Law Society of Saskatchewan
Continuing Professional Development

The Use of Cloud Computing for the Storing and Accessing of Client Information: Some Practical and Ethical Considerations

Jeffrey D. Scott

Jeffrey D. Scott, Legal Professional Corporation

Practice Advisors Webinar Series Part 2: Communication and Cloud Computing
Wednesday, November 6, 2013

The Use of Cloud Computing for the Storing and Accessing of Client Information:

Some Practical and Ethical Considerations

What is Cloud Computing?

Simply put cloud computing is the keeping of one's data on a third party's server (i.e. the cloud computing service provider). The data is accessed with an internet connection.

What is the attraction of Cloud Computing for lawyers?

Cloud computing is attractive due to the economic and technological benefits of the cloud computing service.

Cloud computing service providers can provide large storage capacity to lawyers.

What are the drawbacks to cloud computing for lawyers?

Transferring information from the law firm to an external cloud server raises privacy and confidentiality concerns. Often the cloud service providers, including the actual clouds' computer servers, are located outside of Canada. Foreign legislation (for example: the US: **Patriots Act**) might permit access by the U.S. government to the law firm's data. Hackers might attempt access to the clouds' computer servers- a treasure trove of personal, confidential and commercially sensitive information from a variety of sources. With cloud computing there is a very real potential loss of control over the clients' confidential information

Professional Responsibility

We, as lawyers, often have in our possession highly personal and commercially sensitive information pertaining to our clients. Given that sensitive information lawyers are bound by, for example, codes of professional conduct, rules of court, etc. which prevent unwarranted third-party access to the information.

Failure to uphold the professional duty to maintain the privacy and confidentiality of our client's information could result in disciplinary action.

Due Diligence

Due diligence is imperative when contemplating the use of a cloud service provider. Due diligence includes reading and understanding the terms of the contractual agreement(s) with the cloud and making sure the terms will permit the lawyer to fulfil his or her professional responsibilities and obligations while using the cloud. Due diligence, also, includes checking out the reputation and security measures the cloud provider has in place. **Documenting** due diligence decisions and due diligence follow up is recommended.

Law Society of British Columbia: Cloud Computing Resource Materials

The Law Society of British Columbia recently published policies on cloud computing:

Law Society of British Columbia: Report of the Cloud Computing Working Group (January 27, 2012)

Law Society of British Columbia: Cloud Computing Checklist (January 2013)

Those resource materials are available on the Law Society of Saskatchewan website:

See: Practice Resources: General Resources: Usage of Technology/Internet.

If your law firm is already using cloud computing **OR** if your law firm is contemplating the use of cloud computing I strongly recommend that you review and act on the recommendations contained within the BC Law Society materials.

The balance of my paper will identify and elaborate on some of the information contained within the BC Law Society materials on cloud computing. I do recommend that you review and consider **all** of the information contained with the BC Law Society materials. I have, also, summarized in the balance of my paper information I have obtained from a variety of other resource materials on the use of cloud computing by lawyers.

Some Practical and Ethical Considerations

a) Costs to use a Cloud Service Provider:

What will be the initial set up cost to use a cloud provider?

What are the ongoing (i.e. monthly) fees to use a cloud provider?

Are there usage fees?

What internal office costs will you have in order to use a cloud service (i.e. hardware, software, etc.)?

Do a cost analysis for using a cloud service? Will there be a cost savings?

b) IT Considerations with respect to the use of a Cloud Service Provider:

Does the cloud service application integrate with your other law office systems?

Does your law office have sufficient bandwidth to run the cloud application with adequate performance?

Test the system while running other office systems.

c) User reviews of Cloud Service Providers:

What is the service provider's reputation? What is the service provider's business structure?

What is the business risk of contracting with a service provider?

User reviews of cloud service providers should be undertaken. An internet search, for example, of cloud service providers might disclose issues that users have experienced with respect to specific cloud service providers (for example, privacy and confidentiality breaches).

Speak with colleagues who have experience with cloud service providers. Their practical experience with specific cloud service providers might be helpful when deciding on a particular cloud service provider.

d) Consider the sensitivity of the information that you are contemplating transferring to the Cloud Service Provider:

Some client information is likely more sensitive than other client information. Should highly sensitive client information be transferred from your law firm to an external cloud service provider?

e) Read and, if necessary, Negotiate the Terms of the Cloud Service Provider's Agreements:

Cloud service providers often have a number of agreements that users are obligated to sign. The typical agreements include, for example, a Service Level Agreement and a Privacy and Confidentiality Agreement.

Review the terms of the Agreements. Ensure the contract of service adequately addresses concerns regarding protecting clients' rights and allows the lawyer to fulfill professional obligations. Make sure the contract provides meaningful remedies to the lawyer.

Some of the terms to look for within the agreements include:

1) Ensure the lawyer maintains ownership over the data transferred to the cloud service provider;
2) Are there sufficient remedies available to the lawyer in the event of: data breaches, indemnification obligations and service availability failure? Is the cloud provider required to indemnify you for losses as a result of using their services? Is there third party insurance to cover this?
3) Who is responsible for the security of your data? Do not accept any limitation of liability related to privacy and security. Is the service provider obligated to have

adequate insurance in place? Is the service provider obligated to provide you with certificates of insurance evidencing appropriate insurance?

