The Law Society
of British Columbia

REPORT OF THE CLOUD COMPUTING WORKING GROUP

Date: July 15, 2011

Gavin Hume, QC (Chair)
Bruce LeRose, QC
Peter Lloyd, FCA
Stacy Kuiack

Purpose of Report: **Discussion and Decision**

Prepared on behalf of: **Cloud Computing Working Group**

Policy and Legal Services Department
Doug Munro 604-605-5313

TABLE OF CONTENTS

1. WHAT ARE THE BENCHERS BEING ASKED TO CONSIDER?.....page 2
2. PURPOSE OF THE REPORT.....page 3
3. OVERVIEW OF THE ISSUES.....page 6
4. ANALYSIS OF THE ISSUES.....page 8
    a. Jurisdictional Issues.....page 8
    b. How the technology affects lawyers' ability to discharge their professional responsibilities.....page 10
    c. Security.....page 13
    d. "Custody or Control" of accounting records.....page 14
    e. Records Retention.....page 15
    f. How the technology affects the Law Society's ability to carry out its regulatory function.....page 17
    g. Potential impact on Rule 4-43.....page 19
    h. Ensuring Authorized Access to Records.....page 20
    i. Lawyers Insurance Fund Issues.....page 20
5. CONCLUSION.....page 21
6. RECOMMENDATIONS.....page 23
7. APPENDIX 1: Due Diligence Checklist.....page 27
8. APPENDIX 2: Definition of Cloud Computing.....page 34
9. APPENDIX 3: Concepts discussed, but not resolved.....page 37
10. SELECTED BIBLIOGRAPY.....page 40

WHAT ARE THE BENCHERS BEING ASKED TO CONSIDER?

The Benchers are being asked to adopt a series of recommendations that fall into three categories. One of the recommendations is to 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" [1]). The second category of recommendations relates to changes to the Law Society Rules and resources to ensure the Society's regulatory function keeps pace with certain technological changes. The third category of recommendations relates to methods to improve lawyers' (and law students) understanding of their obligation to use technology in a manner consistent with lawyers' professional responsibilities.

Lawyers face certain risks when using cloud computing, and cloud computing creates certain challenges for regulatory bodies. Some of these risks are unique to cloud computing, but others are not. Among the issues that require consideration by the Benchers are:

[1] "Cloud computing" is defined in Appendix 2.

- What due diligence and precautions must a lawyer engage in when entrusting records to a third party service provider for storage and/or processing?
- Given that cloud computing can store a lawyer's records in multiple jurisdictions, including outside Canada, what factors should lawyers consider in deciding whether or not to use the technology (e.g. Preserving client confidentiality and privilege, maintaining custody and control of trust records, complying with Law Society investigations that require record disclosure, ensuring records storage outside the jurisdiction is consistent with provincial and federal laws, such as personal information protection legislation, etc.)?
- Given that cloud computing can store a lawyer's records in multiple jurisdictions, including outside Canada, what challenges does this create for the Law Society in performing its regulatory functions, including:
    - Trust regulation and audits;
    - Professional Conduct and Discipline investigations;
    - Custodianships.
- Given the manner in which cloud computing stores data, what implications are there for evidentiary issues? Does this mode of computing affect the ability to collect metadata and/or forensic auditing data?

The Benchers are being asked to take an approach modeled on lawyer regulation, rather than attempting to regulate an emerging technology.

PURPOSE OF THE REPORT

The purpose of this report is to identify the risks associated with lawyers using electronic data storage and processing, accessed remotely over a network (like the Internet), particularly circumstances where those services are provided by a third party vendor, and to suggest how lawyers can use those technologies/services while still meeting their professional obligations.

The privilege of practising law comes with professional obligations and those obligations extend to the use of technology. If a lawyer is unable to meet his or her professional obligations when using a given type of technology or service provider, the lawyer should not use the technology or service provider when acting in a professional capacity. In order to determine whether a particular technology or service provider is acceptable, a lawyer must engage in due diligence. This report suggests some factors designed to assist lawyers in performing their due diligence (see **Appendix 1**). The report also makes recommendations regarding the Law Society's regulatory rules and processes to facilitate efficient and effective investigations in the face of emerging technologies.

Technological change tends to outpace the law. In the regulatory context this can lead to ambiguities regarding rights and obligations and can create gaps in the regulatory process, all of which can increase the public risk. This report considers lawyers using electronic, remote data storage and processing. The main focus of the report is on

lawyers using what is commonly termed "cloud computing", but the report has broader application. In approaching the topic the Working Group considered cloud computing to entail electronic data processing and/or storage accessed over the a network such as the Internet. The more detailed description the Working Group favours is the NIST Definition of Cloud Computing[2] (see **Appendix 2**). There is a great deal being written about cloud computing every day. The selected bibliography is a starting point for some of this discussion, but readers should bear in mind that the field will continue to develop, and due diligence will require keeping pace with emerging standards and legislation.

Lawyers have professional obligations with respect to managing their clients' information. These obligations include the need to preserve confidential and privileged information, and also the requirement to comply with personal information protection legislation. In addition to these obligations, lawyers are subject to the regulatory authority of the Law Society. This includes the requirement to immediately make available records for copying when faced with a 4-43 order, records during a 3-79 compliance audit, practice records during a custodianship and during a practice standards inquiry. When a lawyer uses cloud computing his or her ability to comply with these obligations may be affected. This report analyses the responsibilities of lawyers, and the regulatory authority of the Law Society, in light of technology that in some instances places lawyers' records on servers that are in the possession of third party vendors and which may be located in foreign jurisdictions.

In analyzing these issues the Working Group applied certain principles, including:

- Lawyers must engage in due diligence to ensure they can meet their professional obligations while using technology for any work that may attract solicitor and client confidentiality and/or privilege;
- The due diligence lawyers must perform when considering the use of a particular technology includes due diligence with respect to the service provider of that technology as well as with respect to the technology itself;
- Any changes to the *Legal Profession Act,* the Law Society Rules, and the *Professional Conduct Handbook* must protect the public interest to ensure the public is confident lawyers are discharging their professional obligations and are being effectively regulated;
- Technological change is neither good nor bad; it presents positive opportunities as well as risks;
- The Law Society regulates lawyers, not the development of technology. Where possible, any rules and policies should strive to be technology neutral and directed towards the responsibilities of lawyers;

---

[2] Peter Mell and Tim Grance, Version 15, 10-7-09, available at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (Accessed December 2, 2010). Anyone looking for a thorough, one stop overview of cloud computing may wish to read, Lee Badger, Tim Grance, Robert Patt-Corner and Jeff Joas, NIST, *Draft Cloud Computing Synopsis and Recommendations* (Special Publication 800-146: May 2011).

- Cloud computing is already in use by lawyers and members of the public. It is reasonable to assume its use will only continue to grow.[3]

Cloud computing is subject to considerable hype, and many authors have commented as to its scope and meaning. The seeming ubiquity of the term, in advertizing and media, and the wide range of applications people use in daily life that rely on cloud computing, make it easy to take a laissez-faire attitude towards its adoption. While it is perfectly acceptable for a teenager to uncritically embrace "The Cloud" to create a virtual shrine to Justin Bieber, the same does not hold true for a lawyer dealing with confidential and privileged information. As Jansen and Grance caution:

> *As with any emerging information technology area, cloud computing should be approached carefully with due consideration to the sensitivity of data. Planning helps to ensure that the computing environment is as secure as possible and is in compliance with all relevant organizational policies and that data privacy is maintained.*[4]

The Working Group is of the view that this cautionary note is apposite.

