Office of the
Privacy Commissioner
of Canada

Reaching for the Cloud(s):

Privacy Issues related to Cloud Computing

March 2010

Table of Contents

Executive Summary 1
Review of Cloud Computing 2
What is Cloud Computing? 2
Overview of the Cloud 2
Overarching Problems with Cloud Computing 3
Seeming Jurisdictional Neutrality 3
Consumer Lack of Control 4
Compromising Meaningful Consent 4
Function Creep 4
Innovation Dampening 4
Privacy Risks of Cloud Computing 5
Jurisdiction 5
Creation of New Datastreams 5
Security 5
Data Intrusion 6
Lawful Access 6
Processing 6
Misuse of Processing Data 6
Permanence of Data 7
Ownership of Data 7
Reach of the Office of the Privacy Commissioner 7
Processing 7
Direct cloud relationship 8
OPC-specific Jurisprudence 8
Accusearch 8
Canadian Jurisprudence on Jurisdiction 9
The Ground Rules 9
Morguard 9
Beals 10
Jurisdiction on the Internet 11
Disney 11
Intermix 12
Conclusion 13

Executive Summary

Cloud computing is a general term for an emerging kind of infrastructure. It describes any system where information and/or applications are stored online, allowing access to be achieved by the user via a device. For the purposes of that application or data the personal computer becomes in essence a “dumb terminal”, a machine that interacts with a cloud-mainframe in order to store, retrieve, or manipulate data.

Overarchingly, the cloud computing model raises concerns about:

- Appearance of jurisdictional neutrality
- Consumer lack of control
- Compromising meaningful consent to advertising
- Function creep
- Innovation dampening

There are also privacy-specific issues inherent in the cloud infrastructure:

- Jurisdiction
- Creation of new data
- Security
- Data intrusions
- Lawful access
- Processing
- Misuse of data
- Data permanence
- Data ownership

Where the Privacy Commissioner has jurisdiction over the subject matter of a complaint but the complaint deals with cloud infrastructure(s) and thus is not obviously located in Canada, current jurisprudence is clear that the Privacy Commissioner may exert jurisdiction when her assessment indicates that a real and substantial connection to Canada exists.

Real and substantial connection, as a test, must be approached from the standpoint of principled flexibility and although the jurisprudence sets out a number of factors that may be considered in making the assessment, the list is not exhaustive and none of the factors are determinative in and of themselves – it is clear that the assessment must be conducted on a case by case basis, taking into account the entire context of the complaint.

Review of Cloud Computing

What is Cloud Computing?

The term "cloud computing" is seemingly omnipresent these days – it appears in media reports, in business literature, in technology literature. At the same time, the term is so nebulous that many consumers may not be fully aware of what cloud computing actually is.

A 2008 Pew Internet Study defined cloud computing as "an emerging architecture by which data and applications reside in cyber space, allowing users to access them through any web connected device."[1] As such, cloud computing includes such common activities as storing photos online (on sites such as flickr); storing videos online (at sites like YouTube); using online applications such as Google's Office suite, Facebook or Twitter; using webmail like gmail or hotmail; paying to store computer files online or even backing up files online using services such as Jungle Disk. Indeed, the Pew Internet Study focused on these 6 activities, and shows that 69% of the online users surveyed had performed at least one of the listed activities, with 40% of the users performing two or more of the activities.[2] Such high numbers of uptake suggest that cloud computing isn't "the wave of the future" as much as it is an increasingly common use of today.

Jonathan Zittrain includes what he calls "tethered appliances" within the cloud, cautioning that such devices may be particularly insidious because "the code and data may well remain near the user so they do not seem" to be cloud computing devices, though they actually are because the user has ceded her freedom to control her code and data.[3] Such tethered appliances would include the ubiquitous iPhone as well as reading devices such as Amazon's Kindle.

However cloud computing is engaged, the effect may be said to replicate the mainframe/terminal days of early computing – that is, the personal computer becomes in essence a "dumb terminal", a machine that interacts with a cloud-mainframe in order to store, retrieve, or manipulate data.

