

CHAPTER ____

LEGAL CHALLENGES OF THE CLOUD

July 26, 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*. Mark also co-chairs the annual WSBA Law of Lawyering Conference. Before co-founding his small 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
LEGAL CHALLENGES OF THE CLOUD

Mark J. Fucile

- I. ELECTRONIC UPDATE:
NEW WSBA ADVISORY OPINIONS ON METADATA
AND CLOUD COMPUTING
(Reprinted from Mark's November 2012 Ethics & the Law column in the
WSBA Bar News)

- II. OUTSOURCING:
HERE AND THERE
(Reprinted from Mark's June 2010 Ethics & the Law column in 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 UPDATE:
NEW WSBA ADVISORY OPINIONS ON METADATA
AND CLOUD COMPUTING**

(Reprinted from Mark's November 2012 Ethics & the Law column in 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.

II. **OUTSOURCING: HERE AND THERE**

(Reprinted from Mark's June 2010 Ethics & the Law column in the WSBA *Bar News*)

Law firms have been outsourcing both legal and business functions for a long time. Contract lawyers and paralegals are ready examples of the former and computer network and photocopy services are equally ready examples of the latter. Guidance about our duties when we outsource has also been available for a long time. Both the ABA and the WSBA have issued ethics opinions over the years discussing various aspects of outsourcing. The RPCs address the broader concept of lawyers' supervisory duties as have both the Washington Supreme Court and Washington's federal district courts in, respectively, disciplinary and disqualification cases.

More recently outsourcing in the legal profession has taken a new twist with the technical ability to outsource to foreign countries as in a variety of other fields such as software development and "call centers." The same quest for economic efficiency that motivated earlier rounds of outsourcing domestically appears to be driving the current movement overseas. The difference, of course, is that both selection and supervision can be more difficult when outside contractors are across the world rather than across town. The ABA issued an ethics opinion in August 2008 on outsourcing that takes the threads of its earlier advice on the subject and weaves them into the international context. In this column, we'll look at the ethical aspects of outsourcing in both its traditional and newer forms. Whether outsourcing across town or across the globe, key areas from the ethics perspective include the duties of competency, supervision, confidentiality and accurate billing.

Competency. RPC 1.1 requires lawyers to provide competent representation to their clients. Outsourcing differs from co-counsel relationships where a client retains more than one firm to handle a matter and, depending on the arrangements involved, the firms may only be responsible for the discrete tasks for which they were assigned. By contrast, when a lawyer chooses to outsource a portion of the lawyer's work, the lawyer remains responsible for its performance. (*See Tegman v. Accident & Medical Investigations, Inc.*, 107 Wn. App. 868, 876, 30 P.3d 8 (2001), *rev'd on other grounds*, 150 Wn.2d 102, 75 P.3d 497 (2003).) Therefore, it is critical for a firm to undertake "due diligence" to ensure that the provider of the outsourced services can perform them with the requisite skill.

Another element of competent selection involves checking conflicts to avoid disqualification. Depending on such variables as the degree of association with your firm, the nature of the work and confidential information shared, conflicts created by the outsource provider may be imputed to your firm. (*See First Small Business Investment Co. of California v. Intercapital Corp. of Oregon*, 108 Wn.2d 324, 738 P.2d 263 (1987) (analyzing disqualification of associated firms through shared information).) It is important to remember that Washington cases have also examined staff conflicts in determining firm disqualification. (*See, e.g., Oxford Systems, Inc. v. CellPro, Inc.*, 45 F. Supp.2d 1055 (W.D. Wash. 1999); *Daines v. Alcatel, S.A.*, 194 F.R.D. 678 (E.D. Wash. 2000).)

Supervision. Proper supervision lies at the heart of a lawyer’s responsibility for outsourced services regardless of whether the service provider is a lawyer or a nonlawyer. RPC 5.1(b) requires a “lawyer having direct supervisory authority over another lawyer . . . [to] make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.” RPC 5.3(b), in turn, requires a “lawyer having direct supervisory authority over . . . [a] nonlawyer . . . [to] make reasonable efforts to ensure that the person[’]s conduct is compatible with the professional obligations of the lawyer[.]”

ABA Formal Ethics Opinion 88-356 (1988) interpreted RPC 5.1(b) as applying to domestic contract lawyers and ABA Formal Ethics Opinion 08-451(2008) did the same in the international context. RPC 5.3 applies the supervisory duty over retained nonlawyers more explicitly by framing the obligation as applying to any “nonlawyer employed or retained by or associated with a lawyer[.]” The WSBA RPC Committee has applied RPC 5.3(b) in recent informal ethics opinions involving both domestically outsourced legal services (Informal Ethics Op. 2201 (2009) (independent paralegal)) and business services (Informal Ethics op. 2193 (2008) (advertising distribution)). Depending on the circumstances, non-U.S. lawyers who are undertaking outsourced legal work on U.S. law (as opposed to the law of their home country) may be considered “nonlawyers” (like law clerks) for purposes of supervisory duties and, therefore, the more explicit provisions of RPC 5.3(b) may apply.

