2015 ABA Conference on Professional Responsibility

Emerging Issues in Confidentiality: Confidentiality in a Mobile Technology-Laden Society

Pamela A. Bresnahan
pabresnahan@vorys.com
(202) 467-8861
Raymond D. Pinkham
rdpinkham@vorys.com
(202) 467-8806

Vorys, Sater, Seymour and Pease, LLP
1909 K St., NW, Ninth Floor
Washington, DC 20006
1. **Mobile Devices**

Given the proliferation of mobile devices, including laptops, smartphones and tablets, confidential information is taken with us everywhere we go. Increasingly, lawyers and law firms have become targets of cyber attacks. This risk is greatest when an attorney accesses unencrypted data over an unsecured wireless network.

The latest ABA Legal Technology Survey Report indicates that 14% of law firms experienced a breach last year in the form of a lost or stolen computer or smartphone, a hacker, a break-in or a website exploit.¹

The ABA CyberSecurity Handbook even goes so far as to state that “it may be prudent for all lawyers and law firms to adopt a working assumption that their computer networks and critical IT systems – as well as those of vendors to whom they may outsource the storage and processing of client confidential information – are vulnerable to such attackers, increasingly the target of such attackers, and at this time remain largely indefensible and at high risk of being breached.”

One important aspect of dealing with the current environment is knowing and understanding the professional rules and ethical obligations applicable to cyber security and the protection of client information in the digital world.

ABA Model Rule 1.6(a) states that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” The amended Model Rule 1.6 has the following new paragraph (c): “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

Model Rule 1.6, Comment [18], was revised to include factors to be considered in determining the reasonableness of a lawyer’s efforts to prevent the disclosure of confidential client information.

Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not

required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

As examples, a lawyer should make reasonable efforts to prevent disclosures or access, such as avoiding a lawyer’s sending an email to the wrong person, someone’s “hacking” into a law firm’s network, or staff’s posting client information on the internet. As Comment [18] makes clear, not every disclosure is a violation, but reasonable precautions are required.

One of the main concerns is access to a loss or stolen device by unauthorized users. See Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. State Bar Ass’n Journal, May 2013, Vol. 85, No. 4. One of the most basic rules regarding protecting confidentiality is the protection of the data itself, including password protection. This includes making a password “strong” and not simply “password” or “123456.” A “strong” password includes upper and lower case letters, numbers, symbols and even spaces.

Due to the “vast amounts of confidential information” that now can be stored on laptops, flash drives or smartphones, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies is considering the following precautions as recommendations related to the protection of confidential client information:

1. 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;
2. encouraging the use of strong passwords;
3. purging data from devices before they are replaced (e.g., computers, smart phones, and copiers with scanners);
4. installing appropriate safeguards against malware (e.g., virus protection, spyware protection);
5. installing adequate firewalls to prevent unauthorized access to locally stored data;
6. ensuring frequent backups of data;
7. updating computer operating systems to ensure that they contain the latest security protections;
8. configuring software and network settings to minimize security risks;
9. encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them; and,
10. avoiding “wifi hotspots” in public places as means of transmitting confidential information (e.g., sending an email to a client).

Attorneys and firms should also consider use of Mobile device management which allows firms to update all devices – and potentially remotely wipe the device if necessary.
An Ethics Opinion from the Florida Bar provides practical steps for lawyers to take in order to protect client confidentiality before a device is disposed of, including (1) identification of potential threats to confidentiality and implementation of policies to address such threats; (2) inventory all devices that contain hard drives or other storage media; (3) proper supervision of all nonlawyers to adequately assure that confidentiality will be maintained; and, (4) proper sanitization of a device by requiring meaningful assurances from a vendor at intake of a device and confirmation or certification of sanitization at disposition. The Florida Bar Ethics Op. 10-2 (2010).