4) Who is responsible for privacy and regulatory compliance?
5) What ability do you have to audit or view audits of the cloud provider's performance? Is the cloud provider obligated to produce audit reports on a regular basis that are conducted by reputable 3rd party experts? How often does the cloud provider have their security audited?
6) If the cloud provider ceases business, how long will it take you to get your data? In what format will the data be returned to you?
7) Does the cloud provider use cloud services itself? If so, is the cloud provider required to give notice if contemplating contracting out to another cloud service provider? Be wary of this-where will the data end up?
8) Is the cloud provider responsible for sub-contractors?
9) Does the agreement set out the location of the cloud's servers? Are there multiple storage locations?
10) Who has access to your data?
11) What is the language, guarantees or representation from the cloud provider with respect to the security of your data?
12) What laws are applicable to the data?
13) What encryption method is applicable to the data-in transmission and in storage?
14) Can the cloud provider access your data? If so, for what purpose?
15) To what extent is confidentiality and privilege of your client's information reasonably protected? Clear contractual language should be used to ensure the confidentiality and privilege of the clients' information is protected.
16) What are the cloud provider's breach notifications requirements?
17) Can you terminate the service? At what cost or penalty or on what terms?
18) Is the cloud provider obligated to provide notice to the lawyer if a security or privacy breach occurs? If a breach occurs what professional obligations will you have-i.e. notice to the client, notice to the Law Society?
19) Will your data be sanitized (i.e. removing all trace of the lawyer's data) from the cloud provider in the event of a termination? Cloud service provider must not retain any of your law firm's information after the contract is finished.
20) Make sure the cloud service provider is obligated to return to you all of your law firm's information at the end of the agreement.
21) What notice is the cloud service provider obligated to provide when the agreements with the provider are changed?
22) What happens if the cloud provider ceases business or had their servers seized or if they are destroyed or damaged?
23) Is the cloud computing system available 24/7?
24) What help desk hours are available by the cloud? What kind of support is provided-phone, email, web-based chat?

25) What are the back-up systems of the cloud provider? Where are the back-up systems located? Is the cloud service provider obligated to notify you if they change backup providers?
26) What are the penalties to the cloud provider should the cloud provider go down?
27) Are there maintenance periods? If so, what notice will be given?

f) Notification to the Client and Obtaining the Written Consent of the Client:

The lawyer should inform the client of the lawyer's intention to use a third party's storage of the client's information. The lawyer should, also, inform the client where the third party's storage is located. The client's written consent to store their data in the cloud should be obtained. Consideration should be given to including the client's written consent in the retainer agreement.

g) Back-Up:

Maintain a local backup of your data. Ensure the backup is stored in a safe, secure and fireproof location.

h) Successor:

It would be good succession planning to inform one's successor that you are using a cloud service provider and to provide the successor with a copy of all agreements entered with the cloud computing service.

i) Professional Liability Insurance:

Will professional liability insurance cover privacy issues arising from the use of a cloud? It would be prudent to contact SLIA and ask that question.

Application of Privacy Legislation to Lawyers and the Use of Cloud Service Providers:

Law firms, like other organizations, must comply with privacy legislation. **THE FEDERAL PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT,** SC 2000, c.5 ("PIPEDA") applies to organizations that collect, use or disclose personal information in the course of commercial activities, including federal works, undertakings and businesses. Given the nature of the practice of law this includes private sector lawyers and law firms.

The Office of the Privacy Commissioner of Canada has prepared a booklet called: "A Privacy Handbook for Lawyers: PIPEDA and Your Practice" (the "Handbook"). For any lawyer

considering using a cloud service provider or already using a cloud service provider I recommend that you obtain and read the Handbook. It is available for downloading on the website of the Office of the Privacy Commissioner of Canada.

PIPEDA requires personal information to be safeguarded at all times. Personal information should be safeguarded through the use of, for example, technological measures, passwords and encryption.

With respect to the use of a cloud service provider there is stated on page 8 of the Handbook the following:

> Lawyers must use contractual or other means to provide a comparable level of protection when client information is being processed or stored by a third party. Where any third party service provider may have access to or otherwise handle personal information on behalf of a lawyer, it is strongly recommended that a written agreement be put in place between the third party and the lawyer. Such a contract should include provisions governing the jurisdiction where information will be processed or stored, ownership and use of information, the level of privacy controls used by the service provider, access and correction procedures, audits, and deletion procedures. **Lawyers must remember that they remain accountable for information transferred to third parties for processing.** PIPEDA also requires organizations to be transparent about their personal information handling practices. Accordingly, organizations should notify clients when using a service located outside of Canada and advise them that their personal information may be subject to the laws of a foreign jurisdiction (emphasis added).

Conclusion:

Cloud based computing can offer many advantages to lawyers. However, when considering the use of a cloud it is imperative that due diligence is done. We, as lawyers, must keep in mind that we are accountable to our clients (and ultimately to the Law Society) for the use and outsourcing of our clients' information. The "buck stops with us"-we are obligated to protect and preserve the confidentiality of our clients' information.

Jeffrey D. Scott November, 2013

Jeffrey D. Scott Legal Professional Corporation

3066 Rae Street

Regina, Saskatchewan S4S 1R7

Telephone: 1-306-546-4728 Fax: 1-306-546-4729