Overview of the Cloud

A survey of the literature suggests that the value of cloud computing for organizations is evident. After all, cloud computing infrastructures allow for immediate access to hardware resources without capital investment, get projects to market faster because they don't require tech setup, allow for IT to be charged as an operational cost, and make it easier to scale operations.[4] As Cory Doctorow points out, the cloud infrastructure also allows companies that supply services to access unlimited amounts of storage and hosting,

---

[1] John B. Horrigan (September 2008) "Data Memo: Use of Cloud Computing Applications and Services". Pew Internet and American Life Project at http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf [Pew Internet]

[2] Pew Internet at 1

[3] Jonathan Zittrain (30 July 2009) "Ma'am, the cloud is coming from inside your house" Future of the Internet (and how to stop it) Blog. [Zittrain Blog]

[4] Bandyopadhyay, Subhajyoti, Marston, Sean R, Zhang, Juheng, Li, Zhi and Ghalsasi, Anand, "Cloud Computing: The Business Perspective" (June 3, 2009). Available at SSRN: http://ssrn.com/abstract=1413545 at 7 [The Business Perspective]

and those who run supercomputer applications to tap into the existing high performance computing grid rather than attempting to duplicate it.[5]

Nevertheless, there seem to be a number of drawbacks inherent to computing in the cloud as well. Cloud computing infrastructures are premised on a business model that charges the consumer fees on a perpetual basis for something that they currently pay a flat rate for or even receive for free. Cloud computing depends on net access, access is arguably slower, more expensive and less reliable than hard drives or central processing units (CPUs), and may also be prevented, surveilled or tampered with by external forces, such as government, employers or law enforcement.[6] And, of course, although users pay for the service, they do not have or are not granted "the expertise or control over the technology infrastructure that provides these services."[7] Given these drawbacks, it is surprising to see the uptake of cloud computing that we are seeing, but the Pew Internet Survey suggests that ease, convenience and flexibility are at the root of this uptake. In the survey, 51% of users cited ease and convenience as a reason for use; 41% liked the flexibility of not being tethered to a site or device; and 39% liked the ease of data sharing that cloud computing facilitates.[8]

Cloud computing then, would appear at its most basic to cover any system where information and/or applications are stored online, allowing access to be achieved by the user via any device. This purposely general definition allows for a variety of "cloud computing" situations – an individual user interacting with a cloud application; a company creating a private cloud infrastructure for use within its environs; or even an organization (online or offline) who chooses to use the cloud infrastructure for its data storage and/or processing.

Overarching Problems with Cloud Computing

Once we understand what cloud computing is, a number of overarching problems become evident.

Seeming Jurisdictional Neutrality

First, there is what Picker calls "cloud neutrality" – that is, the "implicit assumption…that changing the location of processing or storage doesn't change anything about how the data stream associated with the processing or storage is used."[9] This, of course, may not be the case and may accordingly cause problems both for organizations who opt to contract with cloud infrastructure providers and for cloud infrastructure providers themselves as well as putting the data and thus the privacy of the individual ultimately at risk.

---

[5] Cory Doctorow (2 September 2009) "Not Every Cloud Has a Silver Lining". The Guardian. http://www.guardian.co.uk/technology/2009/sep/02/cory-doctorow-cloud-computing
[6] Doctorow
[7] The Business Perspective at 7
[8] Pew Internet at 2
[9] Randal C. Picker (2009) "Competition and Privacy in Web 2.0 and the Cloud". John M. Olin Law & Economics Working Paper No. 414 (2d series). University of Chicago at 7 [Competition and Privacy]

Consumer Lack of Control

The recent events with the Kindle also point to some problems inherent in the cloud model, especially in relation to tethered appliances.[10] Whether it is Amazon deciding to remove already purchased copies of a particular novel from people's Kindle libraries without their consent, DRM sites shutting down and thus denying consumers access to music that they have paid for, or even the exercise of power that is implicit in strategies such as Apple's "approval" process for iPhone applications and the implications that has for censorship, it is clear that letting the power reside in the provider of a site can and does create unforeseen problems and risks for consumers.