The practical difficulty of supervising foreign service providers is discussed at length in ABA Formal Ethics Opinion 08-451. The practical difficulty is also highlighted by several Washington disciplinary and disqualification cases invoking the supervisory duty over nonlawyer staff members who were employed directly by the firms involved and who worked in the same offices as their supervisors. *In re Trejo*, 163 Wn.2d 701, 185 P.3d 1160 (2008), for example, concerned a solo practitioner disciplined under RPC 5.3(b) for failing to supervise his assistant who stole client funds. *In re Vanderbeek*, 153 Wn.2d 64, 101 P.3d 88 (2004), also involved a solo practitioner disciplined under RPC 5.3(b) for failing to supervise an office manager who sent clients inaccurate bills. In *Richards v. Jain*, 168 F. Supp.2d 1195 (W.D. Wash. 2001), a firm was disqualified for its handling of an opponent’s privileged information and, in doing so, the court’s opinion focused on a paralegal’s role and the firm’s failure to supervise the paralegal under RPC 5.3(b).

Confidentiality. Comments 16 and 17 to the confidentiality rule, RPC 1.6, are entitled: “Acting Competently to Preserve Confidentiality.” Comment 16 puts the accent on competence: “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.” Comment 17, in turn, shifts the accent to confidentiality: “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.” ABA Formal Ethics Opinion 95-398 (1995), which deals with domestically outsourced computer network services, echoes these duties and couples them with the duty of supervision: “Under Rule 5.3, a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that the service provider will not make unauthorized disclosures of confidential information.” ABA Formal Ethics Opinion 08-451 emphasizes this

duty in the foreign outsourcing context and notes that the legal structures in some foreign countries may not accord the same expectation of privacy provided by U.S. law.

Both ABA Formal Ethics Opinion 88-356, which focuses on domestic outsourcing, and its more recent counterpart, Formal Ethics Opinion 08-451 focusing on foreign outsourcing, grapple with the question of whether advance client consent is necessary before sharing confidential information with an outside service provider. The former assumes that domestic outsourcing often involves close supervision of the outside service provider and concludes that advance consent is not normally required. The latter assumes that foreign outsourcing will usually involve less direct supervision and, therefore, advance client consent is necessary. Both opinions, however, are expressly predicated on those contrasting assumptions and both leave open the converse depending on the level of supervision in individual circumstances.

Accurate Billing. RPC 1.5 governs fees and the Supreme Court has made plain that resulting bills must accurately reflect both time (*In re Dann*, 136 Wn.2d 67, 960 P.2d 416 (1998)) and expenses (*In re Haskell*, 136 Wn.2d 300, 962 P.2d 813 (1998)). ABA Formal Ethics Opinion 93-379 (1993) and WSBA Informal Ethics Opinion 2120 (2006) both address billing for outside nonlawyer services and ABA Formal Ethics Opinion 00-420 (2000) and *In re Marshall*, 160 Wn.2d 317, 335, 157 P.3d 859 (2007), do the same for contract lawyer services. All stress the fundamental requisites for both billing in accord with the attorney-client fee agreement and for billing accurately.

Of particular note, generally no “mark up” is permitted on outside services that are merely passed through to the client. ABA Formal Ethics Opinions 00-420 and 08-451 find that if a contract lawyer is integrated into a firm to such an extent that the lawyer is in practical effect a “contract” associate, then a “surcharge” is permissible on that lawyer’s time in the same way that profit is included in “employee” associate billing rates. Whether the outsourcing is domestic or foreign, however, firms need to carefully assess the nature of the relationship before adding a surcharge without prior client consent.

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

Legal Challenges of the Cloud

Mark J. Fucile


July 26, 2014

WSBA Solo & Small Firm Conference

Slide 2

INTRODUCTION

- ▶ Overview
- ▶ Background
- ▶ Perspective

fucile  reising | LLP

Slide 3

LOGISTICS

- ▶ Materials
- ▶ Questions

fucile  reising | LLP

Slide 4

**TWO PRACTICE TRENDS
WOVEN TOGETHER**


- ▶ Technology
- ▶ Outsourcing

fucile  reising | LLP

Slide 5

**TWO CORE DUTIES
WOVEN TOGETHER**


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

fucile  reising | LLP

Slide 6

**TWO CORE DUTIES
WOVEN TOGETHER**


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

fucile  reising | LLP

Slide 7

**TWO CORE DUTIES
WOVEN TOGETHER**


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

fucile  reising | LLP

Slide 8

**TWO CORE DUTIES
WOVEN TOGETHER**

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


fucile  reising | LLP

Slide 9

**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **ABA Ethics “20/20”
Amendments**


◆ **Comments 16-17 renumbered
(to 18-19)**

fucile  reising | LLP

Slide 10

**TWO CORE DUTIES
WOVEN TOGETHER**


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

fucile  reising | LLP

Slide 11

**TWO CORE DUTIES
WOVEN TOGETHER**


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

fucile  reising | LLP

Slide 12

**TWO CORE DUTIES
WOVEN TOGETHER**

- ▶ **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 13

**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **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 14


**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **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 15

**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **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 16

**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **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 17

**TWO CORE DUTIES
WOVEN TOGETHER**

▶ **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 18

WASHINGTON IN CONTEXT

▶ **Regionally**


- ◆ **Oregon State Bar
Formal Opinion 2011-188**
- ◆ **California State Bar
Formal Opinion 2010-179**

fucile  reising | LLP

Slide 19

WASHINGTON IN CONTEXT


- ▶ **Nationally**
 - ◆ **ABA 20/20 Amendments**
 - ◆ **ABA Legal Technology Resource Center**

fucile  **reising** | LLP

Slide 20

IMPLICATIONS

- ▶ **Regulatory**
- ▶ **Civil Liability**

fucile  **reising** | LLP

Slide 21

SUMMING UP

- ▶ **Core duties of competence and confidentiality**
- ▶ **If we use technology, we need to know enough to use it consistent with our duties**

fucile  **reising** | LLP

Slide 22

QUESTIONS?

fucile  reising | LLP
