The Law Society of British Columbia

Practice Resource

Cloud computing due diligence guidelines

The following guidelines are excerpted from the Report of the Cloud Computing Working Group, dated January 27, 2012

DUE DILIGENCE GUIDELINES[1]

A lawyer must engage in due diligence when using a third party service provider or technology for data storage and/or processing. The purpose of the due diligence is to ensure that the lawyer is able to fulfill his or her professional responsibilities while using a particular service provider or technology. The due diligence may also assist the lawyer as a matter of business risk management. Although these guidelines are designed to assist lawyers in determining whether to use electronic data storage and processing that is accessed over a network, such as the Internet (cloud computing), lawyers may find some of these factors useful in performing due diligence with respect to data storage and processing that does not use cloud based technologies. These guidelines assume the National Institute for Standards and Technology definition of cloud computing, as amended from time to time.[2]

This checklist also contains a section for privacy considerations. It is important to note that while the Law Society views the approach contained in Part B as acceptable the Privacy Commissioner may have a different perspective. The approach in Part B adopts concepts from the Alberta *Personal Information Protection Act*. It is not prescriptive.

If a lawyer uses third party data storage and processing that locates the clients' records outside of British Columbia, the lawyer should advise the client of this fact so the client can determine whether or not to use the lawyer. It is optimal to memorialize the client's consent in a written retainer.

PART A: GENERAL DUE DILIGENCE GUIDELINES

- Lawyers must ensure that the service provider and technology they use support the lawyer's professional obligations, including compliance with the Law Society's regulatory processes. This may include using contractual language to ensure the service provider will assist the lawyer in complying with Law Society investigations.

---

[1] Some of these factors are also raised by commentators on cloud computing, including from the following sources: Wayne Jansen and Timothy Grance, NIST Guidelines on Security and Privacy in Public Cloud Computing (Draft Special Publication 800-144: January 2011); the North Carolina State Bar "Proposed 2010 Formal Ethics Opinion 7, *Subscribing to a Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*" (April 15, 2010), "Proposed 2011 Formal Ethics Opinion 6, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*"; Robert J.C. Deane, *Cloud Computing – Privacy and Litigation Discovery Issues* (Borden Ladner Gervais seminar: 2011)

[2] Special Publication 800-145 (Draft) , January 2011.

- Lawyers are strongly encouraged to read the service provider's terms of service, service level agreement, privacy policy and security policy. Lawyers must ensure the contract of service adequately addresses concerns regarding protecting clients' rights and allowing the lawyer to fulfill professional obligations. Ensure the contract provides meaningful remedies. At a minimum consideration should be given to the following:

    - Lawyers must take steps to ensure the confidentiality and privilege of their clients' information is protected. Clear contractual language should be used to accomplish this objective.

    - Lawyers should try to ascertain where the data is stored/hosted. Consider the political and legal risks associated with data storage in foreign jurisdictions. The lawyer must consider whether he or she can comply with British Columbian and Federal laws, such as laws governing the collection of personal information, when using third party service providers (see Part B).

    - Who owns the data? Confidentiality and privilege are rights that lie with the client. Lawyers must ensure ownership of their clients' information does not pass to the service provider or a third party.

    - What happens if the service provider goes out of business or has their servers seized or destroyed?

    - On what terms can the service provider cut off the lawyer's access to the records?

    - Will the lawyer have continuous access to the source code and software to retrieve records in a comprehensible form? Consider whether there is a source code escrow agreement to facilitate this.

    - How easily can the lawyer migrate data to another provider, or back to desktop applications?

    - Who has access to the data and for what purposes?

    - What procedural and substantive laws govern the services? What are the implications of this?

    - Does the service provider archive data for the retention lifecycle the lawyer requires?

    - Are there mechanisms to ensure data that is to be destroyed has been destroyed?

    - What are the lawyer's remedies for the service provider's non-compliance with the terms of service, service level agreement, privacy policy or security policy?

    - Ensure the service provider supports electronic discovery and forensic investigation. A lawyer may need to comply with regulatory investigations, and litigation disclosure, in a timely manner. It is essential that the services allow the lawyer to meet these obligations.

- What is the service provider's reputation? This essentially requires the lawyer to assess the business risk of entrusting records to the service provider. Lawyers should seek out top quality service providers.

- What is the service provider's business structure? Lawyers must understand what sort of entity they are contracting with as this affects risk.

- Does the service provider sell its customer information or otherwise try and commoditize the data stored on its servers?

- Lawyers should strive to keep abreast of changes in technology that might affect the initial assessment of whether a service is acceptable. Services, and service providers, may become more or less acceptable in light of technological and business changes.

- What security measures does the service provider use to protect data, and is there a means to audit the effectiveness of these measures?

- A lawyer should compare the cloud services with existing and alternative services to best determine whether the services are appropriate.

- If using a service provider puts the lawyer off-side a legal obligation, the lawyer should not use the service. For example, there may be legislative requirements for how certain information is stored/secured.

- Lawyers should establish a record management system, and document their decisions with respect to choosing a cloud provider. Documenting due diligence decisions may provide important evidence if something goes wrong down the road.

- Consider the potential benefits of a private cloud for mission critical and sensitive data, along with information that may need to be stored within the jurisdiction.

