



the risks associated with lawyers using cloud computing technology and suggests how they can use those technologies and services while still meeting their professional obligations.

"Lawyers have professional responsibilities that arise out of their roles as lawyers and fiduciary obligations to their clients. Some of the records are the client records, and so the lawyers have obligations to protect those records, to ensure that they remain confidential and privileged," Munro said.

The report recommended the Law Society publish guidelines to assist lawyers in performing due diligence when deciding whether or not to use a third-party service provider for electronic data storage and processing, including cloud computing. After the guidelines were published, Munro and Bilinsky developed the comprehensive Cloud Computing Checklist released in January 2013, which raises some of the issues that should be considered prior to a lawyer or law firm moving data into the cloud. Since its release, the checklist has

garnered national and international attention, including from the secretary general of the Council of Bars and Law Societies of Europe.

"It involved a lot of research because it wasn't just the report that we'd have to look at. We'd have to look at what other knowledgeable people in the whole legal computing cloud sphere were saying about the things you should be thinking

continued on page 11

PRACTICE TIPS, by Dave Bilinsky, Practice Management Advisor

BC lawyers and cloud computing

♪ *It's coming down, it's coming down, it's coming down*
These clouds could never hope to save us ... ♪

Lyrics, music and recorded by Thrive

THE BENCHERS HAVE recently adopted rule changes based on the [report and recommendations of the Cloud Computing Working Group](#).

The amendments address three areas:

- the requirements for electronic data storage and processing;
- producing records in a complaint investigation or forensic audit; and
- third-party storage providers and security.

I would like address a number of questions that have been raised concerning the use of cloud computing resources by BC lawyers.

Q: Why is the cloud computing report important?

A: The rule changes recently adopted by the Benchers give effect to the recommendations in the [Cloud Computing Working Group Report \(January 2012\)](#). To my understanding, this report is one of the leading examinations of the use of cloud computing resources by lawyers by any regulator. BC lawyers considering using cloud computing resources should refer to the [Cloud Computing Checklist](#) for guidance. The report, recommendations and checklist highlight that the Law Society has provided and continues to provide thoughtful leadership to the profession on the adoption of new technologies.

Q: What guidance is there for BC lawyers looking to use cloud computing?

A: The Cloud Computing Working Group Report supports the idea that the Law Society regulates lawyers, not technology. It is up to the lawyer to determine whether it is appropriate to use a particular technology, recognizing that the professional responsibilities of a lawyer will continue. This places cloud computing on an equal

basis with a lawyer's use of services such as bookkeeping, accounting software, IT consultants or any other provider of services. As a result, the Law Society expects lawyers to exercise due diligence when using any service provider that handles, stores or processes client records, whether those records are in paper form or electronic. The Cloud Computing Checklist provides a list of considerations for a lawyer contemplating moving data to the cloud. Lastly, the Law Society's Practice Advice department is available to discuss cloud computing.

Q: Are BC lawyers prohibited from using US-based cloud computing providers?

A: There is no prohibition against using services in which servers are located outside Canada. However, lawyers must ensure the service complies with any legal limitations on where the records can be stored. Consider, for example, s. 30.1 of the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, chapter 165. If the lawyer acts for clients that are prevented from storing data outside of Canada, this will be a very important consideration. The checklist and the report highlight that lawyers' obligations to preserve and protect privilege and confidentiality do not disappear; accordingly, the checklist includes questions to consider when choosing a service so the lawyer can be satisfied client information is protected. Lawyers should disclose to their clients that they use cloud computing resources and that a client's data may be stored outside of Canada. This advice should be incorporated into the law firm's retainer agreement, since informed client consent is an integral part of responsibly using cloud computing resources.

Q: Does the Law Society prohibit the use of non-BC based cloud computing providers, such as Google or Dropbox, by lawyers?

A: The Law Society neither endorses nor rejects the use of specific products.

While new Rule 4-10 permits the Executive Committee, by resolution, to declare that a specific entity is not a "permitted storage provider" for the purposes of compliance with that rule, no such entity has been so declared.