The Working Group accepts that the use of cloud computing and similar technologies already is occurring, and its continued growth is likely. The Working Group believes that what is required is a clear set of practice guidelines to assist lawyers in determining whether to use certain forms of technology or service providers. While the responsibility to perform due diligence and the final determination as to the suitability of a particular technology or service will lie with lawyers to make, the Working Group believes that guidelines will assist lawyers in performing their due diligence.

In addition, the Law Society requires clear and effective rules to deal with lawyers (or law firms) who are unable (or unwilling) to comply with Law Society investigations in a timely manner by virtue of the technology and services the lawyers use. Lawyers must not be allowed to subvert the regulatory function of the Law Society by pointing to a technological or jurisdictional limitation of the technology the lawyers use for data storage and processing.

The Working Group recognizes that just as cloud computing will continue to evolve, the regulation of professionals using the technology and regulation of the service providers will continue to evolve. As such, this report represents a first step into this area. Time and experience will tell whether the right balance has been struck. The Law Society

---

[3] In addition to the considerable amount of money that corporations like IBM, Microsoft, Google, etc. are putting into cloud computing technology, the issues arising from the technology are being discussed by the United States Government, the American Bar Association Commission on Ethics 20/20, privacy commissioners, etc. (see the selected bibliography attached to this report).

[4] Wayne Jansen and Timothy Grance, NIST *Guidelines on Security and Privacy in Public Cloud Computing* (Draft Special Publication 800-144: January 2011) at p. vi.

needs to be open to revisiting concepts that don't work, particularly concepts that place the public at unacceptable risk of harm.

OVERVIEW OF THE ISSUES

The foundational rules that govern the relationship between lawyers and their clients, and lawyers and their regulator, were developed in a paper world. Some of the rules have changed over time in order to reflect changes in technology. For example, historically when the Law Society investigated a lawyer the lawyer had to turn over his records. With the advent of photocopiers, technology facilitated the ability to make copies of records, rather than removing the originals. Rules were modified to reflect this. Most recently the Law Society amended its Rules to facilitate the copying of computer records, while establishing a method to protect the reasonable expectation of privacy that might attach to certain records stored on a hard drive.[5] The inquiry into cloud computing arose from that work. As a matter of policy, the Benchers have also been engaged in initiatives to move the organization towards electronic models of record keeping and to embrace "Green" initiatives. The Working Group was mindful of this while engaging in its analysis.

Lawyers have professional obligations. These obligations include the duty to preserve client confidences and privilege, as well as the duty to comply with the Law Society's investigative function. The issue of how a lawyer stores and processes business records affects a lawyer's ability to discharge these duties. Modern technology allows for data to be processed and stored remotely from a lawyer's workplace. In some cases the lawyer may be storing data on servers the firm owns and operates, and in some instances that work will be contracted out to service providers.

Remote data storage and processing are not new phenomena. Lawyers have been using record storage companies for some time. Before the advent of the personal computer, mainframe computing provided a form of remote data processing. Email transits data across third party systems. Many issues will be the same when it comes to records stored in a warehouse and records stored on third party servers. Foremost are the issues of trust and security.[6]

The Working Group did not assume that trust and security were more or less reasonable when using a third party contractor for storage of digital records over paper records. However, lawyers must bear in mind that once records are networked, the risks of

---

[5] See, the Law Society of British Columbia, *Forensic Copying of Computer Records by the Law Society* (October 2009).

[6] See, for example, Robert Gellman, World Privacy Forum, "Privacy in the Clouds: *Risks to Privacy and Confidentiality from Cloud Computing*", (February 23, 2009); Bruce Schneier, "Be careful when you come to put your trust in the clouds" (The Guardian: June 4, 2009).

breach change and as such the risk analysis is different.[7] With respect to risk management, Jansen and Grance observe: "Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls."[8]

These foregoing issues suggest, in light of the nature of the records lawyers store with third parties, that due diligence is an important part of any determination as to whether a lawyer should use particular services. In this context "due diligence" would include ensuring proper contractual safeguards are in place.

Cloud computing also creates challenges for regulatory bodies.[9] The Law Society is the regulatory body of a self-governing profession. Whether one views self-governance as a privilege or a right, self-governance in the public interest requires that the Law Society have effective means to investigate complaints against lawyers. The *Legal Profession Act* and Law Society Rules establish a range of powers for the Law Society, and place obligations on lawyers, with respect to investigations. These powers include the authority for the Law Society to copy a lawyer's records, and the obligations include the lawyer being required to immediately produce the records for copying on request.[10] Lawyers also have professional obligations to keep records secure and to maintain them for certain periods of time (often many years). Cloud computing can affect both the Law Society's investigative functions and a lawyer's ability to comply with the investigative function and meet their record keeping obligations. Similarly, cloud computing can affect the Lawyers Insurance Fund in its efforts to defend a claim against a lawyer's professional liability insurance.

When data is stored on third party servers, particularly when those servers are in foreign jurisdictions, it is difficult (and perhaps in some instances impossible) to get an immediate copy of the records. When records are paper the Law Society can photocopy them. When records are resident on a local storage device like a hard drive, the Law Society can make a forensic copy of them. In both these scenarios, best evidence can be preserved. When the records are stored on a remote server accessed over the Internet, the Law Society might be able to access the records (if it has certain information), but efforts to copy the record may result in the loss of metadata and relational data that can be important to an investigation. Likewise, printing the electronic records will also result in a loss of that data.[11] In addition, from a technological standpoint, it may take

---

[7] For a discussion of data breeches and the incidence of attacks on networks versus insider breeches, see, Verizon Business Risk Team, "2008 Data Breach Investigations Report".
[8] Footnote 4, at p. 18.
[9] See, Gellman at fn. 6.
[10] See, for example, Law Society Rules 4-43, 3-79.
[11] "Loss" here refers to loss as a result of the format migration as opposed to the issue of whether the data is still resident on a server.

longer to copy a lawyer's records over the Internet than it does to make a forensic copy of the hard drive on which those records are stored. The Working Group considered how the Law Society can carry out its mandate in the face of cloud computing, and how lawyers can meet their obligations to immediately provide records to the Law Society for copying during investigations.

ANALYSIS OF THE ISSUES

Jurisdictional Issues

Jurisdictional issues are central to any analysis of cloud computing.[12] In many cases the cloud services a lawyer in British Columbia will use will have its servers located in another jurisdiction. In some instances, the servers will be in multiple jurisdictions, either because the service provider has multi-jurisdictional operations or has subcontracted services to providers that operate in other jurisdictions. This makes it very difficult to ascertain where a user's data is located.[13]

There are several problems with lawyers having their business records stored or processed outside British Columbia. Lawyers have a professional obligation to safeguard clients' information to protect confidentiality and privilege. When a lawyer entrusts client information to a cloud provider the lawyer will often be subjecting clients' information to a foreign legal system. The foreign laws may have lower thresholds of protection than Canadian law with respect to accessing information. A lawyer must understand the risks (legal, political, etc.) of having client data stored and processed in foreign jurisdictions.

Because confidentiality and privilege are rights that lie with the client, the Working Group considered whether a lawyer should not unilaterally make a decision to subject the client's information to unreasonable risk of access. When a client retains a lawyer and provides the lawyer with personal information, it is unlikely the client has contemplated that the lawyer will be storing that information in a foreign jurisdiction. The proposed Due Diligence Checklist includes some recommended best practices for dealing with personal information.

Much has been made of the invasive powers of the USA PATRIOT Act and the risks associated with using cloud providers that have servers located in the United States or that are owned by corporations that are subject to US law. There are some that

---

[12] The challenges of jurisdiction are raised in most articles on cloud computing. See, for example, Gellman at fn. 6; ARMA International's hot topic, *Making the Jump to the Cloud? How to Manage Information Governance Challenges*, (2010); European Network and Information Security Agency, Cloud Computing: Benefits, risks and recommendations for Information Security (November 2009).

