Technology and Confidentiality

Professor Nathan M. Crystal,
Attorney at law
Distinguished Visiting Professor Charleston School of Law
Crystal & Giannoni-Crystal, LLC

What are we going to talk about?

- Complying with the duty of confidentiality has become increasingly difficult and risky with the widespread use of modern technology in the practice of law.
    - WHY?
- The basic obligation of lawyers with regard to confidential client information is clear: lawyers must take **reasonable steps** to protect the confidentiality of such information.

What are we going to talk about?

- South Carolina Rule of Professional Conduct (SCRPC) 1.6, comment 18 states: "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

What are we going to talk about?

- If the standard is clear (reasonability), determining when the standard is met is unclear.
  - WHY?
- In the continuously changing field of technology it is difficult (1) to determine what is reasonable and (2) to implement what is reasonable when using modern technology.

Guideline in the near future …

- ABA's Ethics 20/20 Commission, which is considering revisions to the Model Rules, has issued a draft of its proposed revisions to the Model Rules of Professional Conduct dealing with the ethical issues raised by use of technology. See the website of the ABA Ethics 20/20 Commission.

Topics of this presentation

(1) public use of technology

(2) metadata in document transmission

(3) loss of devices and

(4) disposal of devices

(5) outsourcing and "the cloud"

(6) use of social networking sites

(7) dealing with confidentiality breaches

Topics of this presentation

- One way of addressing the problem
  - Development of law firm policies and procedures on the use of technology
    - with the help of competent IT personnel to give advice on technical issues and implementation of appropriate policies
    - Internet policies used by business organizations that deal with sensitive data. See e.g., Sans Institute, Information Security Policy Templates

Topics of this presentation

- Inclusion in the engagement agreement of a provision summarizing the policies, seeking client's consent and request to inform their lawyers if client wishes the firm to use different approaches.

1. Public use of technology

- One easy and obvious point:
- Discussing a client matter in public on a cell phone is not using reasonable precautions to protect the confidentiality.
- Solution is clear -- Don't do it, except to confirm a meeting time or for something routine. In doubt: avoid it!
- Clients will understand and appreciate when you say, "Can I call you back in a few minutes when I am at a place where I can speak confidentially?"

Public use of technology

- Use of computers for handling client matters on public networks, such as ones at Starbucks, at airports, or in other hotspots? It runs the risk that information may be hacked but undue restrictions on the use of such networks could significantly hamper the work of many lawyers who travel a lot.

Public use of technology

- California Ethics Committee Formal Opinion 2010-179:
  - Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop 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.

Public use of technology

- 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.

- Opinion might be wrong if you consider ABA Formal Opinion 99-413 . . .

Public use of technology

- Lawyers could use email without encryption because there is a reasonable expectation of privacy with regard to email and interception of email was criminal.

ABA's opinion does not speak of public networks but …

Public use of technology

- In my opinion, ABA's 99-413 opinion matters because while the expectation of privacy with regard to public networks is less than when using lawyer's own system, such an expectation still exists to a large degree. Moreover, any interception would be criminal.

Public use of technology

- Comments to Rule 1.6 support the view hat special precautions are generally not necessary in the use of a method of communication:
  - "This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

Public use of technology

- Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

Public use of technology

In conclusion, lawyers should generally be allowed to use public networks without special security measures unless:

- the matter is particularly sensitive
- the client has directed otherwise
- the industry in which clients operate (example defense dept) reasonably requires higher precautions

Public use of technology

To confirm, you may consider:

Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010), holding that the attorney-client privilege applies also when client's email to her attorney is composed on company-owned computers even though the company had a policy allowing review of such email

Public use of technology

But there is the reverse of the situation: lawyer *receiving* an email from a client that used an unsecured device:

Lawyer's duty to warn the client that confidentiality is at risk …

Public use of technology

. . . when the lawyer knows or should have known that the client is sending communication from an unsecure device, for example an employer's computer.

See: Formal Opinion 11-459 of ABA Standing Committee on Ethics and Professional Responsibility. It deals with a lawyer's ethical obligations when the lawyer represents a client …

Public use of technology

. . . who may be using the computer system of the client's employer or some other third party for sending confidential emails to the lawyer.

