Where in the World is My Data?
Jurisdictional Issues with Cloud Computing
March 30, 2011

C. Ian Kyer  
Counsel  
416 865 4396  
ikiyer@fasken.com

Gabriel M.A. Stern  
Associate  
416 865 5494  
gstern@fasken.com
Where in the World is My Data?

Jurisdictional Issues with Cloud Computing

1. Introduction

Cloud computing is considered by many to be a lower cost, efficient, easily accessible solution to data storage and retrieval. Storing your data in the “cloud” offers the promise of access irrespective of the location from which you are accessing it. Such universal accessibility, which is being promoted as a low-cost information management solution, is understandably appealing to both businesses and consumers alike. But does cloud computing come at the cost of legal certainty and predictability?

The term “cloud computing” is derived from the practice of IT professionals graphically representing the Internet as a cloud in their network diagrams. A useful formal definition of cloud computing is one provided in a 2008 Pew Internet Study: “an emerging architecture by which data and applications reside in cyberspace, allowing users to access them through any web connected device.” In other words, cloud computing is as a means of ensuring that your information is available to you anywhere you have internet access. The fundamental premise upon which cloud computing is based is that it does not matter where data is stored – what matters is that the data can be accessed anywhere. From a legal perspective, however, the distributed nature of cloud computing creates jurisdictional uncertainty – with information being stored and available “anywhere”, who has jurisdiction over it? Whose laws apply?

For many, jurisdictional risks appear to be the inevitable consequence of the very nature of cloud computing. As one commentator has noted, “A fundamental design premise in the cloud model is that, as a customer, your data will be stored across several, if not many, data centres of the cloud service provider.” This means that it may difficult at any particular point in time to know where your data actually resides, which regulators have jurisdiction and what regulations apply. Similarly, the Privacy Commissioner of Canada has noted that “By its very nature, cloud computing has the possibility of sending, storing and processing data in multiple jurisdictions” and has flagged the issue that “an ascendancy of the cloud model may even call into question the whole notion of data ‘ownership’ upon which much data protection is based”.

This jurisdictional uncertainty has caused some regulators to suggested implementing cloud computing systems creates unacceptable risks. The director of technology risk at the Monetary Authority of Singapore has stated that regulators are “unlikely to allow a bank to put customer data into the cloud without significant due diligence, pointing out that in Singapore such behaviour could be punished with a three year jail term and a hefty fine.” The Australian Prudential Regulatory Authority that regulates Australia’s financial sector has shown no enthusiasm for attempts by

---

1 Witness Microsoft’s recent consumer-focused advertising campaign encouraging computer users to get “to the cloud”. See http://www.microsoft.com/windows/cloud/.  
2 John B. Horrigan. Data Memo: Use of Cloud Computing Applications and Services (September 2008), Pew Internet & American Life Project, at pg. 1. Some have described cloud computing as simply another way of describing “software as a service”, that is, the idea that rather than having locally installed software applications software is run as a service over a network – see George Takach, “Risks of Cloud Computing – Part I” (November 11, 2010), http://mccarthy.ca/article_detail.aspx?id=5158. Yet this is too narrow a definition as the real promise of the cloud includes both run software as a service but also to provide a means whereby the same information can be accessed through different devices, including those with local software installed, from anywhere in the world.  
3 George Takach, “Risks of Cloud Computing: Part II” (November/December 2010), Lexpert at pg. 120.  
financial institutions to have their applications and data hosted outside Australia. Bruce McCabe, a research analyst at KPMG has been quoted as saying that “every large ASX100 company struggles with the regulatory aspects of cloud computing.” The finance sector, he said, is “the most sensitive” to the issue.

Potential users also have concerns. They worry that the distributed nature of cloud computing services could put their businesses and their data at risk because they could become subject to unfamiliar or unacceptable foreign laws. Many worry that using cloud computing providers located in the U.S. or who operate servers in the U.S. puts their data at risk of warrantless searches under the Patriot Act. This is even more a concern in those Canadian jurisdictions that impose an obligation on certain sectors to ensure that certain data is kept outside of the United States.

Lawyers point out that other questions and concerns may arise if cloud computing is used. If software development is conducted using the cloud, jurisdictional uncertainty may arise. Copyright regimes differ from country to country. The applicable law is determined by where the software is created. But if developers on a cloud computing project are scattered around the world, which copyright regime will apply?

