safe Harbour Principles. Pursuant to Directive 95/46/EC, EU Member States are required to provide that the transfer of personal data from Europe to a third country may take place only if the third country in question ensures an adequate level of protection. Until recently, any transfer of personal data from the EU to the US was covered by Commission Decision 2000/520 which had found that transfers from the EU to the US provided adequate protection where the recipient complied with the EU-US Safe Harbour Principles.

As a result of this CJEU's ruling, a new framework for transatlantic exchanges of personal information for commercial purposes was established between the EU and the US in 2016. This framework, known as the "Privacy Shield", seeks to protect the fundamental rights of Europeans whose personal data is transferred to US servers by giving EU citizens better means to seek redress in case of disputes.

The judgment from the CJEU - along with the new Privacy Shield framework - mostly impacts signatories of the Safe Harbour Principles. This being said, it may also impact Canadian multinationals which have either relied on the Safe Harbour Principles to transfer data from their EU to US operations, Canadian businesses that host EU data with service providers with operations in the US, or who outsource services to US service providers for customers resident in the EU. Unless a Canadian organization is involved in any such or similar operations, it is not currently impacted by this CJEU's decision and the Privacy Shield.

Many Canadian organizations are hosting and processing personal data transferred from the EU in Canada. This means that any personal data transferred from the EU would be governed under applicable Canadian private sector data protection laws such as PIPEDA and substantially similar provincial laws pertaining to the collection, use and disclosure of personal information.

In 2001, the EU Commission issued 2002/2/EC: Commission Decision of 20 December 2001 finding that PIPEDA is considered as providing an adequate level of protection for personal data transferred from the EU to Canada. In light of this, many Canadian businesses which are acting in compliance with PIPEDA at all times when processing personal data, are not impacted by this recent CJEU's judgment. It should be noted that with the upcoming entry into force of the new General Data Protection Regulation ("GDPR") in 2017-2018, these "adequacy" are likely to be back on the table.

Finally, it will be important to monitor the impact of US president Donald Trump's January 2017 executive order. As a result of this executive order, US agencies are now required to ensure, to the greatest extent consistent with applicable law, that their privacy policies exclude persons who are not US citizens or permanent residents from protections granted by the federal public-sector Privacy Act. This executive order may have a certain impact in the context of the new Privacy Shield framework, given that Privacy Act protection will be minimized for foreigners, including EU citizens. It may also be considered by Canadian businesses considering transferring personal information to the U.S. in their privacy impact assessment.

6 Is Canadian law particularly "good" or "bad" for certain types of data?—Updated 2017

Canadian law affords solid legal protection to personal information, and even more so to data considered as sensitive information. Canada also has strong constitutional protection against unreasonable searches as obtaining data relating to communications, transmissions and the like requires a warrant in order to do so. Even requests from legal authorities for subscriber information now require a court order following R. v. Spencer, which declared that subscribers' data was worthy of constitutional protection. Overall, the Canadian government is usually

Even in the Cloud, Jurisdiction Matters

prohibited from accessing data for surveillance, although we have recently received Bill C-51, the Anti-Terrorism Act, which brought in more intrusive measures. With the change in government, we were expecting that this law will be modified given that the new government has committed to changing it by repealing the problematic elements of Bill C-51, and introducing new legislation that better balances Canadians' collective security with their rights and freedoms. While that has not been the case yet, it is still expected that certain changes will be brought to the Anti-Terrorism Act in the medium to long term, although the scope and depth of such changes remain unclear.

7 How can "who owns and operates the cloud" impact jurisdiction?

Data is usually subject to the laws of the jurisdiction with which it has a real and substantial connection. This may be the jurisdiction in which the data is stored and to which the cloud provider is reasonably connected to. The location of the owner of the data and the type of data may also be taken into account, but are not necessarily determinative as the data may fall under the jurisdiction of any country regardless of ownership and type of data. For instance, in Microsoft v. United States, an appellate US federal court reversed a district court decision and ruled that the US government did not have the right to demand emails stored in a foreign jurisdiction by an email provider headquartered within US borders. The court agreed with Microsoft's argument that cloud information stored on its servers in Ireland should fall under the jurisdiction of the land where its servers are located. The Supreme Court has recently accepted to hear the appeal of this case by the US government.