Compromising Meaningful Consent

The model itself also creates problems. That is, if the cloud model becomes the de facto model of computer use, then companies will no longer be supporting themselves by selling actual copies of their software. There is a risk attendant upon this – that abandoning the sale of content will lead necessarily to a dependence on the free, advertising-supported content model.[11] While there is no problem inherent in this model itself, it does (arguably) become a problem when there are no longer alternatives and thus meaningful choice and consent to such a model becomes less viable.

Function Creep

The cloud computing model may also act as an incentive for companies to extend the size and scope of their organization or their consents in order to take advantage of the information they're gathering.[12]

Innovation Dampening

In terms of competition and innovation the cloud computing model also raises concerns. Critics have pointed to the site specificity that may be created or built in doing business with a particular cloud entity.[13] For instance, some organizations rely on information built up over long periods of time for the optimal efficacy of their platforms – this time investment combined with the Terms of Use provisions that forbid exporting the data to other sites creates dual problems, with user ability to switch providers being restricted at the same time that innovation and the creation of alternate platforms for similar services are restricted because users are less likely to be willing or able to switch platforms.

---

[10] Jonathan Zittrain (20 July 2009) "Lost in the Cloud". OP-ED, New York Times 20 July 2009 [Zittrain NYT]
[11] Randal C. Picker (2009) "Online Advertising, Identity and Privacy" John M. Olin Law & Economics Working Paper No. 475 (2d series) University of Chicago
[12] Competition and Privacy at 13
[13] Competition and Privacy at 9

Privacy Risks of Cloud Computing

Given that cloud computing creates a distance relationship between individuals and their data, there are inherent privacy problems with the model, and with the application of regulatory powers to the model.

Jurisdiction

By its very nature, cloud computing has the possibility of sending, storing and processing data in multiple jurisdictions. Depending on data protection laws and approaches, this may create problems of jurisdiction.[14] Indeed, an ascendency of the cloud model may even call into question the whole notion of data "ownership" upon which much data protection is based, leading instead to analyses that are based on data authentication.[15]

Creation of New Datastreams

The cloud model has the potential to create a huge collection of (new) data, and to expose it to the infomediary/cloud provider. When the infomediary has the ability to see what is happening with every click, this creates a rich stream of data.[16] Although this datastream may not be relevant to the original cloud operation(s), there is a risk that it will be used either by the organization or the cloud infomediary for purposes beyond those for which consent was originally given. In the Pew Internet Study, users expressed great concern about the (mis)use of their data in the cloud – 90% were concerned about their data being sold to another organization; 80% expressed concern about their photos or other data being used in marketing campaigns; and 68% said they would be concerned if their data were analyzed and used to serve them with targeted advertising.[17]

Security

By definition, cloud computing means the sharing/transfer of information across the internet. This raises security concerns, both in the protection of those streams as well as in the safeguards and security applied to the data while it resides in the cloud.

Christopher Soghoian has raised questions about the security of cloud computing transactions, pointing out that cloud providers have tended to "forgo strong security solutions"[18] As support for this contention, he points out that at a minimum, cloud providers could (and should) be using the kinds of encryption currently used by online banks and retailers to protect their data streams, but currently most are not. As for security of

---

[14] The Business Perspective at 9
[15] The Business Perspective at 14
[16] Competition and Privacy at 5
[17] Pew Internet at 2
[18] Christopher Soghoian (2009) "Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era". SSRN

storage, as Doctorow points out, were cloud applications to be designed for the benefit of users rather than for business model efficacy, the data would be heavily encrypted.[19]

Data Intrusion

As discussed, individuals give up a level of control when they interact with the cloud infrastructure. This may take place in a number of ways – cloud service providers or cloud-based applications, who may be able to access, mine or otherwise commoditize the data they hold; government and/or private exercises of power that result in management or shutting down of particular sites or discourses; or simply private actors for whom the lure of such ripe databases is irresistible. In every case, not only is the individual's data in the cloud infrastructure at risk, but the individual may never be aware of the intrusion.