Public use of technology

For further info on this, visit:

http://g.virbcdn.com/_f/files/c1/FileItem-144170-EthicalCoffeeBreak7.pdf

2. Metadata in document transmissions

- Metadata refers to information embedded in electronic documents, such as date of creation, author of the document, changes made to the document, author and date of changes, when the document was last saved, and comments to the document.

Metadata in document transmissions

- ABA Formal Opinion #06-422.
- A lawyer who received a document from opposing counsel in connection with a matter could ethically access and review the metadata contained in the document because no rule specifically prohibited a lawyer from examining the metadata.

Metadata in document transmissions

- Rule 4.4(b) dealing with inadvertently produced material did not apply because a document sent to opposing counsel was not done inadvertently.
- Ethics committee in some states have taken a different view. See, e.g. New York and Florida.

Metadata in document transmissions

- E.g. New York, Opinion #749 – 12/14/2001
  - Lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents.

Metadata in document transmissions

- So?
- Consider:
  - South Carolina Ethics Committee has not advised on the issue.
  - If a lawyer is appearing in a matter in another jurisdiction, the rules of the jurisdiction in which the tribunal sits will apply. See SCRPC 8.5(b)(1).

Metadata in document transmissions

- Given this split in authority, lawyers should take reasonable precautions to protect from disclosure the metadata in their documents.
- The ABA Committee observed that counsel sending a document could take a variety of steps to avoid revealing metadata, including use of scrubbing programs.
  - See also: Robert Brownstone, Metadata: To Scrub Or, Cal. Bar J. (Feb. 2008).

3. Loss of devices

- We are talking of loss of pen drives, smart phones, laptops, or other devices.

- These devices contain enormous amounts of information, much of which is confidential.

Loss of devices

- Reasonable precautions require law firms to recognize the possibility of loss of devices and to develop appropriate policies to reduce the risk of loss.
- A firm could prohibit the use of personal devices on firm matters.
  - Lawyer would be required to use only firm flash drives, PDAs, and laptops that have file encryption, that are password protected, and that contain confidentiality notices with instructions for return the device.

Loss of devices

- Are these steps ethically required?
- Maybe not, particularly for solo practitioners and small firms where the costs of such steps might be substantial.

Loss of devices

- At a minimum, however, if a lawyer uses a device for professional purposes, the device should be password protected, with a strong password, i.e. one containing both letters, numbers, and at least one character (the more digits, the better).
- In addition, check if your insurance policy covers cyber loss.

4. Disposal of devices

- The number of devices with hard drives that store confidential client information is enormous, including computers, printers, copiers, scanners, cellular phones, personal digital assistants, flash drives, memory sticks, and facsimile machines.

Disposal of devices

- When such devices are disposed of there is a risk of disclosure of confidential client information.
- So? You can get inspired by Opinion #10-2, Florida Bar Professional Ethics Committee.

Disposal of devices

- Based on the general duties of confidentiality (SCRPC 1.6), competence (SCRPC 1.1), and supervision (SCRPC 5.3), the Florida Bar Professional Ethics Committee identified the following specific obligations:

(a) inventorying devices that contain hard drives or other storage mechanisms;

Disposal of devices

(b) instructing nonlawyers (employees and independent contractors) of the confidentiality obligation of lawyers and make sure that they agree to comply with those obligations, and that they take reasonable steps to comply with that obligation.

Disposal of devices

(c) assuring that devices are cleansed of confidential information before disposition, either by having this occur at the lawyer's office, by meaningful confirmation or by some other reasonable means.

(d) keeping abreast of changes in technology to keep current firm policies regarding disposal of devices;

Disposal of devices

(e) recognizing that threats to confidentiality could occur with the use of devices located in places other than the lawyer's office, such as copy centers, business centers at hotels, and home offices. The Florida Committee advised that lawyers should inquire and determine whether the use of devices at such places poses a threat to confidentiality.

