INFORMATIONLAWGROUP
privacy. security. technology. intellectual property.

Info Law Group

Posted at 2:17 PM on October 19, 2010 by Tanya Forsheit

Legal Implications of Cloud Computing -- Part Five (Ethics or Why All Lawyers-Not Just Technogeek Lawyers Like Me-Should Care About Data Security)

So, you thought our cloud series was over? Wishful thinking. It is time to talk about ethics. Yes, ethics. Historically, lawyers and technologists lived in different worlds. The lawyers were over here, and IT was over there. Well, maybe not just historically. As recently as last year, I attended an ediscovery CLE where a trial lawyer announced to the audience of litigators, with great emphasis, that they would have to start talking to the "geeks" and understanding technology in order to competently handle ediscovery in almost any commercial litigation. This made the audience laugh. I have found myself on conference calls with seasoned litigators who claim that ediscovery is not their area of practice. As a more general matter, I find that lawyers believe that they do not need to concern themselves with security controls for protecting sensitive information because they are already subject to existing ethics rules and standards governing the protection of privileged information. In the meantime, lawyers everywhere, particularly solo practitioners, are singing the virtues of cloud computing solutions for case management and are casually storing client data - often unencrypted - with a third party.

Here's the reality: Technology - whether we are talking cloud computing, ediscovery or data security generally - IS very much the business of lawyers. This is true both from a legal ethics point of view and from a best practices data security point of view. The issue of ethics and the use of cloud by lawyers is not new - I recommend this piece by Jeremy Feinberg and Maura Grossman and this blog post by E. Michael Power. A few State Bar associations have opined on the subject of lawyer use of cloud computing and other technologies. This blog post does not purport to cover that entire universe. Instead, this post focuses on three recent documents, ranging from formal opinions to draft issue papers, issued by three very prominent Bar associations -- the American Bar Association (ABA), the New York State Bar Association (NYSBA), and the State Bar of California (CA Bar). These opinions and papers all drive home the following points: as succinctly stated by the ABA, **"[l]awyers must take reasonable precautions to ensure that their clients' confidential information remains secure"**; AND lawyers must keep themselves educated on changes in technology and in the law relating to technology. The question, as always, is what is "reasonable"? Also, what role *should* Bar associations play in providing guidelines/best practices and/or mandating compliance with particular data security rules? Technology, and lawyer use of technology, is evolving at a pace that no Bar association can hope to meet. **At the end of the day, do the realities of the modern business world render moot any effort by the Bar(s) to provide guidance or impose restrictions? Read on and tell us - and the ABA - what you think.**

The ABA Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology

On September 20, 2010, the ABA Commission on Ethics 20/20 Working Group on the Implications of New

Technologies issued for comment its "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology." **The Commission is seeking public comment and has set a deadline of December 15, 2010**.

The Commission articulated its objective as follows:

> The Commission is studying how lawyers use [certain] forms of technology as well as the current state of data security measures for each form of technology. The Commission's efforts have been guided by the reality that information, whether in electronic or physical form, is susceptible to theft, loss, or inadvertent disclosure. The Commission's goal is to offer recommendations and proposals regarding how lawyers should address these risks. To that end, the Commission invites comments on several confidentiality-related issues arising from lawyers' use of technology.

The Commission's research to date, and the Issues Paper itself, focus on two categories of technology: (1) cloud computing; and (2) "technology controlled by lawyers or their employees," including devices that can store or transmit confidential electronic information, such as laptops, cell phones, flash drives, scanners, and photocopiers. **The Issues Paper broadly defines "cloud computing" as "any service provided online and operated by a third party" or "services that are controlled by third-parties and accessed over the Internet."** That means everything from webmail (Hotmail, Gmail, etc.) to online data storage to software as a service (SaaS), e.g., Salesforce.com.

In the information security and privacy law community, we often talk about the problem of organizations conflating "compliance" with "security." The Commission immediately recognizes this issue, noting that there is likely to be a difference between attorney use of these technologies that would be unethical and *attorney use that would not be unethical but might be ill-advised from a security point of view*. Some of my information security friends might be troubled by the following statement by the Commission:

> the Commission recognizes that there may be a gap between technology-related security measures that are ethically required and security measures that are merely consistent with "best practices." For example, it may be consistent with best practices to install sophisticated firewalls and various protections against malware (such as viruses and spyware), but lawyers who fail to do so or who install a more basic level of protection are not necessarily engaged in unethical conduct. Similarly, it might be inadvisable to use a cloud computing provider that does not comply with industry standards regarding encryption, but it is not necessarily unethical if a lawyer decides to do so.

