

CHAPTER 1

**ELECTRONIC IQ:
SOCIAL MEDIA AND CLOUD COMPUTING**

WSBA Law of Lawyering Conference
December 18, 2014

Mark J. Fucile

Fucile & Reising LLP
Portland Union Station
800 N.W. Sixth Avenue, Suite 211
Portland, OR 97209-3783

Phone: (503) 224-4895
Fax: (503) 224-4332
E-mail: mark@frllp.com
www.frllp.com

MARK J. FUCILE of Fucile & Reising LLP handles professional responsibility, regulatory and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark is the inaugural chair of the WSBA Committee on Professional Ethics and is a past chair of its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is also a former member of the Oregon State Bar Legal Ethics Committee and is a current member of the Idaho State Bar Section on Professionalism & Ethics. Mark writes the quarterly Ethics & the Law column for the WSBA's *NWLawyer* and the monthly Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*. Mark is a contributing author/editor for the current editions of the WSBA's *Legal Ethics Deskbook*, the WSBA's *Law of Lawyering in Washington* and the OSB's *Ethical Oregon Lawyer*. Before co-founding his firm in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches the Legal Profession course as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Washington, Oregon, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law.

TABLE OF CONTENTS

ELECTRONIC IQ: SOCIAL MEDIA AND CLOUD COMPUTING

Mark J. Fucile

- I. ELECTRONIC IQ:
COMPETENCE IN AN ERA OF HIGH-TECH LAWYERING
(Reprinted from Mark's July-August 2014 Ethics & the Law column for the
WSBA NWLawyer)
- II. ELECTRONIC UPDATE:
NEW WSBA ADVISORY OPINIONS ON METADATA
AND CLOUD COMPUTING
(Reprinted from Mark's November 2012 Ethics & the Law column for the
WSBA Bar News)
- III. WSBA ADVISORY OPINION 2215 (2012)
(Available on the WSBA web site at www.wsba.org)
- IV. PRESENTATION SLIDES

**I. ELECTRONIC IQ:
COMPETENCE IN AN ERA OF HIGH-TECH LAWYERING**
(Reprinted from Mark's July-August 2014 Ethics & the Law column for the
WSBA *NWLawyer*)

Competence is one of our fundamental duties. RPC 1.1 defines competence in the regulatory context to include “the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” The Washington Supreme Court in *Hizey v. Carpenter*, 119 Wn.2d 251, 261, 830 P.2d 646 (1992), described the related civil concept of the duty of care in similar terms: “To comply with the duty of care, an attorney must exercise the degree of care, skill, diligence, and knowledge commonly possessed and exercised by a reasonable, careful, and prudent lawyer in the practice of law in this jurisdiction.”

We often associate “competence”—or any shortcomings—with our substantive knowledge of the law. But, office practice failures such as missed deadlines have long been a staple of both regulatory discipline (*see, e.g., In re Lopez*, 153 Wn.2d 570, 106 P.3d 221 (2005) (brief not timely filed)) and legal malpractice (*see, e.g., Huff v. Roach*, 125 Wn. App. 724, 106 P.3d 268 (2005) (underlying action not timely filed)).

Increasingly, our “competence” in both a regulatory and civil sense is also being measured by how we use technology. Particularly as it applies to safeguarding client confidential information, the comments to the confidentiality rule—RPC 1.6—have long woven competence in the selection and use of technology into our bedrock duty of confidentiality. The ABA’s recently adopted “20/20” amendments to its influential Model Rules that are under review in Washington also include the notion of staying current with new technology as a central element of our duty of competence. In this column, we’ll survey first our duties of “electronic” competence and then use electronic file storage as a practical example.

Before we do, however, two important qualifiers are in order. First, in the regulatory context, not every instance of negligence automatically implies a lack of competence under RPC 1.1 (*see In re Anshell*, 141 Wn.2d 593, 609 n.4, 9 P.3d 193 (2000)). Second, in the civil context, any asserted negligence must have caused the damages sought to support a claim for legal malpractice (*see Daugert v. Pappas*, 104 Wn.2d 254, 257-63, 704 P.2d 600 (1985)).