Lawful Access

Beyond the generalized risk of government intrusion, cloud computing also raises particular concerns when it comes to lawful access. Lawful access itself is, of course, of concern whether the information is stored on a user's computer, with an ISP or in the cloud. However, use of the cloud infrastructure raises some additional risks.

For instance, where many companies are using a centralized cloud infrastructure, a lawful access request to the cloud provider has the potential to garner information from all the diverse companies. Alternatively, where personal data and ISP data are stored together in a cloud, a lawful access request may result in access to information above and beyond that intended by lawful access legislation. Finally, as with other forms of intrusion, the remove that is created between data and holder by the cloud infrastructure increases the possibility not only of individuals being unaware of lawful access to their data, but their service providers potentially being similarly unaware.

Processing

An organization contemplating moving towards storage or processing using the cloud computing infrastructure of a third party should be considered to be "outsourcing for processing" and accordingly needs to consider issues of security of the information (both from intrusion and in terms of backup and recovery), binding the cloud provider to privacy controls equal to those imposed on the organization as data controller, and must ensure that access and correction procedures are possible, and that deletion procedures are adequate and appropriate.

Misuse of Processing Data

It is especially important to set such parameters on a processing or storage relationship, because of the possibility (discussed above) that a cloud provider might inappropriately access, manipulate or mine the data entrusted to them by an organization. In such a case, regulators will need to be able to distinguish between

[19] Doctorow

the actions of the cloud provider *as processor* and actions which are outside the processing relationship and thus will attract the attention of a regulator directly to them.

Permanence of Data

Another pervasive risk of cloud computing is the risk of data permanence. In addition to contractual measures to ensure data is protected while held by the cloud provider, it is important to consider what happens to the data at the end of the contract. Measures will need to be put in place to ensure that any copies of the data will be removed permanently from the cloud infrastructure, and within what time period this will be done.

Ownership of Data

In addition, the creation of new datastream(s) may raise concerns about ownership of data. While ownership of data entrusted to a cloud infrastructure for storage seems fairly straightforward, the ownership of data that is uploaded to a cloud-based infrastructure may be less certain. Finally, there is also the secondary data that is generated by interactions with a cloud-based infrastructure – although it may well be "personally identifiable information" for the purposes of PIPEDA, users may not be aware of the creation/existence of this data.

Reach of the Office of the Privacy Commissioner

The Privacy Commissioner of Canada is tasked with overseeing compliance with both the *Privacy Act*[20] and the *Personal Information Protection and Electronic Documents Act.*[21] The Privacy Act regulates the information-handling practices by Government of Canada bodies, while PIPEDA uses the federal government's trade and commerce powers to exert jurisdiction over the collection, use and disclosure of personal information by private sector organizations in the course of commercial activities.

Although it seems most likely that a complaint dealing with cloud computing would come under PIPEDA, it is also possible that the Government of Canada might create a "private cloud" infrastructure internally to facilitate information sharing, or even that some or all government institutions might make use of a cloud infrastructure for data processing or storage.

Processing

Where an organization has transferred data to a cloud-infrastructure provider, it is likely that under PIPEDA such actions would be considered as a transfer for processing, and accordingly under Principle 4.1.3 of Schedule 1 the organization would be required to ensure that a comparable level of protection is provided for the information. The organization would remain in control of the information and responsible for meeting the

[20] R.S.C. 1985, c. P-21
[21] S.C. 2000, c. 5

PIPEDA requirements. The Office of the Privacy Commissioner has investigated such complaints before and done so effectively. It has also released guidelines for transborder data flow.[22]

Direct cloud relationship

It is important to note that the transfer of information to a third party cloud-infrastructure provider for processing is not the only way in which the Office of the Privacy Commissioner might become involved. For instance, an organization (public or private) might create a "private cloud" in-house to facilitate information sharing between different locations or parts of the organization. Alternatively, an individual might interact with a cloud-infrastructure provider directly, either using it for storage or by accessing and using cloud-based applications. Finally, there is always the possibility that information entrusted to a cloud-infrastructure provider could be accessed, used, mined or otherwise commodified without consent by the cloud-infrastructure provider. In each of these situations, the provisions of the applicable legislation (PIPEDA or the Privacy Act) would apply to the subject matter of such a complaint.