As a result of this perceived distinction, the Commission is considering three non-mutually exclusive options in terms of what its work product might be: (1) white paper/guidance; (2) online resource; and/or (3) proposed amendments to the Model Rules of Professional Conduct, such as Model Rules 1.1 (competency), 1.6 (duty of confidentiality), 1.15 (safeguarding client property), or the comments to those Rules.

Thus, as a preliminary matter, it is important to recognize that **many lawyers who use the cloud and other technologies may take the view that they need NOT employ security best practices or even standard, cheap and easily implemented security controls because it is technically not "unethical" for them to opt against doing so.** The ABA will undoubtedly consider the consequences of this possibility in preparing its final work product.

Interestingly, the Commission also recognizes the existence of data security statutory law in a number of states

that already requires lawyers and other organizations to maintain certain security controls:

> The Commission recognizes that any guidance or rule amendments that it offers would have to operate within an increasingly large body of law that governs data privacy, some of which already applies to lawyers. For example, Massachusetts recently adopted a rigorous law on data privacy, . . . which applies to many lawyers and law firms (including those outside of Massachusetts) that have confidential information about Massachusetts residents.

You can read more about the Massachusetts data security regulations here.

Cloud Computing Confidentiality Issues

The ABA Commission has identified a number of confidentiality issues with respect to lawyer use of the cloud. Notably, ***many of these issues have existed and still exist in contexts independent of cloud, including more traditional outsourcing and use of contract lawyers and staff***. It is curious that the cloud computing hype has brought these issues to the attention of the mainstream legal community for the first time. Following are the confidentiality issues identified by the ABA Issues Paper:

- unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet;
- the storage of information on servers in countries with fewer legal protections for electronically stored information [for more on this subject, read on here];
- a vendor's failure to back up data adequately;
- unclear policies regarding ownership of stored data;
- the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business;
- the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information;
- policies for notifying customers of security breaches;
- policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms;
- insufficient data encryption;
- the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information.

Acknowledging that cloud computing is a form of outsourcing, the Commission invites feedback on the extent to which the procedures outlined in ABA Formal Ethics Opinion 08-451 (describing a lawyer's obligations when outsourcing work to lawyers and non-lawyers) should apply in the cloud computing context and seeks input

into whether cloud computing should affect the Commission's ongoing examination of possible amendments to Model Rule of Professional Conduct 5.3.

InfoLawGroup has written extensively about the due diligence and contract negotiation process for organizations looking to use the cloud. The Commission acknowledges that those issues are equally relevant to lawyers considering using the cloud. Specifically, the Commission seeks to determine which terms and conditions are essential for lawyers, such as:

- the ownership and physical location of stored data;
- the provider's backup policies;
- the accessibility of stored data by the provider's employees or sub-contractors;
- the provider's compliance with particular state and federal laws governing data privacy (including notifications regarding security breaches);
- the format of the stored data (and whether it is compatible with software available through other providers);
- the type of data encryption; and
- policies regarding the retrieval of data upon the termination of services.

Interestingly, the Commission asks for comments on whether lawyers ***have an obligation to negotiate particular terms and conditions*** before incorporating cloud computing services into their law practices.

"Traditional" Technology Confidentiality Concerns

The ABA Commission also addresses more "traditional" technology issues in its Issues Paper.

I have heard many lawyers express shock at the notion that they might not be able to use traditional email - whether locally-hosted or cloud-based webmail - to transmit sensitive information to a client. What do you mean I can't send the HR data as an excel spreadsheet attached to an email? Lawyers assume that the attorney-client privilege has them covered. However, the confidentiality concerns related to personally identifying information (Social Security numbers, medical information, financial account information, credit card numbers) raise new concerns and lawyers cannot forget that their clients - and their employees - are entrusting them with that information with an expectation that it will be protected in accordance with the laws and standards applicable to everyone else. The ABA is starting to take notice and seems particularly concerned with mobile media in this regard:

> [T]he Commission is considering whether to recommend that lawyers take certain precautions, such as:
>
> - providing adequate physical protection for devices (e.g., laptops) or having methods for deleting data remotely in the event that a device is lost or stolen
> - encouraging the use of strong passwords

● purging data from devices before they are replaced (e.g., computers, smart phones, and copiers with scanners

●installing appropriate safeguards against malware (e.g., virus protection, spyware protection)

● installing adequate firewalls to prevent unauthorized access to locally stored data

● ensuring frequent backups of data

● updating computer operating systems to ensure that they contain the latest security protections

● configuring software and network settings to minimize security risks

● encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them

● avoiding "wifi hotspots" in public places as a means of transmitting confidential information (e.g., sending an email to a client)

Do Lawyers Need Cyberinsurance?