However, if the Law Society discovers during the course of exercising its regulatory function that lawyers who use certain services are unable to comply with the rules for disclosing records, either because the service provider refuses to assist with the regulatory disclosure or is incapable of providing the records, the Law Society can



disapprove the use of that service for lawyers. But at this time, no cloud provider is prohibited by the Law Society.

Q: What has changed in BC regarding cloud-based computing?

A: In my view, the recent rule changes address how storing data in the cloud may impact the regulatory work that the Law Society is mandated to perform in the public interest.

The Law Society must have access to the files, documents and other records of a lawyer under investigation. If those files, documents and other records are stored, either in paper form or electronically, in a way that prevents the Society from gaining access to them, then the rules envision a process by which lawyers who are unable to provide such records can be suspended until they are able to do so.

For example, a lawyer who is required under Rule 3-5 (Investigation of complaints) or 4-43 (Investigation of books and accounts) to produce and permit the copying of files, documents and other records, provide information or attend an interview and answer questions, fails or refuses to do so, may be suspended until he or she has complied with the requirement to the satisfaction of the Executive Director (Rule 3-5-01).

In particular, Rule 10-4(4) contains provisions that a lawyer needs to consider when using any cloud provider:

(4) A lawyer must not maintain records, including electronic records, with a storage provider unless the lawyer

(a) retains custody and control of the records,

(b) ensures that ownership of the records does not pass to another party,

(c) is capable of complying with a demand under the Act or these Rules to produce the records and provide access to them,

(d) ensures that the storage provider maintains the records securely without

(i) accessing or copying them except as is necessary to provide the service obtained by the lawyer,

(ii) allowing unauthorized access to or copying or acquisition of the records, or

(iii) failing to destroy the records completely and permanently on instructions from the lawyer, and

(e) enters into a written agreement with the storage provider that is consistent with the lawyer's obligations under the Act and these Rules.

These are new provisions, but the concepts are not new. No lawyer would store records – paper or electronic – with a provider that accessed them or copied them, except as necessary to provide the service to the lawyer. No provider would be permitted to gain unauthorized access to the lawyer's records. Further, when a lawyer destroys records, he or she needs to ensure that the records have been completely and permanently destroyed – regardless of whether the records are in paper or electronic form. What the Benchers have done is made it clear that these responsibilities apply to records that are stored with a cloud provider.

* * *

To recap, the Law Society has simply updated the Rules to incorporate the potential use of cloud computing and the requirement for the Law Society to have

access to a lawyer's records should the need arise, no matter where those records may be stored. Further, the lawyer's responsibilities apply equally, whether the records are in paper or electronic form.

The Cloud Computing Checklist is designed to ensure lawyers turn their minds to compliance with Law Society audits and investigations, regardless of the technology they may be using.

Any questions on the use of cloud computing resources by BC lawyers can be directed to Practice Management Advisor Dave Bilinsky at daveb@lsbc.org.

With respect, I submit that BC lawyers' use of cloud computing resources has not come down and that, in fact, these clouds can save us a great deal of time, energy and resources. ❖

I gratefully acknowledge the assistance of Law Society staff lawyer Doug Munro who co-authored the Cloud Computing Checklist with me, based on the ground-breaking work of the Cloud Computing Working Group.

A version of this article originally appeared on slaw.ca on November 18, 2014.

Feature – Cloud computing... from page 9

of." Bilinsky said. "Take the policy positions that were set out in the report and try to put them into a form that is a bit more workable for lawyers to use."

Some examples of the questions on the checklist are: Has the cloud provider had any security breaches? What happens if the cloud provider ceases business or has their servers seized or destroyed? Who has access to your data?

"You're relying on the security of the trust of the cloud provider to put into place adequate safeguards around that data," Bilinsky said. "You have to ensure it doesn't get sold to third parties, that only authorized people have access to both the physical location of the data, and access

to the data electronically, which can prove problematic."

While the Law Society does not recommend particular cloud computing services over others, Bilinsky suggests that lawyers use technology that provides zero knowledge encryption along with a password keeper program.

Not only does the checklist guide lawyers when they engage, with due diligence, in protecting the confidentiality and security of client files, but it also provides help to lawyers when thinking about their obligations to the Law Society.