OPC-specific Jurisprudence

In assessing the jurisdictional reach of the Office of the Privacy Commissioner, the following Federal Court decision is relevant.

Accusearch

The case of *Lawson v Accusearch Inc.*[23]was an application for judicial review in which the jurisdiction of the Office of the Privacy Commissioner was at direct issue.

In that case, an individual attempted to file a complaint with the Office of the Privacy Commissioner against Accusearch Inc., an American company that provides background searches, psychological profiles, e-mail traces, phone records etc. The individual alleged that Accusearch was collecting, using and disclosing personal information about Canadians for inappropriate purposes and without the knowledge and consent of the individuals in violation of PIPEDA.

On receipt of the complaint, the Privacy Commissioner examined the issue preliminarily and concluded that she was barred from accepting the complaint because investigation would require the exercise of her powers extraterritorially, which was outside the bounds of her jurisdiction as set out in PIPEDA.

Justice Harrington was of the opinion that the Commissioner's conclusion that she was barred from accepting the complaint was in error, suggesting that "the Commissioner did not distinguish her power to investigate from the effectiveness of her investigation."[24] He analogized the situation to that in SOCAN[25], where the Supreme Court of Canada found that there is sufficient connection for the taking of jurisdiction where Canada

---

[22] Guidelines for Processing Personal Data Across Borders (http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp)
[23] [2007] 4 F.C.R. 314
[24] Accusearch at para 27
[25] *Society of Composers, Authors and Music Publishers of Canada v Canadian Ass'n of Internet Providers*, [2004] 2 S.C.R. 427 at 457

is either the country of transmission or of reception, and found therefore that although the Privacy Commissioner was correct that Parliament had neither intended to nor effectively legislated extraterritorially, nevertheless PIPEDA could apply where the dispute was sufficiently connected to Canada to ground the exercise of Canadian jurisdiction.[26]

The Court went on to conclude that the Privacy Commissioner had jurisdiction to investigate complaints related to the flow of information across national borders.[27] This finding was based primarily on an analysis that showed that the Privacy Commissioner had jurisdiction over the subject matter of the complaint (the collection, use and disclosure of personal information) and over the person insofar as a reasonable and substantial connection could be found between the entity or the actions complained of and Canada. He also considered jurisdiction over the place, but found that the fact that an investigation might be ineffective because the Privacy Commissioner was unable to subpoena or otherwise force organizations in another country to cooperate with her investigation was not a sufficient ground to refuse jurisdiction over the complaint. Accordingly, the Federal Court granted the application for judicial review and returned the complaint to the Office of the Privacy Commissioner.

Accusearch, then, establishes that notwithstanding the extraterritoriality of a company or website, where the Privacy Commissioner of Canada has jurisdiction over the subject matter of a complaint and can establish a real and substantial connection to Canada, she may exert jurisdiction over the complaint.

Canadian Jurisprudence on Jurisdiction

The Ground Rules

Morguard

The germinal Canadian case on jurisdiction is *Morguard Investments Ltd. V De Savoye,*[28] which was about jurisdiction between Canadian provinces. This case dealt with the issue of whether the courts in one province (British Columbia) should recognize and enforce a judgment of the courts from another province (Alberta), when the defendant did not live in the issuing jurisdiction at the time of the action.

