2012 Family Law Seminar

ISBA CLE

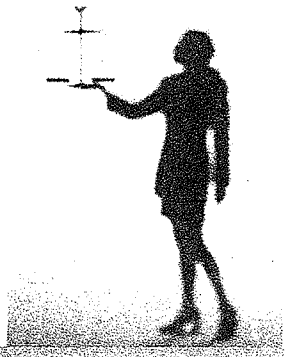
Protecting Lawyer and Client Electronic Information

8:45 a.m.-9:45 a.m.

Presented by:

Erik S. Fisk
Whitfield & Eddy, P.L.C.
317 Sixth Ave. Suite 1200
Des Moines, Iowa 50309
Phone: (515) 288-6041
Fax: (515) 246-1474

Michael Alft
Iowa Support Master
Alft & Wilson Publishing
Phone: (800) 735-9426



Friday, October 26, 2012

DIVORCE IN THE CLOUD: CLIENT AND ATTORNEY CAVEATS FOR CLOUD AND ELECTRONIC ISSUES IN FAMILY LAW

Erik S. Fisk
Whitfield & Eddy, P.L.C.
317 Sixth Ave., Suite 1200,
Des Moines, Iowa 50309-4195
(515) 288-6041
www.linkedin.com/in/eriksfisk
twitter: eriksfisk

I. OVERVIEW, DEFINITIONS, AND INTRODUCTION

What is Cloud computing? Particularly for attorneys, who generally do not come from math and science backgrounds, this is a difficult concept for a layperson to get her head around. There are also many different definitions, some of which are quite outdated. The most precise and clear definition is provided by the National Institute of Standards and Technology, of the United States Department of Commerce, and is set forth in "The NIST Definition of Cloud Computing."[1] The broad overall definition is as follows:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. [2]

The essential characteristics of the model are as follows:

> *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

---

1 Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing." , NIST Special Publication 800-145, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last accessed October 5, 2012).

2 Id.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability [usually as a pay/charge per use] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.[3]

The service models include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), which are defined as follows:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[4]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [e.g., iCloud, Google Docs, Salesforce, Dropbox, Citrix, Facebook, Flickr]

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including

---

3 Id.

4 A cloud infrastructure is definied in the standard as "the collection of hardware and software that enables the five essential characteristics of cloud computing." Id. It includes both the physical layer of the hardware resources, including servers, storage, and network components and the "abstraction layer," which is the software deployed across the physical layer. Id.

network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. [e.g., Digital Ocean, Heroku – for developers/programmers]]

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). [e.g., Amazon Web Services, Flexiscale][5]

Typically, then, when most laypersons talk about the "cloud," they mean to talk about the SaaS service model, which is what this presentation will mostly focus on. Finally, as to deployment, the classification of the cloud can be explained as one of the following:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

---

5 Id.

II. CLOUD COMPUTING ON "OUR" SIDE

Cloud computing has made its way into the practice management of many firms.[6] Ranging from simple administrative computing applications or sharing protocols to full range and full scale document collaboration, case management applications , or more specifically to web enabled document automation.

Attorneys, as with any new form of technology, should weigh the benefits of use against the risks. By choosing to use cloud computing, the attorney must find ways to minimize the risks that may arise from this form of technology in practice management.

State bar authorities appear to have come to a consensus that the cloud computing concept is appropriate under the right circumstances.[7] All appear to require some degree of reasonable care on the part of the attorney to safeguard the confidentiality and security of information. The ABA adds that, in addition to consulting with their local bar authorities, attorneys should have an understanding of: "1) the nature of the law firm's relationship with the cloud computing software provider, and 2) best practices for the use of the cloud computing applications."[8]

Many SaaS vendors rely on a virtualization model to use virtual machines to let multiple subscribers maintain personalized desktops on a single, centrally located computer or server.[9] The central machine may be anywhere. All users, who may or may not be accessing the machine

---

6 "Guidelines for the Use of Cloud Computing in Law Practice, eLawyering Task Force, American Bar Association, Jan. 15, 2011, available at http://meetings.abanet.org/webupload/commupload/EP024500/relatedresources/cloudcomputingguidelines05.30.2011.pdf (last accessed October 5, 2012).

7 Attached as Exhibit "A" is a chart of the positions various state bar associations have taken on the issue, along with a basic summary of the position.

