

Legal Cloud Computing: Concepts and Ramifications



April 27, 2010

Sébastien Lapointe, *Holmested & Associés s.e.n.c.*

Legal Aspects of Cloud Computing

- Normal businesses using *cloud computing* (“**CC**”) face a slew of practical and legal difficulties
 - e.g. Issues relating to controlling the data so hosted
 - e.g. Security and privacy issues
 - e.g. Evidenciary issues (eDiscovery)
 - e.g. Cloud standards
 - e.g. Regulatory compliance (e.g. *Sarbanes-Oxley Act*)
 - e.g. Document retention and persistent data integrity
 - etc.
- Law practitioners even more so, including because of privileged nature of information and the need for confidentiality – further complicates things

Typical Actors

- **F.** : **Firm** (a law firm using CC in our example)
- **P.** : **Provider** (the cloud infrastructure service provider)
- **User** : Individual **end-user** of CC services
- **C.** : **Client** (a client of our example law firm)

Structure of this Presentation

- Factual Problems with CC
- Legal Issues with CC
 - Applicable Law
 - Personal Information and Privacy
 - Security & Unlawful Access
 - Lawful Access & eDiscovery
 - Data Portability & Availability
 - Contracting Issues

Factual Problems

Factual Problems

CC implies several problems in practice:

- **Cloud Neutrality (the illusion of):** Users assume changing the location of processing or storage doesn't change anything about how the data is used – but it does (e.g. where, by whom, etc.)

Factual Problems (cont.)

- **Control and Power over Data:** CC implies a loss/lack of control and expertise over the technology infrastructure and F.'s & C.'s data

e.g. Kindle library and tampering with ebooks

e.g. DRM servers going offline

Factual Problems (cont.)

- **Use of Data:** CC implies delivering data to P. on on-going basis which coupled with control factually allows all sorts of ways to use it.

e.g. P. can monitor every keystroke and operation

e.g. P. could datamine its CC data (F.'s data or secondary data)

e.g. P. could profile users for targetted advertising

e.g. P. could use information on its servers, etc.

e.g. P. could try and use or commoditize the data its holds

Factual Problems (cont.)

- **Ownership of Data:**

- Agreement usually clear that F.'s data is F.'s
- In practice things are more complicated, as use of CC generates new data (*secondary data*) that P. may consider his unless you agree otherwise
- Issue may crop-up in bankruptcy proceedings of P.

- **Location:** CC often implies an “export” of data to another jurisdiction (e.g. U.S.) and F. may not even know which (P. may itself deal with a P.)

Legal Issues

(Especially relevant to law practitioners using CC, on top of ethical issues)

No CC specific statute... yet (U.S.
is considering it)

But common law and existing
legislation **can and do** apply...

Legal Issues

- Applicable Law
- Personal Information and Privacy
- Security & Unlawful Access
- Lawful Access & eDiscovery
- Data Portability & Availability
- Contracting Issues

Legal Issue 1: **Applicable Law**

Applicable Law

- CC often makes it difficult to determine what the law of the arrangement is or what territories can exert jurisdiction on that data or its use
- With different geographic locations of F., P., servers and Users what is the applicable law?
All of them may apply
- Transborder dataflow may trigger legal obligations in multiple jurisdictions (or may even be a problem as the initial export may be a problem (e.g. *EU Data Protection Directive 95/46/EC*)

Applicable Law (cont.)

- Lawyers that place information and data in the clouds have to be aware of legislation that may be relevant to *situs* of that data or where F. and P. are operating
- Problem is this may be anywhere, unless care is taken to limit what P. can do with the data (where it will be stored) and how services are provided
- This assumes P. can even know which countries data will be exported to (ask!)

Legal Issue 2: **Personal Information & Privacy**

Personal Information & Privacy

- Legislation implemented to protect the privacy of individuals in the private sector (collection, use and disclosure of personal information in the course of commercial activities)
- Examples of legislation:
 - Canadian legislation (PIPEDA) - applies in the absence of "Substantially similar" provincial legislation
 - Provincial legislation (BC, Alberta, Quebec)
 - EU Directive 95/46/EC
 - etc.
- “**Personal information**” (“**PI**”) means information about an identifiable individual (but generally not the name, title or business address or telephone number at work).