With respect to certain trust records, the Trust Regulation Department at the Law Society of British Columbia recommends the following as *best practices*:

1. All bank reconciliations (for all trust and general bank accounts) should be printed the same date it was completed and stored in hard copy;[3]

2. A full and complete trust ledger should be printed in hard copy at the close of each client file matter and stored in hard copy;

3. A master billings file should always be maintained in hard copy;

4. Have a disaster recovery plan in case the cloud provider shuts down. Regularly back up all files and records in possession of the member. Store backup files in a fire safe, safety deposit box;

[3] Reference to "hard copies" is a best practice. An electronic copy that can be provided in print or PDF form is acceptable. Note, however, the obligations regarding cash transactions in Rule 3-61.1 require a cash receipt book.

5. All Members should print off or export to electronic file (i.e. pdf) all accounting records required by Division 7 Rules on an ongoing basis and store locally;

6. If client files are stored electronically, all key documents supporting transactions and key events on the file must be printable on demand in a comprehensible format (or exported to acceptable electronic format (ie PDF) and available for at least 10 years from the date of the final accounting transaction.

The Lawyers Insurance Fund notes that there may be data breaches and other risks in using a particularly technology, including cloud computing, that may lead to losses by lawyers and clients. These are not risks to which the professional liability insurance policy responds, so lawyers will want to consider the risks and how best to protect themselves as part of their due diligence. Steps that might be taken include:

- A lawyer should obtain informed client consent for the use of the services;
- A lawyer should require the service provider to indemnify the lawyer for any claims the lawyer faces as a result of using the service; and
- A lawyer should consider buying insurance on the commercial market to cover risks such as data breaches.

PART B: PRIVACY CONSIDERATIONS

Lawyers need to ensure that their process for collecting, retaining and using personal information complies with the applicable legislation. If the lawyer is dealing with private sector collection of personal information, it is possible that the BC *Personal Information Protection Act*, SBC 2003, c. 36, or the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 will apply, or both may. Jurisdiction may be overlapping, and lawyers should aim for the higher standard. It is also possible that the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 (FIPPA) will apply. For example, the lawyer may perform contract work for a public body that entrusts the lawyer with personal information the public body has collected. FIPPA, subject to certain exceptions, prohibits personal information that is collected by a public body from being stored or accessed outside Canada.[4] If a lawyer is using cloud computing, they need to understand the obligations that attach to that data before they collect it in order to ensure they are complying with privacy legislation. Understanding where the data is stored and/or accessed takes on increased importance.

Lawyers may be collecting, retaining and using personal information from a number of sources including employees and clients. If a lawyer is using data storage outside of Canada it is recommended that the lawyer advise the individual at the commencement of the relationship. In the case of prospective clients, this could occur during the conflict checking process. It is important for an individual to know before the personal information is collected that it is being stored/processed outside of Canada.

It is important to remember that there are obligations with respect to the collection, use and retention of personal information. Some of this personal information may also attract solicitor and client privilege. A lawyer has a professional obligation to protect solicitor and client privilege that overlays the legislative requirement for dealing with personal information. The

[4] FIPPA, Section 30.1.

checklist below may be sufficient for personal information, but may fall short of the requirements for protecting information that is governed by confidentiality and privilege. A lawyer must understand the nature of the information they are collecting, using and retaining and ensure appropriate safeguards are in place. The checklist also draws on concepts from the Alberta *Personal Information Protection Act*, SA 2003, c. P-6.5 (AB PIPA) which articulates a high standard.

Step 1:

Lawyers should review their privacy policy and determine whether it supports the use of the service contemplated (eg. cloud computing). It is possible that the privacy policy is out of date. It is also possible that the law firm will have collected a considerable amount of personal information that the firm is now contemplating storing in a manner not addressed at the time it was collected.

Step 2:

Lawyers must identify which legislation governs the information they are collecting.

Public sector:

If the personal information is governed by FIPPA, the lawyer must ensure the information is only stored or accessed within Canada, unless one of the exceptions is met. It may be necessary to set up a separate system to address this sort of information.

Private sector:

While personal information may be stored or processed outside of British Columbia, it is essential to take steps to protect the personal information. Consider the following:

- The lawyer must enter into a data protection arrangement with the service provider that ensures equivalent levels of data protection as are required in BC/Canada;[5]

- Where data is being processed, consent is not required;

- Consent is required if the personal information is being disclosed for a secondary purpose (consider the risk here regarding confidential and privileged information);

- Because of the openness principle, notice should be given to the client that data will be processed outside Canada. At a minimum, notice should include alerting the client to the potential that a foreign state may seek to access the data for "lawful access" purposes;[6]

- The purpose of notice is to alert the client to the risk that their personal information may be accessed by a foreign government;

- The lawyer's policy and practices must indicate:[7]

[5] See PIPEDA Case Summary No. 313.
[6] See s. 4.8 of Schedule A of PIPEDA.
[7] AB PIPA, s. 6(2).

  - The countries outside Canada where the collection, use and disclosure will occur;
  - The purposes for which the service provider has been authorized to collect, use or disclose the personal information.

- Before or at the time of collecting or transferring personal information to a service provider outside Canada, the lawyer must notify the individual:[8]
  - Of the way to obtain access to written information about the lawyer's policies and practices regarding service providers outside Canada; and
  - The name or position of a person who is able to answer the individual's questions about the collection, use, disclosure or storage of personal information by the service providers outside Canada.
- While the notification does not require information about the countries outside Canada, the privacy policy should contain this information.

[8] AB PIPA, ss. 13.1(1) and (2).