8 Guidelines, supra, note 6.

9 Id.

from the same location, will all be connected to the machine via some form of network or the internet.

Whether the vendor addresses security itself or uses a third-party hosting company, you should review the service level agreement (SLA) with an eye toward the support, confidentiality, and maintenance of attorney or law firm data.[10] Specific issues identified by the ABA to look for in the SLA include:

1. Make sure there are data return and retention policies. Return of data should be in a readable format and within a reasonable amount of time upon request.

2. Understand how the provider would handle government and civil search and seizure actions if handed a subpoena to deliver the contents of your law office.

3. Check for geo-redundancy of the servers or if there is data escrow offered through companies with servers located overseas. Servers located outside of the United States may be subject to international laws. Make sure that the servers are housed in Tier4[11] data centers.

4. Make sure the provider's services are in compliance with Federal Regulations. For example, make sure the service is Peripheral Component Interconnect (PCI) compliant if the provider will be collecting credit card information.

5. Look for a clear definition of the "use of the service" as it relates to the following: server memory, CPU time, hard drive space, growth of storage space used, "reasonable use" of the network, including computer hardware, network servers, and/or any third-party computer software programs used by the provider to host the service.

6. Understand how backups, maintenance and updates to the service are handled. Data should remain encrypted and only decrypted with the permission of the attorney. Does the provider conduct regular security audits? How often are data backups conducted?

---

10 Id.

11 American National Standards Institute (ANSI) Telecommunications Infrastructure (TIA) Standards for Data Centers, ANSI/TIA-942, defines a tiered structure for data center safety, security, and availability, from Tier 1 (least security), to Tier 4. Tier 4 centers include the following summary characteristics: meets or exceeds all Tier 1, Tier 2 and Tier 3 requirements; all cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems; fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995% per year (can be down only .4 hours per year). Industry experts estimate Tier 3 facilities are twice as expensive as Tier 1 facilities to build and higher Tier facilities take decidedly longer to implement.

7. Who has access to the law office data? Look for confidentiality, privacy policy and nondisclosure statements.

8. Consider whether the software services provider maintains an Internet Media policy that insures against data loss. The malpractice policy of the law firm may not provide coverage for data loss, and to secure a separate policy for this kind of coverage may be prohibitive, particularly for solo practitioners and small law firms. It is easier for the service provider to secure this coverage and spread the cost over all of the law firm clients they are servicing. The attorney is always responsible for keeping a client's data confidential and has financial exposure if it is disclosed, even if the disclosure is inadvertent. A claim against the software services provider for data loss that is covered by an insurance policy would mitigate the financial impact on the law firm.[12]

Finally, the technology is always changing. Because it changes so rapidly, the ABA does not, nor can it, give a predictive list of security requirements and standards. Instead, they recommend the following basic requirements to help the lawyer or law firm keep up with the technology to benefit both the law business and clients:

1. Keep up to date on the security issues related to the use of the technology chosen for the law firm. Designate an attorney at the firm who is responsible for this task or retain the services of an IT consultant familiar with implementing cloud solutions in a law firm environment.

2. Consider establishing a law firm policy covering the best practices for use of cloud computing applications by firm members, including the firm's use of online social media applications.

3. Attorneys using cloud computing applications on mobile devices, might follow these basic security tips:

   - If you use wireless networking, ensure that all wireless traffic is encrypted with WPA2. [the older, WEP encryption can be hacked in a manner of seconds]
   - Keep antivirus software and all software patches updated. Turn on the software firewall for the computer.
   - Use a safer browser, such as Mozilla with the No Script add-on installed, or use another pop-up blocker.
   - Avoid free Wi-Fi hotspots when using any cloud computing application remotely. Use a cellular phone modem adapter instead.

---

12 Guidelines, supra note 6.

4. Never write down usernames and passwords for access to any cloud computing application. Make sure that the passwords you create are strong and change them regularly. If you have a number of passwords, use an application like KeePass to organize them all.[13]

III. CLOUD COMPUTING AND ELECTRONIC INFORMATION ON THE CLIENT'S SIDE - THE GOOD, THE BAD, AND THE UGLY

Even for less savvy clients, the availability of "spy gear" and simple creative ingenuity has opened up avenues for access to vast expanses of information. For example, consider the traditional example of the sly spouse who wishes to obscure or eradicate accurate records of finances and assets. The sly spouse may shred documents, secret them in a safety deposit box, or move books, documents, or even cash or assets with friends or family.