In light of these concerns and the potential confusion we have sought to explain (a) how jurisdictional legal issues are addressed in Canada in the context of the Internet, and then (b) discussing when jurisdictional issues should actually be of concern to users and vendors of cloud computing services.

2. Jurisdiction and the Internet

2.1 Jurisdictional Misconceptions

When it comes to analyzing its jurisdictional aspects, cloud computing could not be better named. There is much cloudy thinking – much shade and little light. The first step to a clearer understanding of the issues is to understand that cloud computing is subject to the same legal rules as any other any service that operates over the Internet. Those rules are a combination of domestic law, foreign law and international law and convention. Cloud computing may operate in a world without boundaries, but commercial laws operate in a world where boundaries are of extreme importance.

To navigate this legal maze requires a good grasp of the conflict of laws principles that govern international transactions. Conflict of laws is central to cloud computing because the Internet, the very basis of the “cloud”, is multinational. While cloud computing and other e-commerce innovations are giving new prominence to this area of law, private international law is not a creation of cyberspace. It is a series of national rules and principles that have been developed over centuries to assist legislatures and courts in dealing with three questions that arise in transactions with one or more international or at least multi-jurisdictional elements. Which courts may take jurisdiction over the parties or the transaction? Which laws apply? When will the courts of one jurisdiction enforce a judgment rendered by the courts of another jurisdiction? Before trying to offer some guidance in answering these questions, there are four popular misconceptions that must first be addressed.

(a) Misconception #1: Choice of law clauses solve the jurisdictional dilemma

Many people believe incorrectly that the parties to a transaction may, through a choice of law clause, choose the laws that apply to their dealings with each other. They believe that parties may contract out of the application of local laws.


7 For example, the British Columbia Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165, which governs how personal information collected by public bodies in the province can be disclosed, provides at Section 33.1, that personal information held by public bodies can only be disclosed outside Canada in limited circumstances.
This is true only in a very limited sense. It is correct that many jurisdictions permit parties to an international or multi-jurisdictional contract to choose the laws that apply to their contract in the absence of overriding public policy. This means that the parties may choose the contract law of one jurisdiction to be applied to their contract. Contract law deals with such matters as the formation of the contract, its interpretation and enforcement including breach of the contract and the determination of any damages that might be suffered. The choice of law, however, does not mean that tort claims will be dealt with under that law or that intellectual property created by the parties will be assessed under that law or that consumer protection laws will be determined by that choice. These extra-contractual laws apply in situations where third parties are involved and are ones in which the state has an interest. The application of such laws either expressly or by implication cannot be contracted out of by the parties.

What this means is that not all legal relationships that result from offering or using cloud computing services can be controlled through a choice of law clause.

(b) Misconception #2: There are separate rules for determining jurisdiction in Cyberspace

To read some papers on jurisdiction and the Internet, one would think that the only cases and laws that one needs to consider are cases dealing expressly with the Internet or the “Cloud”. That is simply not true. There are some special laws that have been passed dealing with the Internet but the general rule is that this method of doing business is subject to the same general rules and principles as other business methods that have an international or multi-jurisdictional element to them. We need to consider the private international law rules and principles of each relevant jurisdiction and not just the cases that deal expressly with e-commerce or the Internet. While, as discussed in greater detail below, there have been key legal decisions concerning how e-commerce issues should be dealt with from a jurisdictional perspective, these cases are premised on the general legal foundations of private international law.

(c) Misconception #3: Jurisdiction for e-commerce is determined by where the server is located

Many business people think that the laws that apply to their e-commerce operations are determined by where they have their server. This may or may not be a relevant fact to be taken into account in determining jurisdiction. It depends upon the context. But even if this were true, cloud computing makes it difficult to determine definitively where the relevant servers are physically located. Because of the diminished important of the location of servers in terms of cloud computing, overcoming this misconception is essential, as we shall discuss in greater detail below.

(d) Misconception #4: There is a single set of rules to determine jurisdiction

This statement is false for three quite different reasons. First, despite the fact that we talk of private international law, there is not a single, applicable, international law. There is not even one set of rules and principles applied around the world. Perhaps the better term to use is conflict of laws because even the rules for dealing with conflicting laws are themselves in conflict. What we have are a series of national approaches to how to answer our three questions: which court has jurisdiction; which laws apply; where will judgment be enforced?