[13] Chantal Bernier, Assistant Privacy Commissioner of Canada, "Protecting Privacy During Investigations" (March 17, 2009).

downplay the risk associated with the PATRIOT Act on the basis that the chance of personal data being accessed is not high.[14] The Working Group observes that one cannot properly analyze risk by only looking at the likelihood of an event occurring. A proper risk analysis also requires tracking the magnitude of harm should the risk materialize. Because of the importance of solicitor and client confidentiality and privilege, any lawyer who is performing a risk analysis of using third parties to process and store data needs to consider both the likelihood of the clients' information being accessed and the potential consequences of that access.

The Working Group also notes that in the American context, the PATRIOT Act is only one issue. It is estimated that there are over 10,000 agencies in the United States that are able to access information stored with third parties by way of a subpoena without notice, rather than a warrant.[15] Cloud providers may also have servers in countries other than the United States. A proper risk analysis by a lawyer requires a broader analysis than merely looking at the PATRIOT Act.

Another jurisdictional issue the Working Group considered is the implication of extra-jurisdictional data storage/processing on the ability of the Law Society to carry out its regulatory functions. As a self-governing profession, lawyers are subject to regulatory oversight by the Law Society. The Law Society is required to consider every complaint against lawyers.[16] In some instances complaints lead to investigations that require the Law Society to access and copy a lawyer's records. Lawyers are required to comply with Law Society Orders for the production and copying of records. In circumstances where a lawyer refuses to comply, or where the records are held by a third party who refuses to comply, the Law Society would have to proceed by way of s. 37 of the *Legal Profession Act* to have the records seized. In the case of cloud computing, *seizure* of the records is not likely possible, so the Working Group recommends seeking an amendment to s. 37 that allows for the court to order copying records as an alternative. The purpose of such an amendment is for greater clarity. The Working Group believes that the self-governing capacity of the profession needs to be preserved and that technological evolutions do not negate the Law Society's regulatory authority any more than they extinguish legal rights and obligations. The challenge becomes finding a means by which lawyers may make use of new technology while still being able to comply with their professional responsibilities.

---

[14] See, for example, The Treasury Board of Canada, "Frequently Asked Questions: USA PATRIOT ACT Comprehensive Assessment Results" at http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp#Q3 (Accessed February 7, 2011).

[15] See the separate submissions of Albert Gidari, Partner, Perkins Coie LLP and James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology, to the Subcommittee on the Constitution, Civil Rights, and Civil Liberties (May 5, 2010), Hearing on Electronic Communications Privacy Act Reform.

[16] Law Society Rules, Rule 3-4. Rule 3-5 sets out the circumstances where complaints must be investigated, or where there is discretion.

With respect to the challenges of complying with regulatory and legal requirements, Jansen and Grance write:

> Use of an in-house computing center allows an organization to structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data. In contrast, a characteristic of many cloud computing services is that detailed information about the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can to some extent alleviate this issue, but they are not a panacea.[17]

The Working Group recognized that the Law Society regulates lawyers, not third party providers or their technology. Absent going to court, the Law Society does not have the statutory authority to compel cloud service providers to provide access to and copies of lawyers' business records. This required the Working Group to consider how access to records, including their timely preservation and copying could be achieved through the medium of lawyer regulation.

How the technology affects lawyers' ability to discharge their professional responsibilities

There are a number of technological issues associated with cloud computing. This report does not attempt to be exhaustive in this respect. As noted, the intention of the Working Group is that any rule reforms state principles in as technology-neutral a manner as possible. The Working Group considered technology issues through two principle lenses. The first was how the technology might affect lawyers' ability to discharge their professional responsibilities. The second was how the technology might affect the Law Society's ability to carry out its regulatory function.

There are several ways in which cloud computing affects lawyers' ability to discharge their professional responsibilities. A central issue is that Rule 3-68 of the Law Society Rules states:

> 3-68 (0.1) In this Rule, "records" means the records referred to in Rules 3-60 to 3-62.

---

[17] Footnote 4 at p. 14.

> (1) A lawyer must keep his or her records for as long as the records apply to money held in trust and, in any case, for at least 10 years.
>
> (2) A lawyer must keep his or her records at his or her chief place of practice in British Columbia for as long as the records apply to money held in trust and, in any case, for at least 3 years.
>
> (3) A lawyer must protect his or her records and the information contained in them by making reasonable security arrangements against all risks of loss, destruction and unauthorized access, use or disclosure.
>
> (4) A lawyer who loses custody or control of his or her records for any reasons must immediately notify the Executive Director in writing of all the relevant circumstances.

A lawyer who uses cloud computing for trust accounting purposes will likely be off-side this rule by virtue of where the records are stored. The Working Group observes that many lawyers using closed systems that their firm controls will also be off-side this rule by virtue of the requirement that the records be stored at the lawyer's chief place of practice. There are many good reasons to locate a firm's servers outside the chief place of practice, however. In fact, it might constitute a best practice in some instances from a data risk management perspective (cooling systems, fire protection, cost, data backup, etc.). In considering Rule 3-68 the Working Group analyzed whether the rule was a relic of a paper paradigm and considered what the essential elements of the rule should be by asking what the rule's purpose is.

The Working Group is of the view that the two critical issues are:

- The Law Society's ability to access and copy the required records in a timely manner; and
- Lawyers' ability to discharge their obligations under 3-68(3) and (4).

If the Law Society can access remotely stored records on demand, and those records are sufficient for the purposes of the audit and investigative function of the Law Society, does it matter if the records are stored at the "chief place of practice" or elsewhere in British Columbia? Record storage outside the jurisdiction raises operational issues, but the core question is whether the "chief place of practice" requirement remains defensible.

The "chief place of practice" requirement is called into question when records are stored remotely in electronic form. The critical question is whether the records are available on demand at the time of request and in a format acceptable to the Law Society. Essentially, for electronic records, the location the record is stored is less important than the ability of the lawyer to produce the record on demand in an

acceptable form. The Working Group recommends that the Act and Rules Subcommittee craft a provision for electronically stored records that reflects this reality. Electronic records should be capable of being stored outside the chief place of practice provided the lawyer can make the records available at the time of request in an acceptable format (eg. print or PDF). The "records" covered in Rule 3-68(1) should be retained for 10 years from the final accounting transaction on the file.

As a separate matter, the Working Group notes that it is possible to read Rule 3-68(2) to mean that the record must be stored from three years from when there is no longer money in trust, or alternatively for as long as money is held in trust and for at least three years. At some point the Act and Rules Subcommittee, as part of its general review of the Rules may wish to consider this issue.

The requirement that the records be stored in the chief place of practice exposes a logical problem with the rules. Rule 3-59(2) sets out the formats in which a lawyer must keep accounting records. Rule 3-59(2)(c) allows lawyers to keep accounting records in "an electronic form that can readily be transferred to printed form on demand." The chief place of practice requirement means that a lawyer who stores accounting records on a hard drive at his or her office, can meet the requirements of Rule 3-59 by printing a copy. A lawyer whose servers are located across town may have the technological capacity to print the records pursuant to Rule 3-59(2)(c) but could be off-side Rule 3-68(2). This is not easily defensible. While there are interpretation ambiguities (Rule 3-68 only applies to Rules 3-60 to 3-62) and practical challenges with remote storage, the key issue is whether the content of a print record is acceptable.

The Working Group believes that the chief place of practice requirement should be removed for electronic accounting records, and that the emphasis should be on the electronic accounting records being made available on demand in an acceptable format. While a paper record will be sufficient in some cases, in other cases it will not. The Working Group is of the view that the Law Society should have the discretion to require the metadata (or data that establishes a forensic accounting trail) associated with electronic records (including accounting records). While the authority to copy records under Rule 3-79 and 4-43 will include the authority to copy metadata, Rule 3-59(2)(c) fails to recognize that in some circumstances the Law Society may require more information than is contained in the print record.