The electronic world opens up both a whole new world of places to hide and a slew of ways to track hidden information. At the most basic level, web surfing histories and social networks leave traces of hidden accounts, transfers, or business deals. Keyloggers or keylogging software can keep track of web traffic, passwords and communications with others. GPS tracking and smartphone apps can track ATM withdrawals, secret business meetings, and the like.

Consider some of the following recent examples:

(1) One woman used keylogger software to find her husband's hidden bank accounts[14];

(2) By monitoring LinkedIn, one woman learned her husband had a secret businesses he had been lying about;

(3) A man analyzed his wife's text messages and found details of her secret life with secret assets;

(4) One spouse created a Paypal account to finance an extramarital affair;

---

13 Guidelines, supra note 6.

14 This, and the following examples, are taken from Veronica Dagher, "Why Hiding Money From Your Spouse Has Gotten a Lot Harder," Wall St. J., April 12, 2012

(5) A woman discovers her husband's secret bank account – after she analyzes the information from a keylogger he surreptitiously installed, but she later found out about and brought to an expert;

(6) A woman uses the "find my phone" software on her family's smartphones (to use the onboard GPS to pinpoint the phone's location) and learned of her husband's trips to an ATM (where he withdrew cash she didn't know about) a strip club, jewelry stores, and multiple girlfriends' apartments; and

(7) A man brings his wife's smartphone to an expert who examines the text messages and finds she is hiding assets and using text messages to set up drug sales. Even worse, she was leading a double life, with multiple boyfriends, sex clubs, and she had even hired a hit man to kill her husband while she was on vacation.

The pattern, at least insofar as it involves financial infidelity, appears to be widespread. The National Endowment for Financial Education reports that 31% of United States adults who combined assets with a spouse or partner say they have been deceptive about money, and 58% of these adults say they hid cash from their partner or spouse.[15] One interesting phenomenon of the cloud is that, sometimes, the information does not go away. Facebook, for example, is well-known for having photographs and entire user accounts that have been "deleted" by the user but are still available years afterward.[16] At the very least, this underscores the basic point that that users lose control of data when they put it in others' hands.

A. POTENTIAL CLIENT LIABILITIES

Of course the potential dangers exist with the federal and Iowa wiretap statutes, the tort of invasion of privacy, spoliation of evidence, and the admissibility of electronic evidence, all of which introduce additional layers of analysis.

---

15 Id.

16 Jacqui Cheng, "Over 3 Years Later, "Deleted" Facebook Photos are Still Online," Arstechnica, available at http://arstechnica.com/business/2012/02/nearly-3-years-later-deleted-facebook-photos-are-still-online (

1. FEDERAL WIRETAP, STORED COMMUNICATIONS ACT, AND STATE EQUIVALENT - OVERVIEW

Generally, the law provides that if the retrieved messages were stored on a home computer to which both spouses have equal access, there is most likely not a violation of the law. Recording telephone and face to face conversations and accessing e-mail and voicemail, though, are regulated by federal and state wiretap statutes. Improper retrieval of electronic communications can constitute a violation of the Electronic Communications Privacy Act of 1986 (the "ECPA"). It is best to tread lightly, because penalties can be severe.

The federal and Iowa's statute prohibit the electronic interception of a voice communication except when at least one party to the communication knows of and consents to the interception at the time of interception. 18 U.S.C. §§ 2510 et seq.; Iowa Code Chapter 808B (2011). While this issue becomes complicated when attorneys are involved in the interception or recording, as further discussed below, there are some general guidelines that help clarify individual's obligations with respect to these communications.

The Federal Wiretap Act was initially enacted in 1968 under Title III of the Omnibus Crime Control Act. The statute was commonly referred to as the "Wiretap Act" or "Title III." In 1986, the federal statute was amended and is now the Electronic Communication Privacy Act (the "ECPA") (18 U.S.C. §§ 2510-3127). Although not technically accurate, some courts and commentators continue to speak of the federal statute as "Title III." The ECPA amended the federal Wiretap Act to include cell phone conversations within the restrictions placed on wiretapping.