Second, there are countries like Canada that are multi-jurisdictional. Although the Canadian Supreme Court has laid down some national principles in cases like Morguard Investments v. De Savoye 8 ("Morguard Investments"), we do not have a single approach to conflict of laws across Canada.

Third, even in a single jurisdiction like Ontario, there are separate rules and principles that govern conflicts in contract, tort, consumer protection and the like.

2.2 Identifying and Managing Jurisdictional Risks

(e) Context - why does jurisdiction matter?

8 (1990), 76 DLR (4th) 256.
Context is everything in looking at jurisdiction and the Internet. What are the international elements in the case at hand and what is the question that we are seeking to answer? Are we asking if the court in the jurisdiction of the customer will take jurisdiction over a dispute between an online supplier of cloud computing services and a customer? Or are we asking whether the criminal laws of Oregon apply to a Russian website that allows you to store and play your music from anywhere around the globe? The answers may well be different but what we need to realize is that the process of determining the answers and the relevant factors in reaching the answer are also likely to be different. Because there is an absence of Canadian case law dealing expressly with cloud computing issues, the jurisdiction question must be reviewed through the lens of existing jurisprudence on e-commerce and the Internet.

(f) When will jurisdiction be taken? What are the implications?

This is a simple question to ask but a very complex one to answer. Generally courts will take jurisdiction if there is a "real and substantial connection" between the jurisdiction and either the people involved or the subject matter of the dispute. The courts will take jurisdiction over people resident or domiciled in their jurisdiction (or ones who have voluntarily submitted or attorned to the jurisdiction) as well as over property situate in their jurisdiction. They may also take jurisdiction where an accident occurred or damages were suffered in the jurisdiction. To get an idea of the breadth of this jurisdictional reach look at the rules for service out of your jurisdiction. This suggests that no matter where information might be stored in the "cloud", to the extent cloud computing services are consumed somewhere, there is a risk that the courts could claim jurisdiction based on the location of the consumer/customer.

When foreign corporate defendants are involved in questions of jurisdiction, the question often centres on whether the defendant is carrying on business in the jurisdiction or, to use an American expression, availing itself of the jurisdiction. It is this question that has been looked at in a number of U.S. decisions involving e-commerce and the Internet. Does simple use of the Internet constitute submission to each jurisdiction where access is possible or are more active exchanges with users in the jurisdiction necessary?

Consider, for example, the case of Desjean v. Intermix Media Inc.11 ("Intermix"). In this case, a statement of claim for a proposed class action was made in the Federal Court against a Delaware corporation (Intermix Media Inc.) for allegedly violating the Competition Act. It was claimed that Intermix Media Inc bundled extra "spyware" or "adware" software with free software that it made available. The Federal Court refused to take jurisdiction after applying the real and substantial connection test. The court reasoned that, although a plaintiff located in Canada may allegedly have been harmed by Intermix Media Inc., there was "no connection between the forum and the defendant" as the company had no servers in Canada, had no business presence in Canada and had "no advertising, marketing or solicitation aimed at the Canadian market".

Particularly interesting in Intermix is the court’s characterisation of the services offered by the defendant:

The record in the present case does not allow me to come to the conclusion that the Web sites Intermix operates are interactive in nature. These Web sites do not allow users to communicate and exchange information with the sponsors of the site, or to order products online. But even if they could be characterized in such a way, I do not think Intermix could be found to have the level of

---

9 After the courts are satisfied that they can take jurisdiction they are sometimes asked to consider whether they should do so. This question is often dealt with under the rules of forum non conveniens.

10 For reference, see an excellent paper by Prof. Michael Geist entitled “Is There A There There? Toward Greater Certainty For Internet Jurisdiction” which sets out the various approaches the courts have taken in answering this question. Available on-line at www.law.berkeley.edu/journals/btlj/articles/16_3/geist/geist.pdf.


12 The decision was subsequently appealed but the appeal was rejected. See (2007) FCA 365.

13 Intermix at para. 29.

14 Intermix at para. 34
interactivity with Canada that could justify a finding of minimum contact. The software that can be downloaded from Intermix’ Web sites is free, there has been no targeting of Canada or of Canadian consumers in any specific way, there is no specific content for a Canadian audience, and Intermix has never purposely availed itself of Canada's laws. 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.15

This reasoning mirrors that in an earlier Ontario case, Pro-C Ltd. v. Computer City, Inc.16 (“Pro-C”), identified two specific elements for the test for determining whether the courts will exercise jurisdiction over a website:

(a) the nature and quality of commercial activity on the site, with “[a]t one end of the spectrum ... situations where a defendant clearly does business over the Internet”, with, at the other end, “a passive website that does little more than make information available to those who are interested in it”;17 and

(b) the extent to which the hosting organization has knowledge that they are making sale to residents on a particular foreign jurisdiction.