Electronic Competence

Newly revised Comment 18 to ABA Model Rule 1.6 neatly summarizes the interplay between competence and confidentiality:

“Acting Competently to Preserve Confidentiality

“Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent

or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. 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)."

The current version of Washington Comment 16 to RPC 1.6 is similar and the new ABA formulation is under review here.

The ABA Model Rule amendments also include an explicit tie between competence and keeping current with new technology in Comment 8 to Model Rule 1.1:

"Maintaining Competence

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology[.]"

The current version of Washington Comment 6 to RPC 1.1 discusses continuing education generally, but does not have the explicit tie between competence and new technology. This new ABA formulation, however, is also under review here.

Example: Electronic File Storage

Although technology has transformed many aspects of law practice, one of the best illustrations is file storage. Paper files are gradually giving way to various forms of electronic storage—ranging from local media to remote "cloud" services. The ability to store and retrieve data seamlessly both within and outside our offices affords many benefits for lawyers and clients alike.

At the same time, the consequences of data loss or theft are potentially more far reaching as well. In years past, a paper file inadvertently left behind at a restaurant after lunch with a client raised potential confidentiality issues if not recovered quickly—but they were normally limited to the single client concerned. By contrast, a laptop left behind at that same restaurant today may magnify the confidentiality issues across the lawyer's entire client base if the computer holds the lawyer's "virtual file room." Similarly, the theft of a law firm's confidential information through "hacking" into its servers—whether on-site or maintained remotely—can present those issues even more starkly.

Beyond the RPCs, many states, including Washington (*see* RCW 19.255.010), have broad data breach notification laws.

The federal district court in Seattle commented on both the rise of electronic data theft and related litigation in *Krottner v. Starbucks Corp.*, 2009 WL 7382290 at *2-*3 (W.D. Wash. Aug. 14, 2009) (unpublished; citations omitted):

“Digital collections of thousands or even hundreds of thousands of people’s personal data are ubiquitous, and theft or loss of those collections is, if case law is any indication, becoming increasingly common. In some cases, information is compromised by hacking into computer networks that store personal information . . . Often, as in this case, plaintiffs raise claims arising from the theft of computers that contain collections of personal information.

“Accompanying the rise in the theft or loss of such data collections is a rise in civil suits. The theft or loss of a data collection brings with it the possibility of what the court will broadly refer to as ‘identify theft.’ In the hands of an identity thief, a plaintiff’s personal information can be used to gain access to his financial accounts, open new accounts in his name, and engage in other schemes limited only by the thief’s ingenuity.”

The WSBA in Advisory Opinion 2215, which was issued in 2012, discussed the general factors that lawyers should consider in evaluating cloud computing services. Although remote storage presents some unique issues precisely because we are using an independent vendor often operating at significant physical distance from our office, much of the advice rings true even for storage that is located closer to (or in) our offices. Advisory Opinion 2215 also echoes the comments noted in weaving together the concepts of competence and confidentiality:

“A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so. While some lawyers may be able to do more thorough evaluations of the services available, best practices for a lawyer without advanced technological knowledge could include:

“1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.

“2. Evaluation of the provider’s practices, reputation and history.

“3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer’s duty of confidentiality and agrees to handle the information accordingly.

“4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.

“5. Confirming provisions in the agreement that will give the lawyer prompt

notice of any nonauthorized access to the lawyer's stored data.

“6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.

“7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider.”

Finally, Advisory Opinion 2215 notes that our duties don't end with selection of a service. It counsels that because technology changes rapidly, lawyers “must also monitor and regularly review the security measures of the provider.”

Summing Up

Lawyers don't necessarily need to become “computer nerds” to meet their duty of competence if we have sufficient internal or external technical assistance. But, any lawyer using technology has to understand it well enough to meet our many responsibilities to our clients—including our fundamental duty of confidentiality.