Finally, the Commission goes as far as to seek comment on whether lawyers need to be procuring cyberinsurance and/or cyber liability insurance in addition to traditional professional liability coverage: "The Commission seeks more information about cyberinsurance and cyberliability insurance, including the underwriting requirements for such insurance and whether typical professional liability policies provide inadequate coverage for technology-related claims and losses."

There is still ample time for interested persons and entities to comment on the ABA's Issues Paper - the deadline is December 15, 2010 and you can contact us for more information.

The New York State Bar Association Formal Opinion

In the meantime, on September 10, 2010, the New York State Bar Association Committee on Professional Ethics issued Opinion 842 on lawyer use of an outside online storage (i.e., cloud) provider to store client confidential information. New York reached the same conclusion as the ABA in its preliminary assessment:

> A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes **reasonable care** to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. **In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.**

(Emphasis added). What is "reasonable care"? The NYSBA finds that "reasonable care" may include "consideration" of the following:

- ensuring that the cloud provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

- investigating the provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate;

- employing "available" technology to guard against reasonably foreseeable attempts to infiltrate the data; and/**or**

- investigating the provider's ability to purge and wipe any copies of the data and to move the data to a different host if the lawyer becomes dissatisfied or otherwise wants to change providers.

The NYSBA also points out that the lawyer must periodically reconfirm that the provider's security measures remain effective as technology changes. Further, and not surprisingly, the NYSBA states that if the lawyer has information to suggest that the provider's security measures are not longer adequate, or if the lawyer learns of a breach of confidentiality at the provider, the lawyer must investigate whether there has been a breach of confidentiality of its client information, must notify clients, and must discontinue use of the service unless the lawyer receives assurances that the problems have been sufficiently remediated. **This sounds a lot like the first ever mandated breach notice requirement for attorney-client privileged information.**

Importantly and interestingly, in the hypothetical addressed by the NYSBA, the online system is password protected AND the data stored is encrypted. Many, if not most, cloud solutions do not encrypt the data and rely on the user to do so himself or herself. Query how the NYSBA would change its opinion in the absence of encryption.

The NYSBA also states that lawyers using cloud services must monitor not only changes in technology, but changes in the law relating to technology, citing recent cases like *Quon* and *Stengart*.

I am ready to bet that many lawyers already using the cloud (a) do not encrypt their data; (b) have not investigated their cloud provider's security measures; and/or (c) do not have a contractual provision requiring the cloud provider to notify them in the event of a data breach. The NYSBA opinion should be a wake-up call to those lawyers to address these issues immediately. Many will be lucky if they even have the ability to retrieve their information and transfer to a different provider with better security measures without incurring significant cost and burden.

California State Bar Standing Committee on Professional Responsibility and Conduct Proposed Formal Opinion Interim No. 08-0002 (Confidentiality and Technology)

The California State Bar Standing Committee on Professional Responsibility and Conduct (COPRAC) Proposed Formal Opinion Interim No. 08-0002 (Confidentiality and Technology), while still not final, also speaks to lawyer use of the cloud.

The procedural history, and time that has already been devoted to this Proposed Opinion, demonstrates the difficulty that Bar associations face in keeping up with technology and technology law. COPRAC tentatively approved the Proposed Opinion at its September 10, 2009 meeting, more than a year ago, for a 90-day public

comment distribution with a January 4, 2010 deadline. Subsequently, at its August 6 & 7, 2010 meeting, COPRAC revised the opinion in response to the public comments received and tentatively approved Formal Opinion Interim No. 08-0002 for an additional 30-day public comment distribution. The most recent comment period closed on September 20, 2010.

The Proposed Opinion examines whether an attorney violates the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties. (Thus the question presented is somewhat more broad than the question addressed in the NYSBA opinion, which only looked at storage of encrypted data.) Relying on Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California, as well as Cal. Bus. & Prof. Code section 6068(e)(1), the Proposed Opinion says - well, "it depends."