8 Are there notable differences between Canadian provinces' legal jurisdictions when it comes to data/cloud?—Updated 2017

Not so much. In Canada, PIPEDA sets out ground rules for how private sector federal works, undertakings and businesses collect, use and disclose personal information in the course of their commercial activities, unless such activities are regulated by provincial legislation that has been declared substantially similar to PIPEDA. Three provinces have enacted provincial data protection legislation that has been recognized as substantially similar to PIPEDA, and therefore, this legislation operates in place of PIPEDA in those provinces for intra-provincial matters. These include the British Columbia PIPA, the Alberta PIPA and the Quebec Act on the Protection of Personal Information in the Private Sector (PIPEDA and these three provincial laws are referred to as the "Canadian Data Protection Laws".)

There is no restriction under these laws to transfer personal information outside of Canada but at the very minimum, Canadian private sector organizations have to enter into a service agreement, and individuals have to be notified of this cross-border transfer:

- Outsourcing Restrictions: Under all these Canadian Data Protection Laws, a business should use contractual means (enter into a contract with the foreign entity) to provide a comparable level of protection while the personal information is being processed in the foreign jurisdiction. This contract should also address or prohibit any re-transfer of the data and be reflective of the kinds of security obligations which may apply. Some jurisdictions may have more stringent provisions. For instance, in Quebec, section 26 of An Act to establish a Legal framework for information technology, provides for a specific obligation for an organization to actually inform a service provider as to the privacy protection required for a technology-based document. This translates into an obligation for any Quebec organization to actually inform its cloud service partner as to the kinds of security measures the service provider should adopt when handling the organization's technology-based document containing personal information.

- Obligation to Inform Individuals of the Location of Their Information: Recent decisions (PIPEDA case summary #2008-394, #2006-333; and #2005-313) of the federal Privacy Commissioner under PIPEDA indicate that individuals should be notified if their personal information will be transferred to and/or stored in a foreign country, and further, that they should be notified of the fact that such information will be subject to foreign laws and

Even in the Cloud, Jurisdiction Matters

may be disclosed to foreign authorities under such laws. In Quebec, there is a legal requirement (under s. 8(3)) that individuals be notified of the location where their personal information will be held. Under the Alberta PIPA, individuals also have to be informed of the fact that their information will be transferred outside of the country. Based on the PIPEDA decisions described and the Quebec/Alberta legal requirements, it is recommended to notify individuals that their information may be transferred to a foreign country and that it will be subject to such foreign country's laws and disclosure requirements. This can usually be done via a privacy policy or a "cross-border" provision can be included in the user agreement. In Quebec, the Commission d'accès à l'information ("CAI"), the province's data protection regulator, recently recommended that organizations undergo a privacy impact assessment to determine the risks associated with the transfer of personal information outside of Quebec prior to completing any cross-border transfer of personal information.

As for Canadian public sector entities, personal information that they manage may be governed by specific public sector laws or health laws which may, in some jurisdictions, provide for more stringent legal requirements and prohibit the transfer of personal information outside of a given province or outside Canada. For example, section 30.1 of the British Columbia's **Freedom of Information and Protection of Privacy Act** and section 5 of the Nova Scotia **Personal Information International Disclosure Protection Act** include some cross-border restrictions. As for Quebec, provincial government bodies and private sector entities are required to ensure that personal information receives protection equivalent to that afforded under the province's privacy laws before it is released outside the province or entrusted with an organization with the task of holding, using or releasing it on its behalf. The Quebec CAI has recently issued its position on this issue in its fall 2016, in its report entitled "Rétablir l'Équilibre" in which it recommends that organizations undertake a privacy impact assessment before transferring personal information outside the territorial limits of Quebec. As for personal health information, we can find cross-border restrictions in many of the relevant laws including the ones from New Brunswick, Ontario, Yukon, Newfoundland and Labrador.

9 Does keeping the data encrypted in transit and "at rest" overcome the challenges with regional jurisdiction?

One of the main risks with cloud computing pertain to having data in transit over the open Internet, although this risk can be mitigated by the use of SSL or other encryption technologies to ensure that the information will be safe while in transit. On the issue of security measures to adopt when using the Internet or computers to transmit or store personal information, PIPEDA Case Summary **#2008-395** confirms that in the context of a security breach involving financial information or driver's license, the fact that personal information was not encrypted (or was not encrypted with up-to-date encryption technology) was determined to be a liability issue.