**II. ELECTRONIC UPDATE:
NEW WSBA ADVISORY OPINIONS ON METADATA
AND CLOUD COMPUTING**

(Reprinted from Mark's November 2012 Ethics & the Law column for the
WSBA Bar News)

Earlier this year, the WSBA Rules of Professional Conduct Committee issued a pair of advisory opinions providing practical guidance on two emerging areas of “electronic ethics”: metadata and cloud computing. The metadata opinion—2216—examines our duties from the perspective of both the sender and the receiver when exchanging documents in electronic form with opposing counsel. The cloud computing opinion—2215—focuses on our responsibilities when using off-site electronic file storage managed by independent vendors. Both opinions are available on the WSBA web site at www.wsba.org.

Core Duties

The metadata and cloud computing opinions revolve around two core duties: competency and confidentiality. RPC 1.1 defines the former and RPC 1.6 the latter.

In the electronic context, the subtitle for Comments 16 and 17 to RPC 1.6 says it all: “Acting Competently to Preserve Confidentiality.” We are expected to competently choose methods of electronic file sharing and storage that protect client confidentiality.

Comments 16 and 17 elaborate on both duties:

“[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3 [the latter two address supervisory responsibilities].

“[17] 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. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. 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. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

These duties are not the simply the province of potential regulatory discipline. Whenever the word “competence” enters the discussion, malpractice risk is sure to follow. Similarly, the

Supreme Court in *Eriks v. Denver*, 118 Wn.2d 451, 824 P.2d 1207 (1992), held that the professional rules reflect our underlying fiduciary duties.

Metadata

Lawyers increasingly share documents in electronic form with their opponents in both transactional and litigation contexts. A ready example from transactional practice is a draft contract. An equally ready example from litigation practice is a draft settlement agreement. With electronic file sharing, the concern is on the “metadata” embedded within the document. The Supreme Court in *O’Neill v. City of Shoreline*, 170 Wn.2d 138, 145, 240 P.3d 1149 (2010), aptly defined metadata as “data about data.” Metadata can often reveal, for example, when changes to a document were made, who made them and can include editors’ comments. The electronic comments in particular may contain attorney-client communications.

Opinion 2216 looks at metadata from the perspective of both the sender and the receiver. (In doing so, it examines our duties outside the context of formal discovery. Under RPC 3.4, our duties within the context of formal discovery are largely governed by the procedural rules of the forum in terms of what must be produced and what may be withheld.)

From the sender’s perspective, Opinion 2216 weaves together the twin duties noted earlier by explaining that we need to sufficiently understand the technology we are using to ensure that we protect confidential material such as attorney-client communications and work product. Opinion 2216 notes that the particular method chosen can vary with the circumstances and will likely change as technology evolves. The options currently available, however, range from transmitting documents in hard copy (or its equivalent, such as fax or mechanically scanned documents) to “scrubbing” software that removes sensitive metadata.

From the receiver’s perspective, Opinion 2216 counsels that a lawyer is not prohibited in the first instance from looking at metadata in a document that the lawyer receives from the other side. In many situations, the metadata may be irrelevant because it does not reveal anything of practical value or simply mirrors what the sender intended the receiver to see—such as a “redlined” document. If, however, the metadata contains what appears to be inadvertently produced privileged information, then RPC 4.4(b) directs that the lawyer notify his or her counterpart on the other side. At that point, RPC 4.4(b) leaves to evidence law the question of whether privilege has been waived through inadvertent production and leaves to procedural law the method for litigating potential privilege waiver. These last two points are addressed, respectively, by ER 502 and CR 26(b)(6). Finally, Opinion 2216 generally disapproves specialized “data mining” software that attempts to extract attorney-client communications or work product even if the sender has taken reasonable steps to protect the document involved.

Cloud Computing

Lawyers have used off-site storage for a long time. Traditionally, “off-site storage” meant a physical location (ranging from professionally managed facilities to individual storage units) where lawyers stored their closed files. More recently, “off-site storage” has evolved into “cloud computing” where documents are stored electronically on remote servers managed by

independent vendors and accessed via the Web. Some firms use electronic storage as back-up, some as a primary means of accessing documents and some do both.