A number of state bar ethics opinions generally address the issue of the types of measures attorneys should take in protecting confidential client information:

1. Alabama State Bar Association, Ethics Opinion 2010-02 (electronic documents must be secured and reasonable measures must be in place to protect the confidentiality, security and integrity of the documents and the lawyer must ensure that the process is at least secure as that required for traditional paper files. Attorneys must have “reasonable measures in place to protect the integrity and security of the electronic file, including ensuring that only authorized individuals have access to the electronic files, appropriate firewalls and intrusion detection software is in place and that electronically stored files are “back up” in case of file corruption or damage to the office).

2. Arizona Bar Opinion No. 09-04 (issued in December 2009). This opinion references specific acts to take such as secure socket layer (SSL) protocols, firewalls, password protections, encryption and anti-virus software. “As technology advances, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.

3. State Bar of California, Standing Committee on Professional Responsibility and Conduct, formal Opinion No. 2010-179 (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.

4. State Bar of Massachusetts, Opinion 00-01 (use of unencrypted e-mail for purposes of transmitting confidential or privileged client communications does not, in most instances, constitute a violation of any applicable
ethical rule, including Rule 1.6, because both the lawyer and the client typically have a reasonable expectation that such communications will remain legally and effectively private).

5. Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion 33 (February 9, 2006) ("attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney’s direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services.")

6. New Jersey Committee on Professional Ethics Opinion 701 (April 24, 2006) ("the critical requirement... is that the attorney ‘exercise reasonable care’ against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access.").

7. New York State Bar Association Committee on Professional Ethics, Opinion 1019 (August 6, 2014) (a law firm may give its lawyers remote access to client files, so that the lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing client of the risks).

8. Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200 (November 2011) (with regard to web-based e-mail, i.e., Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concluded that "attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically)

It is also important to keep in mind that various state and federal laws and regulations mandate the confidentiality of certain types of client information, including social security numbers, driver’s license information, financial accounts and related information, health and medical information, etc.

2. Confidentiality and Conflicts of Interest / Screening

There are increasing conflicts and disqualification risks due to increased lawyer mobility and firm mergers. One example was a recent attempt to disqualify Sidley Austin in defense of an auditor against allegations that the auditor failed to spot fraud at commercial lender Oak Rock Financial. A Sidley attorney brought the client to Sidley from Winston and Strawn, but Sidley transactional lawyers were involved in a 2010 investment in Oak Rock.
At a March 2015 hearing on the matter, New York Supreme Court Judge Shirley Werner Kornreich noted that due to mergers and how large firms have become, there are conflicts constantly.²

In another recent decision in a Motion to Disqualify in *Lennar Mare Island, LLC v. Steadfast Insurance Company*, Judge Kimberly Mueller in the US District Court for the Eastern District of California granted plaintiff’s motion to disqualify Hogan Lovells from its representation of defendant Steadfast Insurance Company.³

Beginning in 2005, Hogan started representing the parent corporation of one of the plaintiffs, CH2M Hill Constructor’s Inc., in the Lennar Mare Island matter. The General Counsel for the plaintiff described in a declaration that CH2M is “wholly dependent on Hogan Lovells for nearly all of the most important corporate and regulatory issues currently facing the company.” In August 2014, several attorneys for Hogan started to represent Steadfast Insurance as additional counsel because Steadfast’s counsel at the time informed it that the firm did not have the resources to continue as lead counsel.

Although Judge Mueller focused on the law firm’s duty of loyalty because she concluded that the conflict involved concurrent representation, confidentiality remained a concern in both concurrent and former client representation.

The duty of confidentiality is reflected in ABA Model Rule 1.6(b)(7) stating that “a lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (7) to detect and resolve conflicts of interest arising from the lawyer’s change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

The NY State Bar Association’s Committee on Standards of Attorney Conduct recently recommended that New York adopt new Comments to Rule 1.6 “to give lawyers more guidance about the disclosures that the existing New York Rules of Professional Conduct permit when lawyers and law firms contemplate lateral moves or law firm mergers.” The proposed comments provided more detailed guidance than the ABA comments regarding the specific types of information that is permitted to be shared without client consent in the context of a potential lateral move or law firm merger.