What Intermix and Pro-C therefore suggest is that the degree to which a service is targeted at Canadians will have a strong impact on whether Canadian courts will claim jurisdiction over cases in respect of same. Query however how strong that focus needs to be. Important to the court in Intermix was the fact that the website that offered the software at issue for download did not reach out to Canadians. Contrast this with a website that collects customer information prior to permitting use of a service and which lists “Canada” as one of the options customers can select. In such a case, the courts may find it more likely that there is a real and substantial connection to Canada as there was a conscious focus on Canada.18 The lesson here is that the actual way in which a cloud computing service is designed and advertise can actually have a significant impact on what jurisdiction might apply.

Additionally, specialised administrative tribunals have also been found to be able to claim jurisdiction over the activities of on-line service providers even if they have no physical presence where the services are being received. One of the most compelling examples of this risk is illustrated by the Canadian privacy law regime, as it has been determined that the Canadian federal privacy law regime can apply to non-Canadian organizations carrying on business in Canada, even if they do not have a physical presence in the country. This point was explicitly made in 2007 when the Federal Court confirmed that the Federal Privacy Commissioner had jurisdiction to investigate cross-boarder flows of personal information, even when the organization it was investigating was not located in Canada and where enforcement might be difficult.19

Understanding therefore that breaches of local laws can pose risks in respect of cloud computing, cloud computing service providers and customers must understand that compliance with local laws presents risk because of the numerous issues involved. For example, in 2010 the Alberta Personal Information Protection Act was amended to require that certain notifications must be made when there are breaches of organizations’ privacy obligations.

15 Intermix at para. 42.
16 1999 CanLII 14926.
17 Pro-C at para. 110.
18 Consider, however, whether this decision might be wrong from an IT perspective. For example, many U.S.-based websites that make media available for viewing (e.g. Hulu) block Canadian IP addresses from accessing the media on the site. As such, given that there are (admittedly not perfect) technological measures service providers can use to lock out certain users, then by not implementing such measures, then one could argue service providers who do not are effectively reaching out to all users, regardless of jurisdiction.
Similarly, amendments were proposed to the equivalent federal *Personal Information Protection and Electronic Documents Act*. Because of the nature of Canadian privacy law, providers of cloud computing to Canadians could find themselves subject to both the Alberta and the federal privacy laws. While the breach notification regimes may seem similar, there are numerous subtle differences in terms of (a) the threshold for reporting a breach, (b) the threshold for notifying the affected to individuals, (c) the definition of “significant harm”, (d) the responsibility for notification, and (e) offences. Irrespective of the particulars, however, because multiple jurisdictions might attempt to claim jurisdiction, and these jurisdictions might have significant difference between them, it may be difficult to identify common strategies for managing the risk posed by those jurisdiction where it is believed jurisdiction might be claimed. One method may be to review the jurisdictions within which a service is being offered and attempt to identify a “highest standard” of behaviour so that company policies and practices comply with the strictest obligations across jurisdictions.20

(c) When will courts enforce a foreign judgment?

The B.C. Court of Appeal decision in *Braintech v. Kostiuk*21 (“*Braintech*”) gives us some idea of when the courts will enforce the judgment of another jurisdiction. Kostiuk was alleged to have used the Internet to transmit and publish defamatory information about BrainTech. Braintech obtained a default judgment in a District Court in Texas against Kostiuk and then commenced an action on this judgment in the Supreme Court of British Columbia. After a summary trial Braintech obtained a favourable judgment which was appealed. One of the issues in that appeal was whether there was a real and substantial connection between Texas and the parties or the defamation alleged to have taken place in that state.

Kostiuk in his statement of defence denied service in the Texas action; denied any connection with Texas; denied he had attended to the jurisdiction and alleged fraud on the Texas court. He sought a declaration that the Texas court acted without jurisdiction and an order dismissing Braintech’s claim.