The ECPA Amendments to the Wiretap Act divided the Act into Titles I, II, and III. What was previously Title III is now Title I of the ECPA. Title I (18 U.S.C. §§ 2510-2522) of

the ECPA (or the Wiretap Act) regulates the electronic surveillance of conversations, which can also include email conversations. Title II (18 U.S.C. §§ 2701-2711) of the ECPA (also referred to as the "Stored Communications Act") regulates access to e-mail, fax communications and voicemail. Title III (18 U.S.C. §§ 3121-3127) of the ECPA regulates call-tracing devices such as caller ID. The two titles relevant to the discussion herein are Title I and Title II. I will refer to Title I as the "Wiretap Act," and I will refer to Title II will be referred to as the "Stored Communications Act" (or the SCA).

The Wiretap Act imposes criminal and civil liability for intentional "interceptions" of "electronic communications."[17] Actual and punitive damages may be recoverable. "Minimal" liquidated damages of $10,000 may be imposed for violations of the Wiretap Act.[18] The language in Section 2520 of the Wiretap Act was changed from "shall be entitled to damages" to providing that a court "may" assess damages. Courts have interpreted the change to mean that a damages award is discretionary and have refused to award damages for de minimis violations of the Wiretap Act. The Wiretap Act also includes an exclusionary rule that prohibits courts and administrative agencies from admitting into evidence the content of taped conversations that are acquired in violation of the statute.[19] Attorney's fees and court costs are also available to the prevailing party.

Access to e-mail and voicemail by individuals is primarily regulated under Title II, the Stored Communications Act. This Act prohibits any person from "intentionally accessing

---

17 18 U.S.C. § 2511.

18 18 U.S.C. § 2520.

19 18 U.S.C. § 2515.

without authorization of a facility through which an electronic communication service is provided . . . and thereby obtains . . . access to a wire . . . communication while it is in storage in such system."[20] Under the more recently enacted USA PATRIOT ACT (the Patriot Act) amendments to the ECPA, voicemail is now treated as e-mail.

The Stored Communications Act protects against unauthorized "access" to "electronic communication while it is in electronic storage."[21] This Act provides protection for private communication only during the course of transmission. Because of the way "electronic storage" is defined under the Act, messages that are in post-transmission storage after transmission is complete are not covered under the definition of "electronic storage." Therefore, retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission.

The SCA may also apply to cloud providers. The SCA prohibits service providers from disclosing electronic information, except in specified circumstances. Thus, a Cloud provider will likely resist the disclosure of information in response to a subpoena focused on information not owned by the provider. The SCA applies to providers of electronic communications services ("ECS"), and to providers of remote computing services ("RCS").[22] A Cloud service provider may fall into either category, or both. It may be an ECS provider if it gives its users "the ability

---

20 18 U.S.C. § 2701.

21 18 U.S.C. § 2701.

22 18 U.S.C. § 2702.

to send or receive wire or electronic communications," such as email.[23] An ECS provider cannot "knowingly" disclose "the contents of a communication" that it is holding in electronic storage.[24] A Cloud provider can also be an RCS provider if it provides "computer storage or processing services" that use an "electronic computing system."[25] The RCS provider cannot "knowingly" disclose "the contents of any communication" which it transmits or holds in storage for a customer or subscriber where the communication is transmitted or held "solely for the purpose" of providing a service to the customer or subscriber.

Whether considered an ECS, RCS, or both, the SCA generally prohibits a Cloud provider from disclosing the content of communications that it transmits or holds for its users.[26] There are exceptions permitting disclosure, but few typically apply in civil litigation. In most circumstances, a Cloud provider cannot disclosure information in response to a Rule 45 subpoena seeking the production of electronic communications absent the "lawful consent" of either the sender or recipient of a communication.

2. INVASION OF PRIVACY

Iowa has recognized a tort right to privacy in common law. The common law privacy intrusion tort is violated if someone intentionally intrudes upon the private affairs, seclusion or solitude of another person by means that would be highly offensive to a person or ordinary

---

[23] 18 U.S.C. §§ 2510(15), 2711(1) (adopting and incorporating section 2510).

[24] 18 U.S.C. § 2702(a)(1).

[25] 18 U.S.C. § 2711(2).

[26] Most require a waiver to provide any information at all. An example is attached as Exhibit C.

sensibilities. In cases where wiretap acts may not be violated, the common law invasion of privacy tort may apply to these forms of surveillance. A violation of the invasion of privacy tort might result in an award for compensatory damages, and it may "poison" a party's testimony or rights to receive rights to equitable distribution of assets.