Disposal of devices

- Following the advises of the Florida opinion is good practice.
- Obviously, as IT experts might tell you, there is really no way to completely remove data from a devise in order for the data to be absolutely irretrievable. But once again, the key is:
  - reasonable steps + information to clients.

5.The “Cloud”

- Moving of the firm’s storage, application acquisition, and application maintenance to the internet.
- Data storage is on remote computers that the firm may not be able to identify easily.
- Updates of applications become immediately available through the internet.
- Any device with an internet connection regardless of location can access any of the firm’s applications via the internet.

The “Cloud”

- Because the cloud involves moving storage of firm data outside the firm to servers of various providers, it obviously poses issues of confidentiality.

The "Cloud"

- A few opinions have examined the ethical propriety of lawyers using cloud computing. These opinions have concluded that lawyers may ethically use cloud computing provided they take reasonable precautions to protect client confidentiality.

- See, e.g. N.Y. State Bar Op. 842 (2010).

The "Cloud"

- The New York Opinion provides a useful list. Reasonable care includes:

1. ensuring that the provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process demanding client information;

2. investigating the adequacy of the provider's security measures, policies, "recoverability methods," and other procedures;

3. using available technology to prevent attempts to hack into the stored data;

The "Cloud"

4. exploring the provider's ability to move the data to a different host and purge copies of the data if the lawyer wants to change providers;

5. periodically reconfirming that the provider's security measures remain effective in light of advances in technology;

6. upon learning of any breach of confidentiality by the provider, the lawyer must investigate whether the breach involved the clients' information, notify any affected clients, and discontinue use of the service unless the security issues are fixed;

The "Cloud"

7. monitoring the evolving law relating to technology and protection of confidential communications, especially legal developments concerning privilege waiver;

8. staying abreast of evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost.

The “Cloud”

In other words – due diligence before moving to the cloud—and due diligence on a continuing basis thereafter.

6. Use of Social Media

- Statistics: 56% of lawyers maintain a presence in social media (83% LinkedIn, Facebook: 68%, twitter 2%). Why? Because the social media are booming and lawyers feel that they must be there. In particular:
- Facebook – "what are you doing?"
- LinkedIn – "what do you do?"
- Twitter – "what are you thinking?"

Use of Social Media

- If lawyers put comments about famous case in the media, no problem.
- Information about the law, legal institutions, and similar matters is not subject to the duty of confidentiality even though the lawyer may acquire such information while working on a client matter, so long as the lawyer does not otherwise disclose client confidences. Restatement (Third) of the Law Governing Lawyers §59.(2000)

Use of Social Media

- But what if they comment about their own cases?
- Whether in physical or electronic form, disclosure of confidential information by lawyers as part of a marketing effort is improper.

Use of Social Media

- The ABA Journal reported on a case in which a law firm was fined $25,000 for referring to a $17 million confidential settlement against a builder when the firm wrote to other homeowners in an effort to persuade them to bring similar litigation. See *Martha Neil*, ABA Journal News (April 16, 2009).

Use of Social Media

- The same result would follow if the firm attempted to use the settlement on its website, LinkedIn page, or by email communication.

Use of Social Media

- S.C. Bar Ethics Adv. Op. #-02-15 (holding that an attorney's violation of the provisions of a confidential settlement agreement was a reportable offense under Rule 8.3(a), but the lawyer who had knowledge of the violation was required to obtain client consent under Rule 8.3(c) before reporting because the information related to the representation of the lawyer's client under rule 1.6(a)).

Use of Social Media

- Lawyers must remember that the ethical duty of confidentiality is broad.
- Under Rule 1.6(a) the duty applies to any information "relating to the representation of a client."
- The duty applies regardless of the form of information -- whether oral, written, or electronic -- and regardless of the source of the information -- whether client, third party, or generated through investigation.

Use of Social Media

- The rule does not contain an exception for public information, so merely because the information is part of the public record does not mean that the duty of confidentiality is inapplicable.