The Supreme Court of Canada decision begins with an understanding that "...the rules of private international law are grounded in the need in modern times to facilitate the flow of wealth, skills and people across state lines in a fair and orderly manner"[29] and proceeds from there in an attempt to address the issue bearing in mind this cross-border flow. In arriving at his decision, Justice La Forest considered many factors, looking at English and Canadian jurisprudence, academic works, the importance of the Canadian Constitution in establishing a unified cross-jurisdictional understanding of Canada[30] and the related issue of the judicial structure of Canada leading to the Supreme Court of Canada and thus ensuring that there is no differential

[26] Accusearch at para 26-29
[27] Accusearch at para 51
[28] [1990] 3 S.C.R. 1077
[29] Morguard at 22
[30] Morguard at 25

quality of justice among the provinces.[31] He concludes that "the rules of comity or private international law as they apply between the provinces must be shaped to conform to the federal structure of the Constitution."[32]

Accordingly, the Court determined in this case that "courts in one province should give full faith and credit...to the judgments given by a court in another province or territory, so long as that court has properly, or appropriately, exercised jurisdiction in the action."[33] In order to determine whether the exercise of jurisdiction was appropriate or proper, Justice La Forest used the test of whether "there was a real and substantial connection between the jurisdiction and the wrongdoing."[34]

Using this test, the Supreme Court of Canada determined that the action against De Savoye had been appropriately brought in Alberta. Indeed, given that the properties were in Alberta, the contracts were entered into in Alberta by parties then resident in Alberta, the foreclosure action took place in Alberta, La Forest opined that "a more real and substantial connection between the damages suffered and the jurisdiction can scarcely be imagined."[35]

Morguard, then, creates the basic test for appropriate exercise of jurisdiction – the presence of a real and substantial connection between the wrongdoing and the jurisdiction.

Beals

Of course, Morguard dealt with jurisdiction between provinces, but still within Canada. It was not until *Beals v Saldanha*[36] that this approach was approved for application to judgments that issue from courts outside of Canada. While some provincial courts had previously extended Morguard to apply to such situations[37], this was the first time the Supreme Court of Canada considered the issue.

Guided by the decision in Morguard, Justice Major concluded that:

> International comity and the prevalence of international cross-border transactions and movement call for a modernization of private international law. The principles set out in Morguard and further discussed in Hunt[38] can and should be extended beyond the recognition of interprovincial judgments, even though their application may give rise to different considerations internationally. Subject to the legislatures adopting a different approach by statute, the "real and substantial connection" test should apply to the law with respect to the enforcement and recognition of foreign judgments.[39]

---

[31] Morguard at 25
[32] Morguard at 26
[33] Morguard at 28
[34] Morguard at 31. This test is built upon Justice Dickson's decision in *Moran v Pyle National (Canada) Ltd* [1975] 1 S.C.R. 393
[35] Morguard at 33
[36] [2003] 3 S.C.R. 416
[37] See *Moses v. Shore Boat Builders Ltd.* (1993), 106 D.L.R. (4th) 654 (B.C.C.A.), leave to appeal refused, [1994] 1 S.C.R. xi; *United States of America v. Ivey* (1996), 30 O.R. (3d) 370 (C.A.); *Old North State Brewing Co. v. Newlands Services Inc.*, [1999] 4 W.W.R. 573 (B.C.C.A.)
[38] *Hunt v T&N plc*, [1993] 4 S.C.R. 289. This case dealt with a Quebec statute which barred the removal from Quebec of any documents relating to any business concern in Quebec. The barring statute was being used to frustrate an action in BC, and the Supreme Court of Canada ultimately determined that the presence of such blocking statutes was ultra vires the province since its pith and substance related to matters outside the province of Quebec.
[39] Beals at para 28

Beals, thus, extends the Morguard test of "real and substantial connection" to judgments outside the country.

Jurisdiction on the Internet

There are two recent cases in Canada which show how the "real and substantial connection" test is being applied to online entities.

Disney

Disney Enterprises Inc. v Click Enterprises Inc.[40] deals with a challenge by Disney to the various websites registered to Click Enterprises. The websites were registered with an address in Toronto, Ontario and the company is registered as an Ontario corporation. These websites sold memberships that provided customers with tools and technology to assist them with downloading (copyrighted) films, as well as offering on-line support to subscribers who were having trouble locating or downloading particular films they sought. Disney filed suit in a New York court, and received a judgment for $486,442.17. The decision from the Ontario Superior Court of Justice deals with the issue of whether the New York court properly exercised jurisdiction such that the Ontario court will enforce the New York judgment.