While keeping the data encrypted in transit and "at rest" will address the security requirements from the Canadian Data Protection Laws, it is not clear that encrypted data is automatically considered "anonymized" (and therefore, no longer subject to privacy laws). Encrypted data is usually reversible and therefore, it may be possible in some cases to re-identify the person to whom the encryption relates. To ensure that the data is considered as depersonalized or anonymized (and therefore, falls outside the scope of Canadian Data Protection Laws), the process used should not be reversible.

10 Long term, do you expect globalization of digital business eliminate barriers to who can store, manage and process data? Or will restrictions over where a company is based, the citizenship of employees and the location of the services remain an important factor for many industries?

It is difficult to say whether the barriers will eventually be eliminated. On a global scale, most countries are using a similar legal framework on the issue of data protection, one which is based on the **Fair Information Practices** which dates back to the early 70s. This being said, data protection / privacy laws may remain different simply due to cultural differences. For instance, the EU is considered as one if not the most privacy stringent jurisdiction in the world, but the US is not, in part, because it strongly values

Even in the Cloud, Jurisdiction Matters

freedom of information. Canada sits somewhere in the middle, probably leaning towards the position of the EU, with Quebec having the most stringent privacy laws in Canada. What might happen in the long run are globally accepted standards that make data outsourcing easier playing a more important role—we can think, for example, of ISO security standards such as **ISO/IEC 27018.**

info@cloud.ca
@cloud_dot_ca

420 Guy Montreal, QC H3J 1S6
1-888-796-8364

Even in the Cloud, Jurisdiction Matters

About Éloïse Gratton

Eloïse is a partner at **Borden Ladner Gervais LLP** and National Co-Leader of the Privacy and Data Security Practice Group. She advises clients from various industrial sectors on legal, practical and ethical issues relating to the protection of privacy or anti-spam legislation, in connection with their new projects, products, practices and technologies, providing them, both nationally and internationally, with strategic advice on matters of risk management and regulatory compliance, advising as to best business practices, conducting privacy audits or privacy impact assessments and assisting them in crisis management situations (e.g. class actions for breach of privacy, security breaches, privacy commissioners' or CRTC's investigations).

Éloïse is one of Canada's foremost experts in the field of privacy and is recognized as the "go to" person, relied upon nationally (by both federal and provincial privacy commissioners, as well as by the federal government) as well as internationally. She has testified before the House of Commons, Standing Committee on Access to Information, Privacy and Ethics as well as before the Standing Committee on Industry, Science and Technology. On the international scene, she is a member of the International Association of Privacy Professionals (**IAPP**) Women Leading Privacy Advisory Board.

She has published several books on privacy issues, which have been cited by the Supreme Court of Canada in some of its landmark privacy decisions. She authored *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, one of the first technology and privacy book in Canada (CCH, 2003). Her recent works include *Practical Guide to e-Commerce and Internet Law* (LexisNexis 2015), *Privacy in the Workplace* (CCH, 2014) and *Understanding Personal Information: Managing Privacy Risks* (LexisNexis, 2013). She holds a doctorate degree in privacy law (University of Paris II and U of M) and she has been teaching e-commerce law and privacy and IT law at University of Montreal for several years.

Eloïse is called upon regularly to comment on news reports dealing with new media and privacy issues in Canada, the United States (Wall Street Journal, Fast Company) as well as internationally (U.K., France, Brazil). Her IT and privacy blog was recently awarded Clawbies: Canadian Legal Blog Award. In 2015, she was among the finalists for *Canadian Lawyer* magazine's most influential Canadian lawyers. She was selected by her peers for inclusion in *The Best Lawyers in Canada* 2016 in the field of IT law and ranked by Chambers 2016 as a leading data protection and privacy lawyer.

www.eloisegratton.com

About us

cloud.ca is a regional cloud service for businesses requiring that all or some of their data remain in Canada, for reasons of compliance, performance, privacy or currency. Given the geo-political landscape and the increasing value of data, we believe organizations need to start thinking about the type of data they collect, where it resides and who controls it.

info@cloud.ca
@cloud_dot_ca

420 Guy Montreal, QC H3J 1S6
1-888-796-8364