Personal Information & Privacy

- Legislation from a given jurisdiction may apply if there is a real and “substantial connection” (P., F., servers, etc.)
- Applicable Canadian privacy legislation will apply if F. is operating in Canada, etc.
- Home legislation may prevent F. from using CC because it would entail « exporting » data across borders (e.g. Europe) though not Canada

Personal Information Protection and Electronic Documents Act
(PIPEDA)

- Organization is responsible for PI *under its control* **including information that has been transferred to third party for processing** (Principle 4.1)
- PI must be protected by security safeguards **appropriate to the sensitivity of the information** against loss, theft, unauthorized access, disclosure, copying, use, or modification (Principle s.4.7)
- Exception for data transfers – yes, but must use **contractual (or other) means** to provide a comparable level of protection while the information is being processed by a third party

PIPEDA (cont.)

- Transfer for processing is “**use**” (but normally not seem as “disclosure” per se)
- Must implement **policies and practices** to give effect to PIPEDA, including implementing procedures to protect PI
- Must use **contractual means** to provide a comparable level of protection while the information is being hosted or processed by P., including if outside Canada
- Sending PI outside Canada also requires **advising customers that PI may be sent to another jurisdiction** for processing which may make it accessible by the courts, law enforcement and national security authorities

(cf. Guidelines for Processing Personal Data Across Borders)

PIPEDA (cont.)

In practice:

- **Contractual arrangement** (with P.) is paramount to make sure hosting data with P. will result in a comparable level of PI security
- Must limit use, disclosure and retention by P. just **as if data was held by F.** (the agreement between F. and P. must allow this)
- Can NOT simply hope that P. will play fair and not misuse or permanently delete every piece of data after
- The methods of protection at P. should include:
 - (a) physical measures (restricted access to offices and servers)
 - (b) organizational measures (on-site security clearances and limiting access on a “need-to-know” basis), and
 - (c) technological measures (use of passwords and encryption)

Québec's *Private Sector Privacy Act*

(An Act respecting the protection of personal information in the private sector)

- Dates back to '90s when CC was not around
- Judged “*substantially similar*” to PIPEDA
- Also:
 - Requires consent to handle PI
 - Requires appropriate security measures (s. 10)
 - Prohibition against communicating PI to third parties without consent of the individual (s. 13)
- Plus requires taking all reasonable means (best efforts?) if PI is sent outside Province of Québec to ensure that P. will not use PI for any other purposes (other than the one the individual agreed to) (s. 17)

Québec's *Private Sector Privacy Act* (cont.)

- Exception in s. 20 may allow a business to send PI to a P. under a CC contractual arrangement

20. In the carrying on of an enterprise, authorized employees, mandataries or agents or any party to a contract for work or services may have access to personal information without the consent of the person concerned only if the information is needed for the performance of their duties or the carrying out of their mandates or contracts.

Legal Issue 3: **Security & Unlawful Access**

Security & Unlawful Access

- CC gives extraordinary control to P. and ability monitor data (hosting) and exchange of data (dataflow)
- Misuse of data may be done lawfully or unlawfully: May involve hackers or simply P. itself (i.e. misuse of data by P. or its personnel)
- F. may never know - P. really controls the server(s) – duty to disclose breaches?
- Lawyers must take steps to mitigate these inherent problems of security
- Security issues to consider involve possible **intrusion and misuse** (of course) but also **backup** and **recovery** of data if there is a problem with the server(s) - in practice, will P. do this, to what extent, how, etc.)

Security & Unlawful Access (cont.)

- Recent reports seem to indicate many P. do not put a premium on security: Non-existent or insufficient **encryption** (often seen as slowing down CC application, systems and user exp.)
- May be a problem both regarding:
 - Communication - Data streams (sent through IP protocol – may be intercepted in transit); and
 - Storage - Data actually located on P.'s servers susceptible to intrusion, theft, etc.
- Most P. not using encryption to the level that financial institutions are, this creates risk

Security & Unlawful Access (cont.)