The Working Group also heard from the Trust Regulation Department that Rule 3-68 should include reference to Rule 3-59, as the latter includes general accounting records that may be important to an investigation. The Working Group recommends making this change as it should be non-controversial.

Security

Rule 3-68(3) required the Working Group to consider what constitutes "reasonable security arrangements against all risks of loss, destruction and unauthorized access, use or disclosure."

In addition to the requirement in Rule 3-68(3), lawyers have the duty to protect client confidences. The *Professional Conduct Handbook*, Chapter 5 states:

1. A lawyer shall hold in strict confidence all information concerning the business and affairs of the client acquired in the course of the professional relationship, regardless of the nature of the source of the information or of the fact that others may share the knowledge, and shall not divulge any such information unless disclosure is expressly or impliedly authorized by the client, or is required by law or by a court.
2. A lawyer shall take all reasonable steps to ensure the privacy and safekeeping of a client's confidential information.
3. A lawyer shall not disclose the fact of having been consulted or retained by a person unless the nature of the matter requires such disclosure.
4. A lawyer shall preserve the client's secrets even after the termination of the retainer, whether or not differences have arisen between them.

Any time a lawyer entrusts a client's records to a third party, the obligations set out above may be put at risk. The requirement to take all reasonable steps to ensure the privacy and safekeeping of clients' confidential information supports the need for due diligence and contractual safeguards.

Security of records is a critical issue for a lawyer to resolve when choosing a third party service provider, including a cloud provider. There are too many variables with respect to security for the Working Group to make a blanket statement as to whether cloud computing is sufficiently secure. Jansen and Grance set out a useful list of security pros and cons of cloud computing.[18] As part of their due diligence, lawyers need to understand the security measures associated with the storage and processing of their records. This caution is not limited to the use of cloud providers.

A cloud can be public, private, community or hybrid.[19] Each of these models affects the degree of control the user has over the environment. In addition to this, there are vast differences in the resources of various providers and users. A large firm with a

[18] Footnote 4 at pp. 8-12.
[19] See Appendix 2.

dedicated IT staff may be able to create better data security by operating its systems in-house than a sole practitioner might be able to manage. The sole practitioner might experience a considerable security upgrade by having IT services managed by a specialist provider. These variables bring the issue back to the importance of due diligence on the part of the lawyer or law firm when it comes to managing its records and outsourcing services.

Because of the complex variables and case-by-case nature of security risk analysis, the Working Group did not feel it could assert that cloud computing is more safe or less safe than traditional computing. What is required is for individual lawyers and law firms to assess the security risks associated with their existing records management systems[20] as well as any new system they intend to use. As the Verizon Risk Report notes, networked data may be subject to more attacks but this does not necessarily correlate to a greater number of data breaches.[21] Insider attacks can have devastating consequences. Insider attacks can occur within a traditional firm as well as one that uses cloud computing, so lawyers should not assume that their records are necessarily more vulnerable when they are stored with a cloud provider. A consideration with respect to third party providers, however, is that lawyers do not vet the employees of the third party service providers they use. Having a better understanding of the security checks, access rights and restrictions the third party provider places on accessing the lawyers' business records is important. A data breach with a cloud provider could compromise vast amounts of client information, and lawyers need to take reasonable steps to guard against this risk. Trust is not a given when dealing with service providers.

"Custody or Control" of accounting records

The Working Group analyzed the requirement under Rule 3-68(4) that a lawyer who loses custody or control of his or her accounting records must immediately notify the Executive Director of the circumstances. In particular, the Working Group considered whether custody was lost when the records were stored on a third party system.

The Working Group considered whether the phrase "custody or control" should be synonymous with "possession" for the purpose of Rule 3-68(4). In some respects the interpretation challenge can be tied to the concept that the records in 3-68(4) would be considered to be paper records stored at the chief place of practice. Once one accepts that the records may be electronic, and the servers may be off-site, "custody or control" requires a different analysis.

The *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 has a "custody or control" requirement in s. 3(1). The Working Group discussed Order 02-30, which dealt with a situation where the University of Victoria had an arrangement to

---

[20] "Records management" is used here to include storage, processing, retention and access.
[21] Footnote 7. This may change as more data moved to cloud systems.

store records for the separate entity, the University of Victoria Foundation. The Foundation was not a public body and therefore its records did not fall under the scope of the Act. The University is a public body, so if the records could be found to be under the custody or control of the University, an access application could be made for the records pursuant to s. 3(1).

While decisions of the Privacy Commissioner are not binding on the Benchers for the purpose of interpreting Rule 3-68, they can be informative. Order 02-30 can be used to support a line of argument that the mere fact records are stored with a third party would not always mean that the lawyer has lost custody of them. It would seem to depend on what the third party is able to do with the records, what their responsibilities are regarding the documents, and how the documents are integrated into other records systems would also affect things. In the context of cloud computing this could be used to argue that the terms of service are critical to the issue of custody. It could also be used to argue that a private cloud better supports the concept of custody by the lawyer than a public cloud where the storage is commingled with other records. However, the requirement that the cloud provider secure the documents suggests responsibility for their "safekeeping, care, protection, or preservation"[22] and therefore custody might lie with the cloud provider.

The Working Group is of the view that provided a lawyer ensures through contractual safeguards that custody or control of his or her records does not pass to a third party, that the lawyer can use a third party for the storage or processing of those records. If the lawyer is unable to access those records and provide them on demand during a compliance audit or Law Society investigation, however, the lawyer may be found to have lost custody or control of the records.

Records Retention

Lawyers have record retention obligations. Some of these obligations are driven by limitation periods, which will mean that different files have to be retained for different periods of time. Given how digital data is stored, particularly in a cloud system, the issues associated with retaining "a file" can be complex and lawyers need to turn their minds to how they can meet these requirements.

Rule 3-68 establishes a series of retention requirements for trust accounting files. A review of that rule demonstrates that a lawyer may have retention obligations of 10 years or more with respect to trust records. In addition to retention obligations for trust records, there is the issue of malpractice claims. The Law Society guidelines for file

[22] See Order 02-30, paragraph 23.

destruction,[23] set in consultation with the Lawyers Insurance Fund, help ensure that a lawyer's file still exists when a negligence claim or potential claim is made. The Working Group discussed this issue with the Lawyers Insurance Fund, as noted later in this report.

Another example of the need for proper records management flows from the *Professional Conduct Handbook*, Chapter 10, Rule 8:

> 8. Upon withdrawal, the lawyer must immediately:
> (e) take all reasonable steps to assist in the transfer of the client's file.

If the lawyer does not have a good practice management system in place, particularly when the lawyer is using third party data storage for electronic records, transferring the client file in a timely and complete manner may prove difficult.

Records management is a complex enterprise in a paper world. In the digital world there are greater complexities. In simple terms, records management in the digital world is complicated by the ease with which the records can be copied and disseminated, evolutions in hardware and software can make archived data inaccessible, and spoliation of digital data can occur.[24] A complete analysis of digital records management is beyond the scope of this report. However, lawyers are required to understand how to manage their records (regardless of the storage medium) to ensure they are meeting their records keeping obligations

Records management can be complicated when dealing with cloud providers. Many commentators have asked the question, what happens if the cloud provider goes bankrupt or ceases to operate?[25] Data back-up and escrow agreements might be insufficient safeguards without access to the application software necessary to decode the stored data. In addition, do the cloud providers maintain the data for the period of time a lawyer is required to retain it? What assurances can the cloud provider give that the data will be available in a comprehensible form on request by the lawyer or the Law Society?[26] How will a lawyer know that data that is supposed to have been destroyed, has been destroyed?