The core duties of competence and confidentiality apply with equal measure to electronic storage. The federal district court in Seattle in *In re U.S. Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp.2d 1138, 1144 n.5 (W.D. Wash. 2011), recently emphasized the role independent vendors play in “cloud computing”: “An external cloud platform is storage or software that is essentially rented from (or outsourced to) a remote public cloud service provider[.]” The central involvement of a third party invokes our duty to supervise non-lawyers who assist us under RPC 5.3(a), which requires lawyers and firms to make “reasonable efforts” to make sure that an outside vendor in this circumstance “has in effect measures giving reasonable assurance that the person’s conduct is compatible with the professional obligations of the lawyer[.]” In short, a law firm can “contract out” the storage function but not the responsibility for properly acquainting the vendor with a lawyer’s duty of confidentiality and receiving reasonable assurance that the vendor has safeguards in place that are consistent with that duty.

Opinion 2215 notes that although lawyers do not need to become computer geeks they at least need to sufficiently understand the technology and safeguards that a vendor uses to make a reasonably informed choice that is in keeping with our duty of confidentiality. The opinion also stresses that these duties are not static: “Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider.”

Prudent “due diligence” should also include a review of your firm’s insurance coverage for data loss. Oregon’s mandatory malpractice carrier (the Oregon State Bar Professional Liability Fund), for example, issued a blanket exclusion for data loss earlier this year. If your firm is not covered, then you will need to balance the utility of off-storage with the corresponding risk. Depending on the type of information stored, statutory law (*see, e.g.*, RCW 19.255.010) may impose requirements for client notification if security is compromised. Imagining yourself writing your clients to inform them about how you lost their sensitive personal information should also be a strong practical motivator for doing “due diligence” on electronic storage providers.

Summing Up

Over the past generation, technology has transformed the practice of law. Electronic file sharing and storage are two prominent examples. The evolution in technology, however, has also produced new challenges for law firm risk management. As the new WSBA advisory opinions highlight, wherever technology may take law practice, it won’t change our bedrock duties to our clients of competence and confidentiality.

III. WSBA ADVISORY OPINION 2215 (2012)

(Available on the WSBA web site at www.wsba.org)

This opinion addresses certain ethical obligations related to the use of online data storage managed by third party vendors to store confidential client documents.

Illustrative Facts:

Law Firm contracts with third-party vendor to store client files and documents online on remote server so that Lawyer and Client could access the documents over the Internet from any remote location.

Rules of Professional Conduct Implicated:

RPC 1.1, 1.6, 1.15A

Analysis:

Various service providers are offering data storage systems on remote servers that can be accessed by subscribers from any location over the Internet. This is one aspect of so-called “cloud computing,” and lawyers may be interested in using these services to store confidential client documents and other data. Use of these third party storage systems, however, means that confidential client information is outside of the direct control of the lawyer and raises particular ethical questions.

Under RPC 1.6, a lawyer owes a client the duty to keep all client information confidential, unless the information falls within a specified exception. The duty of confidentiality extends beyond deliberate revelations of client information and requires a lawyer to protect client information against all disclosure. Comment 16 to RPC 1.6 states: “A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3.” In order to use online data storage, a lawyer is under a duty to ensure that the confidentiality of all client data will be maintained.

In addition to client confidentiality, the lawyer is also under a duty to protect client property, under RPC 1.15A. A lawyer using online data storage of client documents is therefore under a duty to ensure that the documents will not be lost.

It is impossible to give specific guidelines as to what security measures should be in place with a third party service provider of online data storage in order to provide adequate protection of client material, because the technology is changing too rapidly and any such advice would be quickly out of date. It is also impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider’s security systems. A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so. While some lawyers may be

able to do more thorough evaluations of the services available, best practices for a lawyer without advanced technological knowledge could include:

1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
2. Evaluation of the provider's practices, reputation and history.
3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer's stored data.
6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.
7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider.

A lawyer has a general duty of competence under RPC 1.1, which includes the duty "to keep abreast of changes in the law and its practice." RPC 1.1 Comment 6. To the extent that a lawyer uses technology in his or her practice, the lawyer has a duty to keep informed about the risks associated with that technology and to take reasonable precautions. The lawyer's duties discussed in this opinion do not rise to the level of a guarantee by the lawyer that the information is secure from all unauthorized access. Security breaches are possible even in the physical world, and a lawyer has always been under a duty to make reasonable judgments when protecting client property and information. Specific practices regarding protection of client property and information have always been left up to individual lawyers' judgment, and that same approach applies to the use of online data storage. The lawyer must take reasonable steps, however, to evaluate the risks involved with that practice and to ensure that steps taken to protect the information are up to a reasonable standard of care.

Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider. Over time, a particular provider's security may become obsolete or become substandard to systems developed by other providers.

Conclusion

A lawyer may use online data storage systems to store and back up client confidential information as long as the lawyer takes reasonable care to ensure that the information will remain confidential and that the information is secure against risk of loss.

Advisory Opinions are provided for the education of the Bar and reflect the opinion of the Rules of Professional Conduct Committee. Advisory Opinions are provided pursuant to the authorization granted by the Board of Governors, but are not individually approved by the Board and do not reflect the official position of the Bar association. Laws other than the Washington State Rules of Professional Conduct may apply to the inquiry. The Committee's answer does not include or opine about any other applicable law than the meaning of the Rules of Professional Conduct. Advisory Opinions are based upon facts of the inquiry as presented to the committee.

IV. PRESENTATION SLIDES

Slide 2

OVERVIEW


- ▶ **Discovery & Social Media**
- ▶ **Cloud Computing**

fucile  reising | LLP

Slide 3

LOGISTICS

- ▶ **Materials**
- ▶ **Questions**

fucile  reising | LLP

Slide 4

DISCOVERY & SOCIAL MEDIA

- ▶ Can be a powerful tool
- ▶ But, there are also some distinct constraints

fucile  reising | LLP

Slide 5

DISCOVERY & SOCIAL MEDIA

- ▶ Begin with an example
- ▶ Follow with the constraints

fucile  reising | LLP

Slide 6

DISCOVERY & SOCIAL MEDIA

The Example

- ▶ Product liability case
- ▶ "Husband" and "Wife" were co-plaintiffs
- ▶ Included loss of consortium claim
- ▶ Presented themselves as a devoted couple
- ▶ Turned out "Husband" and "Wife" hadn't lived together for over 10 years


fucile  reising | LLP

Slide 7

DISCOVERY & SOCIAL MEDIA

The Example

- ▶ Both "Husband" and "Wife" had social media pages with essentially no privacy settings
- ▶ "Wife" also posted comments on "Dr. Phil's" web site
- ▶ Excerpts from "Husband's" video deposition

fucile  reising | LLP

Slide 8


DISCOVERY & SOCIAL MEDIA

The Example

"Husband's" Social Media Page

Q. Mr. [Husband], I'm handing you what I marked as Exhibit 13 . . . That's your Facebook page, right?

A. Yeah. It looks like it.

fucile  reising | LLP

Slide 9

DISCOVERY & SOCIAL MEDIA

The Example

"Husband's" Facebook Page

Q. [T]here's a spot there that says "interests"?

A. . . . Interested in, yes.

Q. And it says what?

A. Women.

fucile  reising | LLP

Slide 10


DISCOVERY & SOCIAL MEDIA

The Example
"Wife's" Dr. Phil Posting

Q. I want to show you Exhibit 10 . . . the posting for May 22, 2006, at 2:31 p.m.

A. Okay...

Q. Would you please read to the ladies and gentlemen of the jury how "Wife" felt about you?

fucile  reising | LLP

Slide 11

DISCOVERY & SOCIAL MEDIA

The Example
"Wife's" Dr. Phil Posting

A. Okay. It says "I raised a husband and have finally escaped after 35 years. It is devastating to him to lose another mommy . . . [I am] so glad I got away."

fucile  reising | LLP

Slide 12

DISCOVERY & SOCIAL MEDIA

The Constraints

- ▶ The "no contact" rule: RPC 4.2
- ▶ Misrepresentation to gain access: RPCs 4.1 and 8.4(c)

fucile  reising | LLP


Slide 13

DISCOVERY & SOCIAL MEDIA

The Constraints

The "No Contact" Rule: RPC 4.2

"In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."