Justice Lax considered that the existing case law established that "the determination of the proper exercise of jurisdiction by a court depends on two principles: the need for order and fairness and the existence of a real and substantial connection to either the cause of action or the defendant."[41]

Where the participants to litigation are connected to multiple jurisdictions, Justice Lax opined that the order and fairness requirement was met where there were reasonable grounds for assuming jurisdiction. In this case, Justice Lax noted that Disney was a Delaware corporation, principally operating in California but distributing films throughout the United States and elsewhere. Click Enterprises, on the other hand, were Ontario residents and had registered the company in Ontario, but their business involved interactive websites through which subscription agreements were sold to residents of the US, including residents of New York. Given that it is established law in Canada that there is sufficient connection for taking jurisdiction where Canada is either the country of transmission or of reception[42], Justice Lax found that there were indeed reasonable grounds for the New York court to take jurisdiction, and thus that the order and fairness requirement was met.

When assessing whether there was a reasonable and substantial connection between New York and the action, Justice Lax canvassed the existing jurisprudence before doing an assessment on the facts of the individual case and determining:

> In this case, Click Enterprises had a commercial purpose that utilized the Internet to enter the United States to carry out its activities. It contracted with payment service providers in the United States to process Internet payments on its websites. Initially, Click contracted through a Canadian corporation

---

[40] (2006) 267 D.L.R. (4th) 291 (Ont. S.C.J.)
[41] Disney at para 11
[42] *Society of Composers, Authors and Music Publishers of Canada v Canadian Ass'n of Internet Providers*, [2004] 2 S.C.R. 427 at 457

and after VISA changed its regulations, it incorporated Click Enterprises Inc. (Delaware) so that payments were made through it. [43]

After concluding that there was a reasonable and substantial connection, Justice Lax went even further and addressed the arguments that were made by Click Enterprises that services were made available worldwide, not just in the US or New York, and that New York was a "random jurisdiction" and thus that the real and substantial connection test was not met. In response, Justice Lax noted that Click Enterprises was aware that they had American customers, that indeed the majority of "testimonials" on the websites were from Americans, and that "when activities are conducted on the Internet, they have the potential to cause harm anywhere and everywhere. The respondents' websites were available through normal distributive channels to the residents of New York and their products caused harm there."[44] She does imply, however, that had some juridical advantage inured to Disney by their choice of forum the Court might have looked deeper, but in the circumstances she was satisfied that New York "was not only an appropriate jurisdiction in which to bring the action, but one that was arguably fairer to the respondents than if it had been brought as it might have been, in a more geographically remote jurisdiction such as California."[45]

After considering the defences raised, Justice Lax concluded that New York had appropriately exercised jurisdiction over the case, and therefore that there was no barrier to enforcing the New York judgment via the Ontario courts.

Intermix

The other recent decision, also from 2006, is *Desjean v Intermix Media Inc.*[46] In that case, Patrick Desjean filed a proposed class action against Intermix Media, alleging that it violated the *Competition Act* by bundling spyware/adware with its free software without disclosing that bundling to consumers of the free software. Intermix was served notice of the claim and responded with an application for an order dismissing Mr. Desjean's claim on the basis that the Federal Court of Canada lacked jurisdiction.[47]

Although Intermix disputed the allegation that they had distributed spyware at all, or that they had failed to notify customers of the adware bundled with certain programs, the finding of the Federal Court was not based on this.