The Working Group is of the view that lawyers cannot assume that their business records will be properly archived and maintained by a third party service provider, whether operating a cloud service or otherwise. Lawyers have a positive obligation to

---

[23] Law Society of British Columbia, "Closed Files: Retention and Disposition", at http://www.lawsociety.bc.ca/page.cfm?cid=2001&t=Client-Files (last accessed: June 2, 2011).
[24] A good starting point for understanding these issues is The Library of Congress, Digital Preservation: http://www.digitalpreservation.gov/.
[25] Jansen and Grance, fn. 4, Gellman fn. 6 at p. 16.
[26] For example, the Law Society might be named the custodian of the practice by the court, thereby stepping into the shoes of the lawyer or firm to operate the practice.

ensure proper records management systems are in place. This obligation extends to ensuring that any third party record storage provider is keeping the data archived in an accessible format, available on demand. This includes having a means to audit compliance.

How the technology affects the Law Society's ability to carry out its regulatory function

Cloud computing technology can have serious implications for regulatory bodies.[27] As discussed, the jurisdictional component is part of the challenge. Regulatory bodies have limited jurisdictional reach, and when records are stored and processed outside the geographical reach of the regulatory body, and by third parties who are not subject to regulation, the regulatory authority can be challenged.

The effect of the jurisdictional limitation is such that, in order to carry out certain essential investigatory functions, an organization like the Law Society would have to seek a court order and then have that court order enforced in a foreign jurisdiction. This introduces delay, increased cost, and uncertainty into the regulatory process. These challenges can adversely affect the public perception of the legal profession's capacity to self-regulate in the public interest. The increased costs would ultimately be borne by the profession as a whole in the form of higher fees. Ironically, these higher fees could off-set some of the cost savings realized through the adoption of cloud computing.

In addition to jurisdictional challenges, the technology can impact the regulatory function. The Law Society has the authority to copy records, including computer records. When a lawyer is faced with an order allowing the Law Society to copy records, the lawyer must *immediately* produce the records and make them available for copying.[28] When the records are stored on cloud services, a lawyer's ability to comply with these rules can be affected as can the Law Society's ability to copy the records.

With paper records, the Law Society can easily make copies. With records stored on hard drives, the Law Society has rules that allow it to make forensic copies of the hard drive. In the latter case, the Law Society also has established a process by which personal information that is not relevant to the investigation can be protected so the Law Society is not accessing it. When the records necessary for an investigation are stored on third party servers the ability of the Law Society to copy those records is compromised.

In order to access the records, the Law Society would require the lawyer to provide the password and information necessary to locate the records. An unscrupulous lawyer

---

[27] See Gellman fn. 6 at 22, Bernier fn. 13 re forensic investigations.
[28] Law Society Rules, Rule 4-43 and 3-79.

would have a much easier time hiding records in the cloud than on a hard drive in his or her office. But even if the Law Society has access to the records, the ability to copy the records may be challenged. If the cloud uses proprietary software, any copy of the information will need access to that application software in order to render the copied information comprehensible.[29] Some cloud providers may provide data copies to users who are migrating data from the cloud, but this will often be in a flat file format such as an Excel spreadsheet. The consequence of this is that relational data that can be important to an investigation will be lost.[30] With a forensic copy of a hard drive the Law Society's forensic expert can testify as to the authenticity of the record at the time the copy was made. With copying data from the cloud, the forensic expert cannot make that claim because, amongst other reasons, the act of copying the logical file alters the data (as opposed to copying the physical file when making a forensic copy). This has implications for evidentiary standards.

The Working Group discussed the forensic copying issues with the Law Society's external computer consultant, the Trust Regulation staff and the Practice Management Advisor. While it would be possible to make a logical file copy by accessing the cloud, a physical copy could not be made. Metadata would be lost, as would the ability of the expert to testify that the record had not been altered. The Working Group considered that metadata is a record that the Law Society is entitled to collect. Metadata has proven to be an important part of some investigations.

The Working Group discussed the possibility that the adoption of cloud computing would revert the investigatory process back to the days of paper records in some respects. This was a challenging part of the analysis. On the one hand, an argument can be made that no investigatory process is perfect and that the Law Society used to be able to investigate lawyers before there was metadata. On the other hand, technology now allows for metadata to be part of the investigation, assisting investigators in proving that a lawyer has fraudulently altered records after the fact. In some respects eliminating the use of new investigatory technology would be like asking the police to stop using radar guns to catch speeding drivers.

The Working Group believes it is essential that the third party service providers lawyers use for electronic data processing and storage are able to provide the Law Society records that include metadata. At the very least the rules should provide the Law Society the discretion to require that metadata, or authenticated forensic investigation data that meets the evidentiary standards for electronic disclosure before a superior court, be provided on demand. It is the lawyer's responsibility to ensure the services he or she uses supports Law Society investigations and audits.[31]

---

[29] David Bilinsky and Matt Kenser, Introduction to Cloud Computing (ABA TechShow 2010).
[30] This relational data could include creation and modification dates for documents.
[31] "Demand" in this case would be subject to the proper process, such as a 4-43 order. This would also allow the standard to evolve over time to keep pace with best practices.

The Working Group recognizes that the potential exists that the Law Society will have to copy records held by third party service providers in a manner that does not, at present, constitute best evidence. This is because data stored on the cloud may be located in many locations and the Law Society will not be able to make forensic copies of the servers the data is stored on. Lawyers should not be allowed to use a technology that prevents the Law Society from obtaining forensic copies of electronic records and then claim the copied records fall short of the best evidence standard. As such, the Working Group recommends that a rule be created that would allow the Law Society to rely on the copied record as being best evidence and place the onus on the lawyer to provide the forensic copy if the lawyer wishes to present "better evidence". This rule should be limited to circumstances where the Law Society is unable to make a forensic copy of the devices on which the records are stored because the Law Society is either unable to locate or access the storage devices to make a forensic copy.

Potential impact on Rule 4-43

Following the report of the Mirror Imaging Task Force in 2008, the Law Society revised Rule 4-43 to create a process to protect personal information. The balance that was sought recognized that the Law Society has the authority to copy computer records and investigate lawyers, but the process of making a forensic copy of computer records can capture irrelevant personal information. In light of this, the Law Society created a process to allow irrelevant personal information to be identified and segregated, so it was not accessed by the Law Society. Cloud computing creates a situation where that process might not be able to be followed.

The reason that the 4-43 process for segregating personal information might not be able to be followed with cloud computing is that it is unlikely that the Law Society will be able to make forensic copies of the servers that store a lawyer's records. The copying process will be different. This may mean that the Law Society will end up copying and accessing records that contain irrelevant personal information. The Working Group is of the view that this is a risk the lawyer bears by choosing to use cloud computing. It is not an excuse to refuse to comply with a Law Society investigation.

While it will be important for the Law Society to take reasonable efforts not to access irrelevant personal information stored with a cloud provider during the course of an investigation, the level of protection contemplated under 4-43 may be impossible to meet. As such, the Working Group recommends rule 4-43 be amended to recognize the process for protecting personal information during investigations is subject to the lawyer using a record keeping system that supports such a process. If the lawyer uses a system that prohibits the Law Society from segregating such information in a practical manner, the lawyer does so at his or her own risk that such information may be inadvertently accessed during the investigation.

Ensuring Authorized Access to Records

The concept of records being stored and processed outside of British Columbia presents conceptual challenges to some of the operational processes of the Law Society. One area of particular concern is custodianships. In circumstances where a lawyer has died or become incapable of carrying on his or her practice, the Law Society will obtain an order of the court that empowers the Law Society to step in as custodian of that lawyer's practice. This essentially puts the Law Society in the shoes of the lawyer, and the Law Society may use the lawyer's records for the purpose of carrying on the practice, and may also engage in an investigation of the records.[32]

If a lawyer uses cloud computing and a custodian is appointed, the Law Society faces the possibility of arriving at an office that has no records and no evidentiary trail as to where those records are located. This creates risk to the public.