Proposed comment 18B states:

> Disclosure without client consent in the contest of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter,

---


including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each client-lawyer relationship; and (vi) information about aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

Proposed comment 18C states:

Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily not permitted, however, if information is protected by Rules 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness about paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; or information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

The Proposed comments also state that attorneys and firms should take all reasonable measures to prevent unauthorized or inadvertent disclosures, including such measures as:

(1) disclosing client information in stages, initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information out the firm(s) during and after the lateral or merger process.

Moreover, effective Ethical Screens include things such as:

1. Notice to affected clients;
   a. ABA Model Rule 1.10(a)(2)
2. Training/guidance for attorneys and others;
3. Written checklists/protocols;
4. Notice to all screened persons;
5. Notice all persons working on screened matter;
6. Physical and operational separation;
7. Limited access to electronic files;
8. Continuing monitoring of the screen and reminders about the screen.

3. **Ethical Implications of NSA Surveillance**

In February 2014, the NY Times reported that a top-secret document obtained by former N.S.A. contractor Edward Snowden indicated that an American law firm was “monitored while representing a foreign government in trade disputes with the United States.” The article reported that the Australian Signals Directorate, the NSA’s Australian counterpart, notified the NSA that it was conducting surveillance, “including communications between Indonesian officials and the American law firm, and offered to share the information.”

The lesson should be clear. Attorneys and law firms engaged in international communications have to consider the potential for interception, especially in high profile cases or cases where the government may have a particular interest, including narcotics and terrorism cases.

On February 20, 2014, in light of these developments, James Silkenat, President of the ABA at the time, sent a letter to General Keith Alexander, who at the time, was Director of the NSA, and Rajesh De, General Counsel at NSA. The letter requested the NSA’s support in “preserving fundamental attorney-client privilege protections for all clients and ensuring that the proper policies and procedures are in place at NSA to prevent the erosion of this important legal principle.”

Mr. Silkenat’s letter explained that the interception and sharing of attorney-client privilege information and communications by government agencies “raises concerns, including chilling the full and frank discussion between lawyer and client that is essential for effective legal representation.” The letter continued, stating that “[a]ny government surveillance and interception of confidential communications between law firms and their clients threaten to seriously undermine and weaken the privilege. . . .”

The letter also referenced the ABA Resolution and Report 118, which was adopted by the ABA House of Delegates in August 2013. The ABA resolution condemned “unauthorized, illegal governmental organizational and individual intrusions in the computer systems and networks utilized by lawyers and law firms.” The resolution also urged federal, state, local, territorial and tribal governmental bodies to “examine, and if necessary, amend or supplement, existing laws to promote deterrence and provide appropriate sanctions for unauthorized, illegal intrusions into the computer networks utilized by lawyers and law firms” as well as urging the United States government to “work with other nations and organizations in both the public and private sectors to develop legal mechanisms, norms and policies to deter, prevent, and punish

---

Unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms.”

On March 10, 2014, General Alexander responded to Mr. Silkenat’s letter, explaining that the “NSA is firmly committed to the rule of law and the bedrock legal principle of attorney-client privilege” and that the “NSA has afforded, and will continue to afford, appropriate protection to privileged attorney-client communications acquired during its lawful foreign intelligence mission in accordance with privacy procedures required by Congress, approved by the Attorney General, and, as appropriate, reviewed by the Foreign Intelligence Surveillance Court.”

Obviously, General Alexander’s letter reframed the issue, explaining that “[g]iven the inevitability of incidental collection of U.S. person information during the course of NSA’s lawful foreign intelligence mission—to include potentially privileged information—the issue is how to provide appropriate protections for any such information when it may be acquired.” General Alexander explained that NSA has policies and procedures in place that are “designed to minimize the acquisition, retention, and dissemination of information to, from, or about U.S. persons, including any potentially privileged information, consistent with the NSA’s foreign intelligence mission.” He further explained that potentially privileged information is given special review and consideration, in that any information that constitutes privileged communications must be reviewed by the Office of General counsel before dissemination, that the collection or reporting of such information be limited, that intelligence reports be written so as to prevent or limit privileged material and to exclude U.S. identities and that dissemination of such reports be limited and subject to appropriate warnings or restrictions on their use.