Under the Restatement (Second) of Torts, the right to privacy can be violated by: "(a) unreasonable intrusion upon the seclusion of another . . .; or (b) appropriation of the other's name or likeness . . .; or (c) unreasonable publicity given to the other's private life . . .; or (d) publicity that unreasonably places the other in a false light before the public . . . ."[27]

Under the "intrusion upon seclusion" theory, the Iowa Supreme Court upheld a violation on one spouse's surreptitious recording of his wife in the bedroom, where the Supreme Court said she had an "expectation of privacy."

3. SPOLIATION

Spoliation is the intentional destruction of evidence.[28] The courts punish spoliators because the lost evidence is often the most revealing and reliable evidence, and because of the unfairness that would result if a party were allowed to destroy evidence and then benefit from the absence of the evidence.[29]

To avoid the possible loss of crucial evidence or to obtain the benefit of the spoliation presumption, a requesting party should put a prospective producing party on notice at the earliest

[27] In re Marriage of Tigges, 758 N.W.2d 824, 829 (Iowa 2008) (citing Restatement (Second) of Torts § 652A(2)).

[28] Hendricks v. Great Plains Supply Co., 609 N.W.2d 486, 491 (Iowa 2000).

[29] Bart S. Wilhoit, Spoliation of Evidence: The Viability of Four Emerging Torts, 46 UCLA L. Rev. 631 (1998).

possible time that any potentially relevant electronic information should be preserved.[30] The theory with these notices is that they should spell out the steps the responding party should take to avoid either the deliberate or accidental destruction of data. Common examples are requests to preserve backup files, suspend routine maintenance, suspend backup recycling practices, and suspend any destruction policies.

IV. WHAT ABOUT ATTORNEY PARTICIPATION/ADVICE IN SLEUTHING?

What should we advise our clients about snooping and sleuthing? A related question is what is the proper level (if at all) of attorney involvement in any snooping or sleuthing? One way to approach this question is through the analogue of telephone recording, which is a little clearer in Iowa and across the nation (though there are disagreements). A fine analysis of the issue of attorney involvement in the recording of telephone conversations is contained in a Congressional Research Service publication authored by Charles Doyle, an attorney specialist in Public Law.[31]

The issue is first framed by a pair of decisions issued by the American Bar Association. The first was issued in 1974, where the ABA concluded in Formal Opinion 337 that the rule covering dishonesty and fraud "clearly encompasses the making of recordings without the consent of all parties." As a result, the ABA cautioned that, "no lawyer should record any conversation whether by tapes or other electronic device, without the consent or prior knowledge of all parties to the conversation." Only a minimal exception for law enforcement officials working within "strictly statutory limitations" was carved out from the opinion's broad proscription.

---

[30] See Exhibit C – Request to Preserve

[31] Charles Doyle, "Wiretapping, Tape Recorders, and Legal Ethics: An Abridged Overview of Questions Posed by Attorney Involvement in Secretly Recording Conversation," CRS Report R42649, available at http://www.fas.org/sgp/crs/misc/R42649.pdf (last accessed October 3, 2012).

In 2001, the ABA issued Formal Opinion 01-422, which rejected the broad approach to Opinion 337. Instead, the ABA's 2001 decision provided the following guideposts:

> 1. Where nonconsensual recording of conversations is permitted by the law of the jurisdiction where the recording occurs, a lawyer does not violate the Model Rules merely by recording a conversation without the consent of the other parties to the conversation.
>
> 2. Where nonconsensual recording of private conversations is prohibited by law in a particular jurisdiction, a lawyer who engages in such conduct in violation of that law may violate Model Rule 8.4, and if the purpose of the recording is to obtain evidence, also may violate Model Rule 4.4.
>
> 3. A lawyer who records a conversation without the consent of a party to that conversation may not represent that the conversation is not being recorded.
>
> 4. Although the Committee is divided as to whether the Model Rules forbid a lawyer from recording a conversation with a client concerning the subject matter of the representation without the client's knowledge, such conduct is, at the least, inadvisable.

The Iowa Supreme Court Board of Professional Ethics and Conduct, Ethics Opinion 98-28 has taken the position that attorneys can advise their clients to record contacts initiated by an alleged abuser for protected parties who are entitled to protection from such alleged abuser under a domestic abuse order.