In addition to custodianships, there can be circumstances where a lawyer refuses to comply with a Law Society investigation, such as a 4-43 order or a 3-79 compliance audit. When the records are not available for copying because they cannot be located, this creates risk to the public. In these instances the Law Society has processes to suspend the lawyer, but that does not solve the problem of not possessing records that may be important for protecting the public interest.

The Working Group discussed potential solutions to these risks. However, because the likelihood and consequences of these risks are difficult to predict, the Working Group preferred monitoring the development of lawyers using this technology to see whether further steps are required by the Law Society. **Appendix 3** highlights some concepts the Working Group briefly canvassed. These concepts do not form part of the recommendations in this report. Rather, they are concepts that might merit consideration in the future should the recommendations in this report prove inadequate for protecting the public interest. If the concepts set out in Appendix 3 are considered in the future, they would have to be analyzed fully to consider both the operational appropriateness and feasibility of the concepts, as well as the general appropriateness of the concepts.

Lawyers Insurance Fund Issues

Cloud computing could result in file material that is either unavailable, or available only through a court order, if stored in a foreign jurisdiction. The Working Group asked the Lawyers Insurance Fund how these problems might impact its ability to manage claims.

---

[32] See the *Legal Profession Act*, Part 6, and the Law Society Rules, Part 6.

The Lawyers Insurance Fund noted that a lack of file material, regardless of the reason, could compromise its ability to investigate and defend a claim, as well as its ability to compensate victims of lawyer theft (if the Law Society's ability to discover thefts was impaired). Cloud computing might also result in some additional costs being incurred if a court order in a foreign jurisdiction was required in order to access records. However, assuming that lawyers take reasonable steps to safeguard against lost data in terms of third party storage and processing of records, the risk will be minimal.

The Lawyers Insurance Fund also provided some general observations. They agreed with the concept that lawyers should be required to meet records retention obligations while using cloud computing or other emerging technologies. As noted, the Law Society has set guidelines for file destruction that the Lawyers Insurance Fund has helped establish, and adherence to these guidelines will help ensure that a file still exists when a negligence claim is made.

They also noted that lawyers' use of technology, including cloud computing, creates other risks such as data breaches. If a lawyer or client suffers a loss as a result, these are not losses arising out of the lawyer's negligent provision of legal services and are not covered by the professional liability insurance policy. Because of this, lawyers will want to consider how best to manage these risks. Steps might include:

- Obtaining informed client consent for the use of the services;
- Requiring the service provider to indemnify the lawyer for any claims the lawyer faces as a result of using the service; and
- Buying insurance on the commercial market to cover risks such as data breaches.

The Working Group encourages lawyers to consider the risks highlighted by the Lawyers Insurance Fund as part of the due diligence and risk management lawyers should perform when determining whether to use third party data storage and processing.

CONCLUSION

Technological change occurs at a breakneck pace. This creates challenges for law-makers and regulatory bodies, but it also presents challenges for professionals who are required to adhere to codes of conduct. When considering the topic of cloud computing, the Working Group rejected the knee-jerk reaction to prevent lawyers from using the technology because it introduces risks and challenges. All technology and business models present risks and challenges. In addition, the Working Group is of the view that the proper role of the Law Society is to regulate lawyers, not attempt to regulate technology. What this means is that lawyers should be allowed to use emerging technologies, provided the lawyer is able to comply with his or her professional responsibilities while using the technology. Cloud computing is no

different. It is for this reason that the Working Group did not attempt to set up regulatory models that are contingent on the type of cloud service that is being used.

The challenge for lawyers becomes understanding the risks associated with the technology or service they are using. This can be a daunting task, particularly if there are barriers to keeping pace with technological change. In some cases generational differences will make the adoption and understanding of new technology a challenge, in other cases the lawyer will lack the resources to stay on top of technological issues. Despite these challenges, lawyers still have professional and legal duties that they owe to their clients, disclosure requirements in litigation, and obligations owed to their regulator. These duties do not disappear in the face of new technology. Rather, it is the lawyer's responsibility to ensure their use of technology and business models comply with these obligations. Failure to do so may lead to serious legal and regulatory consequences, including revocation or suspension of the lawyer's licence to practice law.

There are some instances where a set of rules has become archaic or unworkable, and in those cases it is proper for the law-maker or regulator to consider the policy behind the rules and to modernize the rules. Some suggestions have been made in this report to accomplish that objective. In other instances the underlying obligation is of such central importance that the rules should not be weakened in order to facilitate the use of new technology. A lawyer's obligation to protect confidential and privileged information is an example of the latter. The professional obligations a lawyer has does not preclude the lawyer from using emerging technology; rather, it requires the lawyer to take steps to ensure he or she can use the technology in a manner that is consistent with his or her professional obligations.

The Working Group believes that the proper approach for dealing with lawyers using third party storage and processing of records, including cloud computing, is to provide lawyers due diligence guidelines and best practices. The purpose of the document is to assist lawyers in using records storage and processing services in a manner that is consistent with the lawyer's professional obligations. The responsibility of choosing an adequate service provider lies with the lawyer, as does the risk. Lawyers should ensure their contract of services address these issues.

In addition to creating due diligence guidelines and best practices, the Working Group also makes a series of recommendations to modernize the Law Society Rules to deal with the challenges cloud computing presents to the Law Society as regulator. These recommendations reflect an effort to allow lawyers to use a promising technology to deliver legal services, while ensuring proper safeguards exist to protect the public. These recommendations may need to be amended in the future and it is important that the Law Society monitor how this technology affects lawyers' ability to meet their professional obligations. Experience will tell whether the public is sufficiently protected or if further steps are required.

RECOMMENDATIONS

Recommendation 1: The Law Society should adopt and publish the attached due diligence guidelines for lawyers using third party electronic data storage and processing (see **Appendix 1**).

Recommendation 2: In order to ensure the Law Society's regulatory process keeps pace with evolutions in data storage and processing technology, and to ensure the audit process remains robust, the Act and Rules Subcommittee should draft rules that capture the following concepts:

1. Rule 3-68(0.1) should include reference to Rule 3-59 in order to facilitate the Trust Regulation Department auditing and investigation of accounting records;
2. Rule 3-68 should be amended to remove reference to the "chief place of practice" requirement with respect to electronic records, and instead should require that electronic records be made available at the time of request in a format acceptable to the Law Society (the Law Society should publish guidelines as to what the Trust Regulation Department requires as an acceptable format);
3. The general retention period in Rule 3-68(1) should be 10 years from the final accounting transaction;
4. There should be a general rule regarding records in electronic form that gives the Law Society the discretion to accept copies of those electronic records in paper or another form;
5. There should be a general rule regarding records in electronic form that the Law Society has the discretion to require the lawyer to provide the meta data associated with those records;
6. There should be a general rule that requires lawyers to ensure their electronic records are capable of meeting the prevailing electronic discovery standards of a British Columbia superior court;
7. The Act and Rules Subcommittee should determine how to incorporate the following trust rule requirements:
    (a) If monthly reconciliations are prepared and stored electronically, the reconciliation must show the date it was completed. Each of the monthly reconciliations must be available with appropriate back up documentation and not overwritten by the system.

    (b) If billing records are stored electronically, they must include the creation date as well as any modification dates.

    (c) All accounting records 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 final accounting transaction. If the

member scans all his supporting documentation such as 3rd party documents like bank statements the full version meaning all the pages front and back even if there it is blank page.

