The Dirty Dozen – 12 Contentious Things About Cloud Computing Deals
















Bernice Karn

September 23, 2014

CASSELS BROCK
LAWYERS

What's So Great About the Cloud?

- Cloud Computing Dynamics
  - GREAT BECAUSE:
    - It's cheap
    - It's simple
    - It's flexible and scalable
  - NOT SO GREAT BECAUSE:
    - Customer loses control/oversight
    - Customer becomes dependent on third parties and loses practical ability to bring back in house
    - Local laws could prove to be an impediment

Doing the Negotiation Dance

- The Procurement Process
  - Sophisticated customers may issue RFPs or conduct multiple track negotiations
  - Less sophisticated customers may be talked into something by slick salespeople
  - In most cases, legal review is brought in at the end, once both sides are invested in the deal

Doing the Negotiation Dance

- Lines I am tired of hearing:
  - “We operate on a single line of code”
  - “Our customers don’t worry about these things”
  - “Nobody has ever asked for that before”
  - “We can’t agree to that”

Doing the Negotiation Dance

- Lines I would prefer to hear:
  - “The service is cheap because we don’t make special accommodations for anyone – it’s volume based”
  - “You’re just going to have to trust us”
  - “You’re making this negotiation difficult because you are asking hard questions we don’t like to answer”
  - “We won’t agree to that because we would have to buy extra insurance to cover the risk and that would drive up our costs”

What Are The Dirty Dozen?

- 12 Fundamental Issues for Customers
  - Scope of Services
  - Service Level Commitments
  - Privacy and Confidentiality
  - Securities and Other Compliance Issues
  - Disaster Recovery
  - Record Keeping
  - Inspection and Audit Rights
  - Subcontractors
  - Default and Termination

What Are The Dirty Dozen?

- Limits of Liability
- Indemnities
- Transition Issues

Scope of Services

- Needs to be clear
- Client needs to understand what it is getting and what it is not getting
- OSFI B-10 – Applies to federally regulated financial institutions – includes banks, trust and loan companies, insurance companies
- OSFI guidance has stated that material cloud deals are subject to the B-10 guideline
- OSFI B-10 requires that the following be addressed:
  - Frequency, content, format of services
  - Location of services

Service Level Commitments

- Availability – Savvy customers will want this to be meaningful
- Responsiveness of the solution
- Resolution of problems – timeliness critical
- Sunsetting – special arrangements here likely run counter to the cloud financial model; however, clients need to be comfortable with functionality
- Return of data – Needs to be quick, easy, in a standard format, seamless, at a reasonable cost and data need to be accurate

Privacy and Confidentiality

- Confidential Information
  - Financial statements
  - Trade secrets
- Personal information - Customers and employees
  - Various laws can apply, for example:
    - PIPEDA, PHIPA, PIPA, Quebec privacy legislation
    - FIPPA, MFIPPA
    - EU Directive 95/46/EC
    - Anti-spam legislation

Privacy and Confidentiality

- ***Personal Information Protection and Electronic Documents Act*** (Canada) - Principle 7 (Safeguards)
- ***Personal Information Protection Act*** (Alberta) s. 13.1, s. 34.1(1) and ***Personal Information Protection Act Regulation*** s. 19, s. 19.1
- ***Personal Health Information Protection Act, 2004*** (Ontario) s. 12(2) and s. 50(1)
- ***An act respecting the protection of personal information in the private sector*** s. 17 (Quebec)
- **Canada's new anti-spam legislation** (CASL)

Privacy and Confidentiality

- Privacy legislation generally requires that the data collector ensure that organizational, physical and technological measures appropriate to the sensitivity of the information are used to safeguard the information
- OSFI B-10 also requires that data be segregated
- Alberta's *Personal Information Protection Act* has special notification provisions when a foreign service provider is used to collect personal information from Albertans and has breach notification requirements
- Quebec's private sector privacy legislation requires that, when "communicating" personal information outside the province - the recipient cannot use for new purposes

Securities and Other Compliance Issues

- *National Instrument 52-109*
  - Form 52-109F – requires attestation by an officer of an issuer
  - Based on knowledge, having exercised reasonable diligence, that the annual financial statements together with the other financial information included in the annual filings fairly present in all material respects the financial condition, results of operations and cash flows of the issuer, as of the date of and for the periods presented in the annual filings

Securities and Other Compliance Issues

- *Sarbanes-Oxley Act of 2002*
  - Requires quarterly certification of integrity of financial statements
  - Issuers must establish, maintain and evaluate the effectiveness of internal controls
  - Mandates document retention periods
  - Intentional alteration, destruction, mutilation, concealing, cover up, falsification of documents; intentional certification that financial statements fairly present, in all material respects, the financial condition and results of operations of the issuer (when in fact they do not) – significant fines and jail time for directors and officers