Justice DeMontigny ascertained that the appropriate test for jurisdiction was the real and substantial connection test, as set out in Morguard. He noted that: Intermix's servers were not in Canada and that suffering damage on a computer in Canada is not sufficient to establish a connection; that Intermix does not have offices in Canada and has never maintained or leased office space in Canada; that Intermix has no employees in Canada although it does have a contractual relationship with two independent contractors in Canada who provide services unrelated to this matter; that Intermix has not availed itself of any Canadian laws; that Intermix has no Canadian bank accounts, pays no Canadian taxes, is not registered for GST or PST purposes, and is not registered as a business in any Canadian jurisdiction; that Intermix does not advertise,

---

[43] Disney at para 22
[44] Disney at para 29
[45] Disney at para 29
[46] (2006) F.C. 1395
[47] In fact, they argued that either (a) Federal Court lacked jurisdiction over Intermix and the matter; (b) Mr. Desjean's claim was frivolous and vexatious; or (c) that Mr. Desjean's claim was an abuse of process.

solicit or market to Canada, has never attended trade shows or other promotional events in Canada; that it would, in fact, be manifestly unfair to subject Intermix to the jurisdiction of a Canadian court since it would mean that a company with no business assets in Canada and no physical presence in the jurisdiction could be sued in any country to which its products are downloaded. Accordingly he determined that "bearing in mind that the test to find a defendant has minimum contact must necessarily be more stringent when a foreign country is involved (as opposed to another state in the same country), I am unable to conclude that Intermix has minimum contact with Canada or with the subject-matter of the present claim.

The Federal Court decision was challenged in 2007[48] but the appeal was dismissed.

Conclusion

The Privacy Commissioner of Canada is tasked with overseeing compliance with both the *Privacy Act*[49] and the *Personal Information Protection and Electronic Documents Act.*[50] Although it seems most likely that a complaint dealing with cloud computing would come under PIPEDA, it is also possible that the Government of Canada might create a "private cloud" infrastructure internally to facilitate information sharing, or even that some or all government institutions might make use of a cloud infrastructure for data processing or storage.

Cloud computing is a general term for an emerging kind of infrastructure. At its most basic, it describes any system where information and/or applications are stored online, allowing access to be achieved by the user via any device.

The nature of cloud computing appears, on the surface, to create possible tensions between data protection/privacy agencies, ISPs and customers due to the uncertainty about which organization should be responsible in the case of privacy violations and how to hold companies who are located "in the cloud" responsible under Canadian legislation.

Should the Office of the Privacy Commissioner receive complaints about cloud computing, they are likely to arise from one of four situations:

- An organization choosing to use cloud infrastructure for data storage and/or processing;
- An organization or government body creating a private cloud infrastructure to facilitate information sharing within its environs;
- An individual user who interacts with a cloud application; or
- The misuse of data by a cloud infrastructure provider to whom it has been provided.

In the first case, it is likely that under PIPEDA such actions would be considered as a transfer for processing, and accordingly under Principle 4.1.3 of Schedule 1 the organization would be required to ensure that a comparable level of protection is provided for the information. The organization would remain in control of the information and responsible for meeting the PIPEDA requirements. The Office of the Privacy Commissioner has investigated such complaints before and done so effectively. It has also released guidelines for transborder data flow.

---

[48] (2007) FCA 365
[49] R.S.C. 1985, c. P-21
[50] S.C. 2000, c. 5

In the second, third and fourth situations, the provisions of the applicable legislation (PIPEDA or the Privacy Act) would apply to the subject matter of such a complaint.

Where the Privacy Commissioner has jurisdiction over the subject matter of the complaint but the complaint deals with cloud computing infrastructure and thus is not obviously located in Canada, current jurisprudence is clear that the Privacy Commissioner may exert jurisdiction when assessment indicates that a real and substantial connection to Canada exists.
Jurisprudence indicates that jurisdiction may be exerted over extra-territorial entities when a real and substantial connection to the jurisdiction may be established. This has been the case both when dealing with issues of inter-provincial and international jurisdictions, although a higher standard of connection may be required in international situations. Real and substantial connection, as a test, must be approached from the standpoint of principled flexibility, and although the jurisprudence sets out a number of factors that may be considered in making such an assessment, the list is not exhaustive and none of the factors are determinative in and of themselves – instead, the connection assessment must be conducted on a case by case basis.