(d) A sufficient "audit trail" must be available and printable on demand in a comprehensible format (this should be a requirement of all accounting software whether it's in the cloud or a stand-alone program such as ESILAW or PCLAW etc.).

(e) Audit trail transaction reports must be complete, showing all postings into the software with specifically assigned transactions that correspond chronologically with dates etc.

(f) Cash receipts must always be retained in hard copy.

(g) Ability of system to provide creation dates, what changes were made, and how often the documents (i.e. Word, Excel and/or Adobe) were changed. Ensuring that metadata information is not lost when stored on a cloud.

(h) Ability for LSBC to have view only access & printing access to all items stored on cloud (I.e. emails, documents, accounting records) when required. This does not derogate from any rule that allows the Law Society to copy a record or have that record provided on request. The purpose is to allow for a forensic investigation that does not alter the underlying record.

8. There should be a rule that recognizes, in circumstances where the Law Society has had to copy electronic records held by a third party, the Law Society may rely on the copies as best evidence and the onus is on the lawyer to provide a forensic copy of those records if the lawyer wishes to dispute the quality of the evidence.
9. The Act and Rules Subcommittee should consider, as part of future revisions to the *Legal Profession Act,* amending s. 37 to permit orders for copying or duplication of records, as an alternative to "seizing" records.

Recommendation 3: For the purposes of interpreting Rule 3-68(4), and subject to the other recommendations in this report, if a lawyer ensures through contractual safeguards that custody or control of his or her records does not pass to a third party, the lawyer can use a third party for the storage or processing of those records. If the lawyer is unable to access those records and provide them on demand during an audit or Law Society investigation, however, the lawyer may be found to have lost custody or control of the records, which may lead to disciplinary consequences.

Recommendation 4: In circumstances where the Law Society Rules require a lawyer to either provide the Law Society the lawyer's records or make copies of the records available to the Law Society, and the lawyer either refuses to comply, or is unable to comply by virtue of having used a service provider that does not make the records available in a timely fashion, the lawyer should be suspended until such time as the lawyer complies with the disclosure requirements under the Law Society Rules. The Act and Rules Subcommittee should consider whether this requires creating a new administrative suspension rule, or proceeding by way of Rule 3-7.1. In circumstances where the lawyer is suspended, the Law Society should consider seeking a court order for a custodianship in order to protect the public and ensure the suspended lawyer's clients continue to be served.

Recommendation 5: The Law Society should encourage the CBA BC Branch and CLE BC to include as part of future courses on cloud computing (or similar technology), information about the best practices and Law Society Rules.

Recommendation 6: The Ethics Committee should review its ethics opinions regarding the use of third party service providers and update them to address the concerns arising from the use of cloud computing, or similar technology.

Recommendation 7: Law Schools and PLTC should teach students that lawyers' have an obligation to ensure their use of technology is consistent with their professional obligations.

Recommendation 8: The Law Society's Trust Regulation Department, and the Professional Conduct and Investigation Department, when dealing with investigations involving a lawyer who uses cloud computing, should identify circumstances in which the approach proposed in this report is failing to protect the public interest, in the event modifications to the policy and rules is necessary for the Law Society to fulfill its public interest mandate. Because technology will continue to develop, and standards will emerge, it is important to ensure the Law Society keeps pace with these changes, and staff will play an important role in keeping the Benchers apprised of the potential need for amendments to the policies and rules recommended in this report.

Recommendation 9: The Practice Advice group should modify their resources to reflect the recommendations in this report. This may involve creating checklists to better assist lawyers.

Recommendation 10: Because cloud computing is an emerging technology, the Law Society should ascertain whether any lawyers who use cloud computing are willing to have the Trust Assurance Department determine whether their system meets the present requirements, and the investigators determine whether the system meets the requirement for a 4-43 investigation. This would not be for the purpose of endorsing a

particular system. It would be for the purpose of identifying any concerns to ensure the Law Society's auditing program can address cloud computing.

Recommendation 11: Because cloud computing stores records in a manner where the Law Society may not be able to make forensic copies of hard drives, or segregate irrelevant personal information that is stored in the cloud, Rule 4-43 should be amended to make it clear that the process for protecting personal information during investigations is subject to the lawyer using a record keeping system that supports such a process. If lawyers choose to use systems that do not support that process, they do so at their own risk, and the Law Society may end up having to collect or access personal information that is irrelevant to an investigation.

ACKNOWLEDGEMENTS

The working group is grateful for the input it received on a range of legal, technical, investigative and accounting matters from external consultant Doug Arnold, and Lorene Novakowski of Fasken Martineau; and from Law Society staff: David Bilinsky, Andrea Chan, Felicia Ciolfitto, Danielle Guglielmucci, Graeme Keirstead, Karen Keating, Nancy Lee, Michael Lucas, David McCartney, Doug Munro, Liza Szabo; and from Margrett George in the Lawyers Insurance Fund.

APPENDIX 1

DUE DILIGENCE CHECKLIST[33]

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.[34]

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 CHECKLIST

- 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.

---

[33] 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)

[34] 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;

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;

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.[35] 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 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

[35] FIPPA, Section 30.1.

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;[36]

- 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;[37]

- 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:[38]

    - 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:[39]

    - Of the way to obtain access to written information about the lawyer's policies and practices regarding service providers outside Canada; and

[36] See PIPEDA Case Summary No. 313.
[37] See s. 4.8 of Schedule A of PIPEDA.
[38] AB PIPA, s. 6(2).
[39] AB PIPA, ss. 13.1(1) and (2).

    - 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.

APPENDIX 2 - Definition of Cloud Computing.

Source: National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145 (Draft), Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing (Draft),* January 2011.

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.
>
> Essential Characteristics:
>
> *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
>
> *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).
>
> *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
>
> *Rapid elasticity.* Capabilities can be rapidly and elastically released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
>
> *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability [fn omitted] at some level of abstraction appropriate to the type of services (e.g., storage,

processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application of hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

APPENDIX 3

The material in Appendix 3 represents three concepts that the Working Group discussed, but did not resolve. The concepts arose out of a recognition that in some instances, such as a custodianship, the Law Society will require access to a lawyer's records and the use of cloud computing might create impediments to such access. At this point, however, the Working Group does not believe these concepts merit recommendation. The concepts may prove unnecessary, and in any event there are operational and policy considerations that would have to be worked through to determine whether any of the concepts is appropriate or necessary. To undertake that analysis at this point seemed disproportionate to the potential risk. Experience will determine whether these concepts, or other concepts, require consideration in the future. This appendix is included for greater disclosure of the Working Group's analytical process, and does not constitute a recommended course of action.

Potential Solution #1: Requiring lawyers to use a password manager and provide the master password

One option the Working Group discussed was to require lawyers who use cloud computing to use a password manager and to provide the Law Society the password for the password manager. How this would work is that the password manager would store all the passwords for the services the lawyer was using. The Law Society would have the password to that repository. In the example of a custodianship, the Law Society would use the password to the password manager to access the passwords for the various services the lawyer used. This would allow the Law Society to identify the services being used and review the lawyer's records and carry on the practice.

In discussing this concept, the Working Group was cognizant that such a rule would place a considerable amount of power in the Law Society's hands. With the password to the password manager, the Law Society could access all of a lawyer's records. Doing so would obviously be inappropriate save as allowed by law. As such, any consideration of such a model would require a process to ensure due process was followed. For example, it might require a custodian order or a finding by a hearing panel that the lawyer had failed to comply with a Rule 4-43 order. In addition to a due process, it would also require robust security measures on the part of the Law Society. The Society would have to establish a system that protected the passwords from being improperly accessed. The Working Group considered that any such system should also have an audit function, and be subject to an annual reporting requirement to indicate the number of times it was accessed and following which due process.