Nevertheless, concerns remain over the collection of information that could include attorney-client communications and privileged documents and/or work-product. The lack of detail regarding the scope of such surveillance makes it practically impossible to know which communications and types of data storage are secure.

Particularly sensitive communications are increasingly problematic. Attorneys and clients could meet face to face, but that could potentially involve costly international travel. Encryption of portable devices, e-mail and other communication is another option. Engagement Agreements with clients may start to include disclaimers that given potential governmental surveillance, absolute confidentiality of any attorney-client communications cannot be guaranteed. A July 2014 Human Rights Watch report on the impact of such surveillance indicated that some attorneys have started warning clients that they cannot guarantee their communications will remain confidential, only using e-mail, Gchat or WhatsApp for casual, non-substantive communications, and increasing amounts of travel in order to meet clients face to face.5

4. **Confidentiality in Limited Scope Representation**

As the cost of legal services has increased, the frequency of limited scope representation, commonly known as “unbundling” has also increased. Limited scope representation, or unbundling, refers to the allocation between the lawyer and the client of the duties and responsibilities for handling a legal matter. California Rules of Court, Rule 3.35 defines the phrase as “a relationship between an attorney and a person seeking legal services in which they have agreed that the scope of the legal services will be limited to specific tasks that the attorney will perform for the person.”

Colorado Bar Association Ethics Committee, Formal Opinion 101 (1998) emphasized the importance of “unbundled” representation to “individuals who do not qualify for public or private legal assistance programs, but who cannot afford the full service of a lawyer.” The Colorado Bar Association Ethics Committee concluded that the ethics rules of Colorado allowed “unbundled legal services in both litigation and non-litigation matters.”

It is important to note that the attorney’s fiduciary duties of loyalty and confidentiality are not encumbered, even though the scope of representation may be limited. A publication by the State Bar of California, Committee on Professional Responsibility and Conduct, entitled “An Ethics Primer on Limited Scope Representation” states:

The fiduciary duties of loyalty and confidentiality apply with equal force and effect whether an attorney is providing full service representation for a transactional or litigation matter, or representing the client only on a limited scope basis. The duty of confidentiality is “fundamental to our legal system” and attaches upon formation of the attorney-client relationship, or even in the absence of such a relationship where a person has consulted an attorney in confidence.

Even in limited scope representations, attorneys must perform conflicts checks and avoid the disclosure of confidential client information. In some jurisdictions, this includes even including the fact that the representation is of a limited scope. State Bar of Arizona ethics opinion 06-03: Limited Scope Representation; Confidentiality; Coaching; Ghost Writing goes so far as to the state that “[i]n fact, unless required to do so by the rules, e.g., E.R. 1.6, an attorney may not disclose information pertaining to the limited representation unless authorized to do so by the client. Disclosure of the limited scope may indeed adversely affect the client’s situation.”

Other states frame the issue as one of making sure professional rules against “dishonesty, fraud, deceit or misrepresentation” are not violated. One New York City Bar Opinion (Formal Opinion 1987-2) states that pro se litigants are typically afforded “special treatment” by the courts and are generally held to less stringent standards. The opinion indicates that drafting any pleading, except for assisting a litigant in filing out a form, is “active and substantial legal assistance” that required disclosure to opposing counsel and the courts.

Similarly, Delaware State Bar Association Committee on Professional Ethics, Opinion 1994-2 (May 6, 1994) concluded that it would be improper for an attorney to fail to disclose his/her help when there has been “significant assistance,” which was defined as help that goes
beyond mere assistance with an initial pleading or providing initial general advice and information. Further, if an attorney provides advice on an on-going basis to an otherwise pro se litigant, the Committee on Professional Ethics concluded that this fact must also be disclosed.

Conclusion

Technology allows lawyers and their clients to communicate anytime and anywhere. Confidentiality is sometimes at risk because of the lawyers’ and clients’ mobility. Increased care must be taken because of the risk of interception and use of these otherwise privileged communications.