Use of Social Media

- There is some controversy on the point of generally known information.
- In *Sealed Party v. Sealed Party*, 2006 WL 1207732 (S.D. Tex. 2006), a Texas federal district court held that the Texas Rules of Professional Conduct do not provide an exception to the duty of confidentiality to reveal either "public" information or "generally known" information.

Use of Social Media

- Under the Restatement "generally known" information is not subject to the duty of confidentiality (but information that has simply been revealed to others -- without being generally known -- remains subject to the duty of confidentiality)
- The rules of some jurisdictions, such as New York, provide exceptions for widely known public information.

Use of Social Media

- In conclusion, references to a client even when the references are a matter of public record without client consent is risky at best.
- What about a provision in the engagement agreement allowing the lawyer to refer to aspects of the client's matter in electronic communications to the extent that the information is a matter of public record? If you don't feel comfortable putting this in your engagement agreement, then you should consider the information confidential unless the client expressly consents.

7. Dealing with Confidentiality Breaches

- Many states, including South Carolina, have data security laws. See the website of the National Conference of State Legislature dealing with Security Breach Notification Laws.
  - The South Carolina statute, 39-1-90(A) (applicable to individual's information)

Dealing with Confidentiality Breaches

- "A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system …

Dealing with Confidentiality Breaches

- . . . following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.

Dealing with Confidentiality Breaches

- In case of violation:
  - liability for damages, including attorney fees.
  - For a knowing and willful violation a person is subject to a civil penalty of $1000 for each resident of the state whose information was accessible.

Dealing with Confidentiality Breaches

- The statute only applies to personal identifying information, which is defined as the name of a person in association with some other piece of important information such as a social security or bank account number. See S.C. Code 16-13-510(D).

Dealing with Confidentiality Breaches

- And what's about business?
- Pursuant to the rules of ethics that require lawyers to communicate with their clients and in particular, Rule 1.4(b) ("A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation") . . .

Dealing with Confidentiality Breaches

- . . . in my opinion a law firm representing business clients that suffered a security breach would be ethically required to informs its business clients about the breach.

What to do to reasonably deal with "technology risks"

- To deal with technology risks, law firms need to adopt appropriate policies and procedures.
  - Useful source for developing firm policies and procedures is the regulations adopted by the Massachusetts Department of Consumer Affairs pursuant to the state's data privacy law. See 201 CMR 17.00.

What to do to reasonably deal with "technology risks"

- "Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program."

What to do to reasonably deal with "technology risks"

- In my opinion, at a minimum the reasonable actions that a law firm should take are the following:
- To establish a policy;
- To educate/inform employees and contractors
- To attentively monitor
- To take corrective actions.

What to do to reasonably deal with "technology risks"

- Communication to clients is an important aspect of any data security program.
- When?
  - We have said: in case of a breach but actually communication must start much earlier.

What to do to reasonably deal with "technology risks"

- Communication begins with the engagement agreement.
- In my opinion law firms should include in their engagement agreements a provision dealing with the use of technology.

What to do to reasonably deal with "technology risks"

- **Example:**
  - *This law firm uses various devices in the representation of clients, including desk top and laptop computers, smart phones, tablets, copy and fax machines, and flash drives. These devices use a number of different applications, including word processing, email, and spread sheets.*

What to do to reasonably deal with "technology risks"

- *The devices also contain memory in which information is stored. These devices and their applications have increased the efficiency of the practice of law to the benefit of clients.*
- *At the same time the use of these devices, applications, and data storage systems have increased the transmission and storage location of client information, thereby increasing the risk that such information may be compromised*

What to do to reasonably deal with "technology risks"

- *The firm has instituted various policies and procedures to protect the confidentiality of client information. A detailed statement of these policies and procedures is available at ----. By signing this engagement you consent to the firm's use of these technologies in accordance with the policies and procedures adopted by the firm.*

What to do to reasonably deal with "technology risks"

- *If you have any questions, concerns, or special requests regarding the protection of your confidential information, please discuss the matter with the attorney who is responsible for your case or with ---, the managing attorney of the firm.*

For further information and materials

- You are welcome to contact me at: info@nathancrystal.com

- For additional materials, you can visit my website: www.nathancrystal.com