Potential Solution #2: Requiring lawyers to enter into three party contracts with the Law Society and the Service Provider

Another option the Working Group considered was requiring lawyers to enter into three-party contracts with the Law Society and any cloud provider. The contract would include a requirement for the cloud provider to provide the Law Society access to the records. This would, again, be subject to due process such as a custodian order or a hearing panel decision. The Working Group understands that a three-party contract is similar to the approach of the Chambre des Notaries du Quebéc.

The three-party contract held a certain amount of appeal to the Working Group compared to the password manager concept, particularly because the Law Society does not become a repository of critical information like passwords. However, lawyers may use many cloud providers and these relationships can spring up quite suddenly; they are not like entering a lease for office space. As such, the lawyer may be in an *ad hoc* process of entering into contracts and getting the Law Society involved. This is administratively burdensome. In addition, it is likely that the larger cloud providers (eg. Amazon, Google, IBM, etc.) would not enter into such contracts.

Potential Solution #3: **Creating a Law Society "cloud" for lawyers**

Another option that the Working Group discussed was the idea of the Law Society operating a cloud service dedicated for lawyers. The Working Group did little more than sketch out the concept, as it would require an operational analysis that is beyond the scope of the Working Group.

The idea of a dedicated cloud service for lawyers, operated by the Law Society has some merit. It would allow for the service to be located in British Columbia, thereby eliminating the jurisdictional concerns. One possibility the Working Group considered was a federal cloud for lawyers, operated cooperatively by the law societies throughout Canada. This might allow for the servers to be located in jurisdictions other than British Columbia, while still avoiding some of the concerns arising from data storage in foreign jurisdictions.

If the concept of a law society operated cloud, dedicated for lawyers, is to be considered in earnest, it would be important to create a business structure that was independent from the regulatory branch of the Law Society. The Working Group recognized that the Law Society's investigatory function requires due process to access a lawyer's records, and if the Law Society were operating a cloud service it would have to create proper safeguards to ensure Law Society staff were unable to access the records stored on the service unless proper process had first been followed (eg. A 4-43 order, a custodian order, etc.).

The idea of a Law Society run cloud service would not be a quick solution to the challenges associated with cloud computing, but if the technology proves to be such that the Law Society's ability to protect the public is compromised because it cannot carry out its investigatory functions in the face of cloud computing, the idea might require serious consideration in the future. Cloud computing does not provide a safe harbor from regulatory oversight.

The three "potential solutions" needn't be viewed as mutually exclusive options. Some combination of the three might provide workable solutions. Any future consideration of these concepts would require an analysis of the operational feasibility and appropriateness of the concepts.

SELECTED BIBLIOGRAPY

Law Society of British Columbia Resources:
Legal Profession Act, S.B.C. 1998, c. 9

Law Society Rules

Annotated Professional Conduct Handbook

Ethics Committee opinions:

- March 2001, item 7 *Off-site and independent contractors working for law firms*
- December 1995 items 5 & 6 *Shared office space with non-lawyer / non-lawyer mediator*
- April 1998, item 7 *Advice to the profession regarding transmission of confidential information over the internet*
- March 2005, item 4 *Whether proper for a lawyer to entrust certain matters involving the practice of law to contractor*

Mirror Imaging Working Group, *Forensic Copying of Computer Records by the Law Society* (October 2009).

External Resources (Legislation and Case Law):

Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165

Personal Information Protection Act, S.B.C. 2003, c. 63

Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5

Personal Information Protection Act, SA 2003, c P-6.5

Lawson v. Accusearch Inc. [2007] 4 F.C.R. 314

External Resources (Articles, Reports, Opinion Pieces):

American Bar Association Commission on Ethics 20/20 Working Group on the Implications of New Technologies, *For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology* (September 20, 2010)

American Bar Association Commission on Ethics 20/20 Initial Draft Proposals – Technology and Confidentiality (May 2, 2011)

ARMA International's hot topic, *Making the Jump to the Cloud? How to Manage Information Governance Challenges*, (2010)

David Bilinsky and Matt Kenser, *Introduction to Cloud Computing* (ABA TechShow 2010)

CNW Group, *Award winner's breakthrough efforts reveal how technology can lock-in privacy: Commissioner Ann Cavoukian* (Canada Newswire July 22, 2010).

Robert J.C. Deane, BLG Seminar, *Cloud Computing – Privacy and Litigation Discovery Issues* (2011).

Adam Dodek, *Solicitor-Client Privilege in Canada, Challenges for the 21st Century* (CBA Discussion Paper: February 2011)

Electronic Privacy Information Center, "Complaint [re: Google, Inc. and Cloud Computing Services] and Request for Injunction, Request for Investigation and for Other Relief" before the Federal Trade Commission (March 17, 2009)

European Network and Information Security Agency, *Cloud Computing: Benefits, risks and recommendations for Information Security* (November 2009)

Robert Gellman, World Privacy Forum, "Privacy in the Clouds: *Risks to Privacy and Confidentiality from Cloud Computing*", (February 23, 2009)

Peter Mell and Timothy Grance, NIST Definition of Cloud Computing, Version 15, 10-7-09

Wayne Jansen and Timothy Grance, NIST *Guidelines on Security and Privacy in Public Cloud Computing* (Draft Special Publication 800-144: January 2011)

Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas, NIST *Draft Cloud Computing Synopsis and Recommendations,* NIST Special Publication 800-146.

Rick Klumpenhauer and Curt Campbell, "A Detailed Analysis of Archival Functions and Business Processes for Digital Preservation" Cenera Final Report, 2008.

Legislative Assembly of the Province of British Columbia, *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (May 2010)

Law Society of England and Wales, Law Society Gazette, *In Business: Cloud Computing* (March 2010)

NEC Company, Ltd, and Information and Privacy Commissioner, Ontario, Canada, *Modeling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach,* (May 2010)

Jack Newton, "Putting Your Practice in the Cloud: A Pre-Flight Checklist" (Texas Bar Journal, Vol. 73, No. 8: September 2010) (p. 632)

North Carolina State Bar Proposed 2010 Formal Ethics Opinion 7, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*

North Carolina State Bar Proposed 2011 Formal Ethics Opinion 6, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property* (April 21, 2011)

Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (January 2009)

Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing* (March 29, 2010)

Office of the Privacy Commissioner of Canada, Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing (May 2011)

Chantal Bernier, Assistant Privacy Commissioner of Canada, "Protecting Privacy During Investigations" (March 17, 2009).

Richard C. Owens and Francois van Vuuren, Canadian Privacy Law Review, Vol. 4 No. 10&11 (July/August 2007)

Queen Mary University, Cloud Legal Project: http://www.cloudlegal.ccls.qmul.ac.uk/

Bruce Schneier, "Be careful when you come to put your trust in the clouds" (The Guardian: June 4, 2009).

United States, Senate Judiciary Committee hearing "The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age" (September 22, 2010):

- Statement of James A. Baker, Associate Deputy Attorney General, United States Department of Justice
- Statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology
- Written Testimony of Jamil N. Jaffer
- Testimony of Cameron F. Kerry, General Counsel, United States Department of Commerce
- Statement of Brad Smith, General Counsel, Microsoft Corporation

United States Congress Subcommittee on the Constitution, Civil Rights, and Civil Liberties (May 5, 2010), Hearing on *Electronic Communications Privacy Act* Reform:

- Submission of Albert Gidari, Partner, Perkins Coie LLP
- Submission of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology

The Verizon Business Risk Team, "2008 Data Breach Investigations Report"

Gary J. Wise, *Lawyers in "The Cloud" A Cautionary Tale* (presented at Security for Lawyers in a wired World, October 16, 2009)

David C. Wyld and Robert Maurin, for the IBM Center for the Business of Government, *Moving to the Cloud: An Introduction to Cloud Computing in Government* (2009)