"Lawyers have obligations with respect to the Law Society when we're doing audits and investigations. Lawyers need to make their records available to us," Munro said. "Cloud computing doesn't change

those obligations."

On October 31, the Benchers adopted several changes to the Law Society Rules to address the obligations of a lawyer to the Law Society, giving the regulator more powers to ensure that lawyers comply.

"We clarified the capacity to suspend. That won't give you the records, but what it will do is suspend the lawyer and provide public protection on that level," Munro said.

More changes to the Law Society Rules will inevitably happen, as technology and the discussion around its use evolve over time.

Lawyers who have any questions about the use of cloud computing are encouraged to contact the Law Society's practice management advisor. ❖

Practice watch

by Barbara Buchanan, Practice Advisor

CASH TRANSACTIONS AND RECORDS

AS PART OF its efforts to combat money laundering and terrorist financing, the Law Society limits the amount of cash that a lawyer can accept and requires lawyers to abide by the Law Society's client identification and verification rules. Lawyers who accept cash face additional recordkeeping requirements. Some changes to the recordkeeping requirements were made on October 31, 2014. No changes were made to the amount of cash that may be accepted. Lawyers should ensure that all staff who handle money understand the rules regarding cash transactions.

What additional record-keeping is required when a lawyer accepts cash?

Rule 3-61.1 sets out very detailed requirements. A lawyer who receives any amount of cash for a client that is not the lawyer's employer, must maintain a cash receipt book of duplicate receipts (the "receipt

book") and make a receipt in the receipt book for any amount of cash received. The receipt book must be kept current. The lawyer must record the following for each receipt:

- the date on which the cash is received;
- the name of the person from whom the cash is received;
- the amount of cash received;
- the client for whom cash is received;
- the number of the file in respect of which the cash is received;
- all dates on which the record was created or modified (new);
- the signature of the person from whom the cash was received;
- the lawyer's signature (or an individual authorized by the lawyer to sign the receipt on the lawyer's behalf).

Is any special record-keeping required when a lawyer withdraws cash from a trust account?

Unless it is required under Rule 3-51.1(3.2) or (3.3), a lawyer must not make or authorize a cash withdrawal from a pooled or separate trust account (Rule 3-56(1.3)(d)). Rule 3-61.1(3) requires that, for each cash withdrawal, a lawyer

must make a record of transaction signed by the person to whom the cash was paid and identifying:

- the date on which the cash was withdrawn;
- the amount of cash withdrawn;
- the name of the client in respect of whom the cash was withdrawn;
- the name of the person to whom the cash was paid;
- all dates on which the record was created or modified (new).

It is recommended that lawyers use the

cash receipt book of duplicate receipts to record the information, including the signature of the person to whom the cash was paid.

How long must a lawyer keep cash transaction records?

Rule 3-68 provides that a lawyer must keep the cash receipt book of duplicate receipts and required cash withdrawal records ("cash transaction records") for as long as these records apply to money held in trust and for at least 10 years from the final accounting transaction (new). Cash transaction records must be kept at the lawyer's chief place of practice in BC for as long as the records apply to money held in trust and, in any case, for at least three years.

The record retention requirement in Rule 3-68 applies to cash transaction records as well as to all the other records referred to in Rules 3-59 to 3-62 (e.g. accounting records, including supporting documents, trust account records, general account records, and billing records). However, as of October 31, 2014, records maintained in electronic form do not have to be kept at a lawyer's chief place of practice in BC as long as they are kept for the requisite period and in accordance with the Law Society Rules (see Rule 3-68(2) and new Rules 10-4 and 10-5).

How much cash may a lawyer accept?

Lawyers are generally prohibited from accepting an aggregate amount of \$7,500 or more in cash with respect to any one client matter or transaction, except within the limited exceptions set out in Law Society Rule 3-51.1. A lawyer who accepts cash incrementally must make sure that, in total, it adds up to less than \$7,500, unless acceptance of a greater amount is permitted by the rule (e.g. a retainer or payment of an account for professional fees and disbursements).

When does the prohibition against accepting an aggregate amount of \$7,500 or more apply?

Rule 3-51.1 applies to a lawyer engaged in