In Texas, a non-resident does business in the state if the non-resident: (1) contracts by mail or otherwise with a Texas resident and either party is to perform the contract in whole or in part in this state; (2) commits a tort in whole or in part in this state; or (3) recruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state. Braintech was not a Texas corporation and did not have operations in Texas. It was alleged, however, that the tort was committed there.

The B.C. appeal court stated: “It is apparent the “real and substantial connection” relied upon for the assumption of jurisdiction by the Texas court is the alleged publication there of a libel which affected the interests of resident present and potential investors. This is true only if the mode of communication through the Internet supports this conclusion. …In the circumstance of no purposeful commercial activity alleged on the part of Kostiuk and the equally material absence of any person in that jurisdiction having “read” the alleged libel all that has been deemed to have been demonstrated was Kostiuk’s passive use of an out of state electronic bulletin. The allegation of publication fails as it rests on the mere transitory, passive presence in cyberspace of the alleged defamatory material. Such a contact does not constitute a real and substantial presence. On the American authorities this is an insufficient basis for the exercise of an in personam jurisdiction over a non-resident.”22

Although the case is one in which enforcement was refused in B.C., it is interesting to note that the Texas Court took jurisdiction even though the link to that State was tenuous. It is also worth noting that had there been a real and substantial connection with Texas, under Canada’s *Morguard Investments* rule that provides for deference for foreign judgments, the B.C. court would have enforced the judgment of the Texas Court.

20 This lesson also applies for dealing with other consumer-focused local laws, such as general consumer protection law. Per *Intercity and Pro-C*, the degree of targeting of a service to a particular jurisdiction may be sufficient to subject a service to the laws of that jurisdiction.
22 *Braintech* at para. 58 and 65.
Another case that dealt with the question of enforcing foreign judgements as a result of e-commerce activities was *Disney Enterprises Inc. v. Click Enterprises Inc.*²³ ("*Disney*"). In this case, an Ontario court was being asked to enforce a judgment awarded in New York State against an Ontario corporation. The Ontario corporation, Click Enterprises Inc., offered consumers tools and services to assist in downloading copyrighted films online. When Disney appeared before the Ontario Superior Court of Justice to seek to enforce this judgement, the question the court had to address was whether the foreign (i.e. U.S.) court properly exercised jurisdiction against a foreign-to-it (i.e. Ontario) corporation such that a court in the corporation’s home jurisdiction would enforce the judgment against the corporation. In order to answer this question, the court looked to the real and substantial connection test and found that a real and substantial connection did exist and that the judgment could be enforced. Indeed, the court in *Disney* distinguished the facts in the case from *Braintech*, stating that while in *Braintech v. Kostiuk* the defendant only passively posted on an Internet bulletin board and had no commercial purpose. In *Disney*, Click Enterprises Inc. “had a commercial purpose that utilized the Internet to enter the United States to carry out its activities.”²⁴ In short New York was found to be an appropriate jurisdiction for the original claim as the defendants “had continuous and ongoing business contacts with residents of New York through their interactive websites, which were targeted at residents of this state”.

(d) Risk management through contract?

As has been discussed, the nature of a cloud computing service will have a strong impact on what jurisdictional law might apply. As a result, operators of cloud computing sites might be able to control their jurisdictional risks to a certain degree by preventing customers in certain jurisdictions from accessing the services. What other measures might providers use to mitigate jurisdictional risks? One method, touched upon in the myths discussed above, is through contractual measures. This might not help protect against all risks, but it can mitigate some.

In crude terms, cloud computing is akin to a distributed hosting service. Although it is said that location does not matter, the servers used reside somewhere and are controlled by a service provider that resides somewhere. Those locations will affect what jurisdiction’s laws apply and what jurisdictional risks it will face. Consider the recent experience of WikiLeaks. In late 2010, the controversial website that discloses confidential US government information moved the hosting of its sites to a European provider once the U.S. company Amazon decided to stop hosting the site. This shift has been cited as an example of the benefits of cloud computing – that data at risk in one location can quickly be shifted to somewhere else.²⁶ Yet WikiLeaks’ experience very clearly illustrates that perhaps the key risk factor to consider when evaluating where cloud computing risks might be located from a jurisdictional perspective is the location where the service provider resides. Amazon’s servers that hosted WikiLeaks could very well have been (and were likely) located around the world. But because of U.S. political and legal concerns, the U.S.-based Amazon took action against one of its customers.