- Issue both about securing the data:
 - DURING the term; AND
 - AFTER C. has ceased using the services (i.e. Does P. have the obligation to erase permanently every bit of data relating to F.?)
 - AFTER P. has been involved in bankruptcy or insolvency proceedings (ownership of data may become relevant, but what data?)

Security & Unlawful Access (cont.)

- Businesses will generally have a duty to secure their client's data (e.g. privacy)
- Lawyers must further contend with **ethical** requirements to preserve privileged information
- Common law and statutory requirements are increasing as to the need for any business to adopt "**reasonable security**" (e.g. *Negligence*)
- More and more litigation (like *EMI v. Comerica* in the U.S.) and regulatory enforcement proceedings around the issue of what constitutes "reasonable security"

Examples of legislative requirements as to security: *Québec's Legal framework for information technology Act*

Generally is favorable to CC-type situations but with caveat. Example provisions:

25. The person responsible for access to a technology-based document containing confidential information must take **appropriate security measures** to protect its confidentiality, such as controlling access to the document by means of a restricted view technique, or any technique that prevents unauthorized persons from accessing such information or from otherwise accessing the document or the components providing access to the document.
26. Anyone who places a technology-based document in the custody of a service provider is required to **inform the service provider beforehand as to the privacy protection required** by the document according to the confidentiality of the information it contains, and as to the persons who are authorized to access the document. (...) the service provider is **required to see to it that the agreed technological means are in place to ensure its security and maintain its integrity and, if applicable, protect its confidentiality and prevent accessing** by unauthorized persons. Similarly, the service provider must ensure compliance with any other obligation provided for by law as regards the retention of the document.

Generally confirms the need for contractual and other means of protecting the information contained in the data sent to P.

Legal Issue 4: Lawful Access & eDiscovery

Lawful Access & eDiscovery

- Related to the issues of confidentiality and security
- Possible issue with **lawful access** requests (or **search and seizure** powers) by law enforcement, either against P. or one of its clients
- Can also think of the problem of eventual **seizure or discovery** of evidence by third parties against P. (or some other of its clients)
- All may result in the disclosure of F.'s information or data
- Disclosure may go beyond what's normally allowed by lawful access legislation (remember P. controls all of the data)
- F. may not even be aware of the lawful access request or the seizure, nor be in a position to try and control what is being disclosed
- May happen in every jurisdiction where:
 - P. has offices
 - P. is operating or involved with CC services (e.g. US *Patriot Act*, etc.)
 - P. has equipment
 - P. has clients
 - F. is located

Legal Issue 5: Data Portability & Availability

Data Portability & Availability

- Most P. do not put a premium on ensuring that F. will have easy access to its data to get it out of P.'s hands upon termination (agreement often limited to saying « Yes, it's your data »)
- Often no right for F. to data export tools or fonctionnalités
- APIs are often implemented in a manner that does not make them interoperable
- F. may not even know what format or standard P. is using concerning F.'s data
- F. may thus not be able to easily get its data from P. at the end of its agreement
- As a F. organisation (e.g. lawfirm) relies more and more on a CC, this will become more and more important as F. will feel (and be) more and more locked-in
- Should try and address this issue expressly in the agreement
- Even if mentioned in the agreement, may be a problem in case of bankruptcy of P.

Data Portability & Availability (cont.)

From the start, F. should think about:

- How critical CC service is to its business?
- What is the standard of availability or reliability to which P. will be held?
- After termination, can another vendor provide that software (or an equivalent) and host that data?
- If so, will data have to be converted to a different format? How? What are P.'s obligations?
- Will be especially crucial if P. has right to terminate for convenience

Legal Issue 6: **Contracting Issues**

Contracting Issues

- Beware: **No standards** as to what P. offers or will accept in terms of obligations
- A proper agreement is the **only way** to neutralize legal problems related to CC
- Can mitigate:
 - problems relating to security and duty of care regarding data
 - factual problems with P.