Securities and Other Compliance Issues

- **Software** (*Export and Import Permits Act*, R.S.C. 1985, c. E-19, s. 3(1))
  - **Export Control List** (SOR/89-202)
  - **General Export Permit No. 46 — Cryptography for Use by Certain Consignees** (SOR/2013-1)
- **Duties of directors, liability under corporate statutes** (*Business Corporations Act*, R.S.O. 1990, Chapter B.16, s. 134; *Canada Business Corporations Act*, R.S.C., 1985, c. C-44, s. 122);

Disaster Recovery/Business Continuity

- OSFI B-10 Requirement
  - The cloud provider's measures for ensuring the continuity of service needs to be addressed in contract
  - Includes systems breakdowns, natural disasters, and other reasonably foreseeable events.
  - Customer required to obtain covenants re:
    - Regular testing
    - Notice of test results
    - Remedial actions
    - Test results provided to OSFI
    - Notification if cloud provider makes significant changes to these plans or experiences other significant impacts

Record keeping

- Certain records have to be maintained in Canada
  - Section 238, 239 and 597 of the *Bank Act*; section 243, 244 of the *Trust and Loan Companies Act*; section 261, 262 and 647 of the *Insurance Companies Act*; section 235, 236 of the *Cooperative Credit Associations Act*.
- Public issuers require oversight
- Basic good business practices

Inspection and Audit Rights

- OSFI Inspection Rights - *Insurance Companies Act*, S.C. 1991, c. 47, s. 674; *Bank Act*, S.C. 1991, c. 46, s. 643; *Trust and Loan Companies Act*, S.C. 1991, c. 45, s. 505; *Co-operative Credit Associations Act*, S.C. 1991, c. 48, s. 437
- Audit rights
  - OSFI B-10
    - Customer's right to audit
    - OSFI's right to audit
    - OSFI's right to internal audit reports
  - CSAE 3416 reports
    - Scope issues

Subcontractors

- OSFI requires audit and inspection rights over “significant” subcontracting arrangements
- B-10 requires that subcontractors comply with security and confidentiality restrictions
- B-10 also requires that the cloud agreement address rules for subcontracting – i.e., when approved (or not)
- Good business practice to require oversight over material subcontractors
- Should also ensure that subcontractors provide IP rights, warranties, and indemnities sufficient for cloud provider to give those to customer

Default and Termination

- OSFI B-10:
  - Default situations, remedies and cure periods need to be clearly described
  - Customer must be able to ensure continuity of operations
  - Timely return of assets; data must be returned in format that is usable without prohibitive cost
  - Contract cannot terminate where Superintendent takes over the customer (FRE)
- Termination for convenience
- Not all service level breaches lead to termination
- Service level credits cannot be sole and exclusive remedy

Limits of liability

- Cloud provider's risk allocation technique to make business viable
- Generally accepted, with typical exclusions:
  - Confidentiality/privacy breaches (privacy contentious today)
  - IP indemnity
  - Personal injury/tangible property loss
  - (Gross) negligence/wilful misconduct
  - Breach of law
  - Breach of IP rights
  - Payment of fees (where a mutual limitation)
- *Tercon* case and fundamental breach

Indemnities

- Another risk allocation device
- Should be limited to 3rd party claims
- Typical:
  - IP indemnity
  - 3rd party privacy breaches
  - Confidentiality/Privacy breaches
  - Any sensitive issue
- Provides “leg up” in litigation

Transition Issues

- Probably the most overlooked in cloud deals
- Can be critically important for some applications
- Transition back in house or to new service provider
- Knowledge transfer
- Lengthy period may be necessary
- If a critical application, must receive transition services even in termination for default

Summary

- The cloud offers opportunities but providers must be accommodating of their customers' legal obligations
- Legal issues are evolving and cloud contracts need to adapt to reflect them
- Don't base your template document on something you found on the web – get some professional insight!

The Dirty Dozen – 12 Contentious Things About Cloud Computing Deals

Cassels Brock & Blackwell LLP

Suite 2100, Scotia Plaza
40 King Street West
Toronto, ON Canada M5H 3C2

Tel: 416 869 5300
Fax: 416 350 8877

Suite 2200, HSBC Building
885 West Georgia Street
Vancouver, BC Canada V6C 3E8

Tel: 604 691 6100
Fax: 604 691 6120












CASSELS BROCK
LAWYERS