The WikiLeaks example appears to be a clear cut example of how when operating in a cloud computing environment, one needs to be sensitive to jurisdictional legal issues. But what if the parties in a cloud computing relationship were more equal? Say instead of WikiLeaks obtaining what were likely off-the-rack hosting services from Amazon, a major Canadian bank were to negotiate with Microsoft for the provision of a custom cloud computing environment that allowed the bank’s employees to access and edit all of their work documents from any Internet equipped web browser. In such a situation, the bank would likely want Microsoft to provide certain representations and warranties in respect of the data it will be hosting for the bank. For example, the bank might ask for a presentation and warranty regarding the security of the data. In this case, even though the service in question is a cloud computing environment, if there were problems with the system, the bank would have a contractual recourse against Microsoft. While, as stated above, a choice of law clause is not always a panacea, here two sophisticated parties would have a choice of

²⁴ *Disney* at para. 25-26.
²⁵ *Disney* at para. 30.
²⁶ See, for example, Michael Geist, “Canada can be global leader in cloud computing” (December 5, 2010), *Toronto Star* at pg. A15.
law designed in such a way as to best ensure the enforceability of their bargain. Additionally, because the party that has been harmed through a breach of the agreement would not worry about the jurisdictional issue of where to sue but would likely begin action in the jurisdiction where the breaching party is located (subject of course to choice of law clause).

Of course, as stated above, public policy reasons can often be a reason for choosing not to enforce a choice of law clause. As such, a consumer entering into an agreement to use a cloud computing service offered by Microsoft might have a better chance of creating a jurisdictional risk for Microsoft. Similarly, there would still be significant exposure in terms of jurisdictional risk to the extent that what was in dispute was not whether the terms of a contract have been fulfilled but whether local law has been breached – and as noted above, the application of local laws that result from broad visions of jurisdiction may present the most real risk in terms of cloud computing.

Another option available to sophisticated commercial parties in order to limit cloud computing risks is to ensure that their contracts with IT services vendors limit the scope of subcontracting the vendor can do. This can be done by including in a contract, for example, by included a list of prohibited subcontractors, by requiring that the customer has to approve in writing all subcontractors, or by limiting subcontracting to a discrete list of pre-approved subcontractors. The advantage of limiting subcontracting from the customer’s perspective is that to the extent certain subcontractors are known to operate or use servers in jurisdictions of concern, then the customer has a certain degree of control over data flows in the cloud. Similarly, a customer could negotiate for a negative covenant from the service provider whereby the service provider would agree to not use servers located in particular countries of concern.

Finally, one last cloud computing risk to consider is the risk that in contracting for a cloud computing service, the mere presence of data on a server in country A might be seen to give country A the right to claim jurisdiction over a customer whose data is hosted on that server even if the customer is in no way otherwise carrying on business in country A. It is debatable the degree to which this is an actual concern; on the one hand, such claims of jurisdiction might be seen as unlikely since the presence of data without further activity might not be thought to create a real and substantial connection with that jurisdiction since while there is a “real” connection in the sense that an asset of the company, its data, is physically located in country A, the passive nature of the customer’s relationship with country A may not be seen as “substantial”. However, the fact that data is actually located in a country might alone be seen as both a real and substantial enough connection to establish jurisdiction. Regardless of how real one considers this risk to be, the risk is augmented for customers who need to ensure as a legal or practical matter that their data is or is not in a particular jurisdiction. Consequently, customers may try to address this concern through contractual means by negotiating in their service contract for either a positive or negative covenant with respect to the countries where data may or may not, as the case may be, be hosted from.

3. Conclusions

Because of the nature of cloud computing systems, certain jurisdictional risks will be unavoidable. To the extent that cloud computing services are contracted for between sophisticated commercial parties, the risks involved in cloud computing may be low given that through negotiation the parties may be able to limit the parameters of liability between themselves. The aggrieved party will be able to sue the breaching entity wherever the contracting entity is located, no matter where in the cloud the breach happened. Such certainty of risk avoidance decreases however to the extent cloud computing services are offered to consumer users, as such parties might appeal to the public policy sympathy of the courts. Moreover consumers might be protected by local laws, such as privacy and other consumer protection laws. And the courts, at least in Canada, have shown a willingness to claim jurisdiction over cases involving e-commerce. While cloud computing must navigate the same governed by the same international law morass as any activities that span jurisdictions, the inherently distributed nature of cloud computing services, it is important to understand how these legal principles can create, and be used to manage, risk.