Contracting Issues (cont.)

Useful Analogies

- May be useful to start thinking about the kinds of issues that CC may raise in practice and eventual problems the contract between F. and P. should address
 - e.g. The office rental business (vs. owning your space)
 - e.g. Public utilities
 - e.g. Allowing a neighbor to keep your family's cookie jar

Example: The *Cookie Jar* Analogy

Some problems you may run into:

- Paul may be tempted to grab cookies from the jar
- Paul may be unable to prevent his kids (or other kids) from grabbing cookies from the jar
- Paul may lock the door to his kitchen at night or when he leaves
- Your cookies may end-up mixed with other neighbors (if Paul starts hosting several families' cookie jars in his kitchen)
- Paul may not keep the jar as accessible or as clean as you would were it still in your kitchen
- Paul may not buy the right kinds or brands of cookies your family likes after a while
- Paul may fail to replenish the cookies in the jar
- After a while, who do the cookies legally belong to?
- etc.

Contracting Issues (cont.)

- **Standard form** contracts endemic to CC
- Often try and impose a very **low standard** on P.
- Often: “**As-is**” exclusions of warranties (i.e. services/goods provided as they are without any promise of being suitable or attaining a certain level of performance)
- P. may be reluctant to negotiate as heavier obligations may be seen as incompatible with the cheap pricing model for CC

Contracting Issues (cont.)

- If the CC services are business critical, F. will need to challenge the default P. positions contained in its standard-form contract
- May be easier to comply with legal requirements depending if the service is intended for the public (usually relies on one-sided clickwrap agreements) or for actual businesses

Contracting Issues (cont.)

Risks that a proper CC services contract may try and alleviate:

- Service availability and reliability
- Data security
- Breach response
- Enforcement rights
- Indemnification
- Data portability

Contracting Issues (cont.)

Performance standard can be crucial:

- Should state contractual obligations of P. regarding uptime and availability – get a warranty (even if the remedy is limited by the contract)
- Define **service “availability”** and reliability
- **Describe “quality of service”** (QoS) requirements
- **Include “Service Level Agreement”** (SLA)
 - How availability is calculated (duration vs. number of interruptions)
 - May F. challenge or audit P.’s calculations?
 - The remedy will usually be a credit (against service fees), but may or may not be the exclusive remedy F. is entitled to
 - Often exist but backed by weak standards of obligations
- **The Devil is the details...**

Contracting Issues (cont.)

Agreement with P. should also include provisions regarding:

- Where the F.'s data is going to be stored (what jurisdiction)
- Demonstrable storage **security** and appropriate specific security measures for F.'s data during the agreement that meet Canadian legislative requirements (cf. Privacy)
- What **backup** facilities will be used and how (will services be supported by disaster recovery plans?)
- **Data ownership** and specifically address the issues of new datastreams (data that is uploaded to the CC infrastructure) and secondary data that is generated by interactions with P.'s infrastructure;
- **Data portability** obligations of P. at the end (does it have to do anything?)
- **Copies of F.'s data will be removed** permanently from P.'s infrastructure after termination, and within what time period this will be done;

Contracting Issues (cont.)

BEWARE of typical default CC agreements:

- Service level agreement (**SLA**) terms should be reviewed carefully (may not give you much)
- Drastic **limitations of liability** provisions (often set a limit that is out of proportion to the amount of potential damages) (e.g. return of fees paid – if that)
- Beware of **exclusions of liability** for service interruptions, system failures, etc.
- **Remedies may be limited** (consequential damages usually excluded and often deemed the exclusive recourse of F. in case of problem)

CONCLUSION

- CC is here to stay (too good to pass on)
- Lawyers should beware of the practical pitfalls of CC
- Also beware of legal issues
- Get some control to protect your cookie jar (and your clients' cookies)
- Terms of the service agreement with P. are crucial and should be negotiated

QUESTIONS?

Thank you!

Sebastien Lapointe
slapointe@holmested.ca