Specifically, the Proposed Opinion finds that the answer depends on the particular technology being used and the circumstances surrounding such use. Thus,

> Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client‟s instructions and circumstances, such as access by others to the client‟s devices and communications.

It is a safe bet that most lawyers using the cloud today have never undertaken such a risk assessment.

The hypothetical scenario addressed by the CA Proposed Opinion is also fascinating in that lawyers do it every day and the conduct implicates security concerns beyond cloud computing - specifically, use of public wifi:

> Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm‟s access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm‟s computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney‟s supervisor is also permitted access to Attorney‟s computer to review the substance of his work and related communications.
>
> Client has asked for Attorney‟s advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

The CA Bar, not unlike the NYSBA, enumerates a number of factors attorneys should consider *before* using particular technology, as follows:

- The attorney's ability to assess the level of security afforded by the technology, including:

- consideration of how the particular technology differs from other media use;
- whether reasonable precautions may be taken when using the technology to increase the level of security; and
- limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds.

It is worth pausing here to note, as does the CA Bar in its Proposed Opinion, that many such reasonable precautions, such as encryption, firewalls, and password protection, are free or inexpensive and easily implemented:

> encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. . . . if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced. Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended.

Some free encryption services out there include Secret 1-2-3 for Outlook email, and TrueCrypt for disk encryption.

The Proposed Opinion also goes out of its way to admonish attorneys who are not comfortable with technology to get assistance from others who are conversant with technology and technology law:

> Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. **If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.**

(Emphasis added.)

But I digress. Back to the list of factors the Ca Bar proposes attorneys should consider *before* using various technologies:

- legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information.
- the degree of sensitivity of the information. If the information is of a highly sensitive nature and there is a

risk of disclosure when using a particular technology, **the attorney should consider alternatives unless the client provides informed consent**.

- Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.

- "The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions."

- Client instructions - if a client has instructed an attorney not to use certain technology or an attorney is aware that others have access to the client's electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should *not* be used in the course of the representation.

It seems unlikely that most attorneys today have a provision in their engagement letters that describes "the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal)." Query whether it is even possible to obtain such informed consent in the initial engagement letter given the rapid changes in technology and security risks. Does this mean that the attorney must email the client to obtain consent each time he/she logs in at a hotel or at Starbucks? What about BlackBerry and iPhone use?

Like the NYSBA, the CA Bar is not merely concerned with privilege - it also proposes requiring assessment of the impact of disclosure of non-privileged but still confidential information, something lawyers rarely consider: "[h]arm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed."

So, how does the CA Bar answer the hypothetical question about the associate's use of wifi in the coffee shop and/or at home? The answer may surprise you:

- wifi in the coffee shop (or at a hotel or in the airport, etc.) is off limits unless the attorney uses security measures and/or notifies the client and obtains informed consent:

  > **"due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection . . . to work on Client‟s matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall."** The Proposed Opinion provides a non-exhaustive list of local security features available for use on individual computers (operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions) as well as network safeguards that may be employed (network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring).

But that's not all the Bar thinks would be required in some (unidentified) circumstances: "Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."

And the Bar is quick to note its belief that client files stored on a computer may be at risk regardless of whether the attorney has a file open when an attorney is using an unsecure network connection without firewalls.

- wifi at home is fine IF the wireless systems has been configured with appropriate security features - otherwise, notice and client informed consent may be necessary.

So, at least according to the ABA, the NYSBA and the CA Bar, cloud computing and technology are no longer just for us technogeek lawyers. That's enough ethics and cloud for now (and probably for the month, right?). More to come soon.

Comments (0) Read through and enter the discussion with the form at the end

New York Office
244 Fifth Avenue, Suite 2580
New York, NY 10024
Tel:
646.389.1289

Denver Office
1117 S. Clarkson St.
Denver, CO 80210
Tel:
303.325.3528

Los Angeles Office
1500 Rosecrans Ave., Suite 500
Manhattan Beach, CA 90266
Tel:
310.706.4121

Salt Lake Office
5962 S. Fontaine Bleu Dr
Salt Lake City, UT 84121
Tel:
801.953.3858

Connecticut Office
3040 North Street
Fairfield, CT 06824

Tel:
203.292.0667