fucile  reising | LLP

Slide 14

DISCOVERY & SOCIAL MEDIA

The Constraints

The "No Contact" Rule

- ▶ Simply viewing static web pages: Permitted
 - ◆ NY State Bar Op. 843 (2010)
 - ◆ OSB Formal Ethics Op. 2005-164 (2005)
- ▶ Interactive communication with a represented opponent: Prohibited

fucile  reising | LLP

Slide 15

DISCOVERY & SOCIAL MEDIA

The Constraints

Misrepresentation to Gain Access: RPCs 4.1 & 8.4(c)

- ▶ "In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person"
- ▶ "It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation . . ."

fucile  reising | LLP


Slide 16

DISCOVERY & SOCIAL MEDIA

The Constraints

Misrepresentation to Gain Access


- ▶ Philadelphia Bar Op. 2009-2 (2009)
- ▶ SD County Bar Op. 2011-2 (2011)
- ▶ NH Bar Op. 2012-1305 (2012)
- ▶ Massachusetts Bar Op. 2014-5 (2014)
- ▶ Pennsylvania Bar Op. 2014-300 (2014)
- ▶ NY City Bar Op. 2010-2 (2010)
- ▶ OSB Formal Ethics Op. 2013-189 (2013)

fucile  reising | LLP

Slide 17

CLOUD COMPUTING


- ▶ Technology
- ▶ Outsourcing

fucile  reising | LLP

Slide 18

CLOUD COMPUTING


- ▶ RPC 1.1: Competence
- ▶ RPC 1.6: Confidentiality

fucile  reising | LLP

Slide 19

CLOUD COMPUTING

▶ **Comments 16-17 to RPC 1.6
“Acting Competently to
Preserve Confidentiality”**

fucile  reising | LLP

Slide 20

CLOUD COMPUTING


▶ **Comment 16:
Putting the accent on
competence**

fucile  reising | LLP

Slide 21

CLOUD COMPUTING


▶ **Comment 17:
Putting the accent on
confidentiality**

fucile  reising | LLP

Slide 22

CLOUD COMPUTING


- ▶ **ABA Ethics “20/20” Amendments**
 - ◆ Comments 16-17 renumbered (to 18-19)

fucile  reising | LLP

Slide 23

CLOUD COMPUTING


- ▶ **ABA Ethics “20/20” Amendments**
 - ◆ Comment 8 to Model Rule 1.1 amended to include “relevant technology”

fucile  reising | LLP

Slide 24

CLOUD COMPUTING

- ▶ **WSBA Advisory Op. 2215**
- ▶ **“20/20” Amendments under review in Washington**


fucile  reising | LLP

Slide 25

CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**

- ◆ Frames the ethical duties when using cloud computing in terms of competence and confidentiality
- ◆ Relies on Comments 16-17


fucile  reising | LLP

Slide 26

CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**
Selection

“A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so.”

fucile  reising | LLP

Slide 27


CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**
“Best Practices”

“1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.

“2. Evaluation of the provider’s practices, reputation and history.

“3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer’s duty of confidentiality and agrees to handle the information accordingly.

fucile  reising | LLP


Slide 28

CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**
“Best Practices”

“4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.

“5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer’s stored data.

fucile  reising | LLP


Slide 29

CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**
“Best Practices”

“6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.

“7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider.”


fucile  reising | LLP

Slide 30

CLOUD COMPUTING

▶ **WSBA Advisory Op. 2215**
Continuing Review


“Because the technology changes rapidly, and the security threats evolve equally rapidly, a lawyer using online data storage must not only perform initial due diligence when selecting a provider and entering into an agreement, but must also monitor and regularly review the security measures of the provider. Over time, a particular provider’s security may become obsolete or become substandard to systems developed by other providers.”

fucile  reising | LLP

Slide 31

FOR FURTHER READING

- ▶ ABA Formal Ethics Op. 466 (2014)
Lawyer Reviewing Jurors' Internet Presence
- ▶ ABA Formal Ethics Op. 462 (2013)
Judge's Use of Electronic Social Networking Media
- ▶ ABA Formal Ethics Op. 11-459 (2011)
Duty to Protect the Confidentiality of E-mail Communications with One's Client

fucile  reising | LLP

Slide 32

QUESTIONS?

fucile  reising | LLP