However, the rule is different for attorneys who do the recording themselves. Iowa Supreme Court Board of Professional Ethics and Conduct, Ethics Opinion 83-16 (1982), takes the following position for attorneys recording conversations: "With certain exceptions spelled out in this opinion [relating to recording for purposes of law enforcement investigations], no lawyer should record any conversation whether by tapes or other electronic device, without the consent or prior knowledge of all parties to the conversation." While many states have taken a different approach, based on the ABA's cue, Iowa has as of yet declined to do so and, in fact,

reaffirmed the position taken in 83-16 later in 1995 in Ethics Opinion 95-09 (1995).

The Iowa Supreme Court adopted this approach in Iowa State Bar Association v. Mollman, 488 N.W.2d 168, 169-70, 171-72 (Iowa 1992). In Mollman, the attorney was disciplined for wearing a "wire," at the insistence of the FBI (and in the hope of more lenient sentencing) to set up a former client and long-time friend to the discuss the latter's cocaine usage. The Iowa Supreme Court applied the logic and reasoning of Opinion 83-16 and DR 1-102(A)(4) and 4-101(B) (stating a lawyer shall not knowingly reveal the confidence or secret of a client or use them to the lawyer's own advantage.

While Mollman was an extreme example, it is still the current law, and it appears to suggest that a lawyer can be disciplined for recording a conversation that would not otherwise violate the wiretap act.

V. CONCLUSION

It is important to think about the cloud as another source of potentially relevant information. Cloud users and thoughtful practitioners should add "the cloud" to the checklist of sources where potentially relevant material should be preserved, collected and reviewed when litigation is reasonably anticipated and explored if it may be relevant to the matters in dispute. That said, complexities in cloud discovery arise out of the different relationship a user may have to his or her data given the intervening variable of a cloud service provider and the likelihood that key information governance questions – including those relating to record retention, e-discovery and data privacy – may be unknown not even to the request, but even the user himself.

EXHIBIT A – CLOUD COMPUTING (SAAS) PERMITTED

Jurisdiction	Permitted?	Standard?	Specific Requirements or Recommendations*
ALABAMA Opinion 2010-02	Yes	Reasonable Care	• Know how provider handles storage/security of data. • Reasonably ensure confidentiality agreement is followed. • Stay abreast of best practices regarding data safeguards.
ARIZONA** Opinion 09-04	Yes	Reasonable Care	• "Reasonable security precautions," including password protection, encryption, etc. • Develop or consult someone with competence in online computer security. • Periodically review security measures.
CALIFORNIA Opinion 2010-179	Yes	Reasonable Care	• Evaluate the nature of the technology, available security precautions, and limitations on third-party access. • Consult an expert if lawyer's technology expertise is lacking. • Weigh the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions.
IOWA Opinion 11-01	Yes	Reasonable Care	• Ensure unfettered access to your data when it is needed, including removing it upon termination of the service. • Determine the degree of protection afforded to the data residing within the cloud service.
MAINE** Opinion 194	Yes	Reasonable Care	• Vendor and possibly its employees should have an enforceable obligation to maintain confidentiality. • Vendor should notify if there's any type of breach. • Data should be transmitted to the vendor in a secure fashion.

MASSACHUSETTS Opinion 12-03	Yes	Reasonable Care	• Review (and periodically revisit) terms of service, restrictions on access to data, data portability, and vendor's security practices. • Follow clients' express instructions regarding use of cloud technology to store or transmit data. • For particularly sensitive client information, obtain client approval before storing/transmitting via the internet.
NEW JERSEY** Opinion 701	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security. • Use available technology to guard against foreseeable attempts to infiltrate data..
NEW YORK Opinion 842	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data. • Use available technology to guard against foreseeable attempts to infiltrate data. • Investigate vendor security practices and periodically review to be sure they remain up-to-date. • Investigate any potential security breaches or lapses by vendor to ensure client data was not compromised.
NEVADA Opinion 33	Yes	Reasonable Care	• Chose a vendor that can be reasonably relied upon to keep client information confidential. • Instruct and require the vendor to keep client information confidential.
NORTH CAROLINA 2011 Formal Ethics Opinion 6	Yes	Reasonable Care	• Review terms and policies, and if necessary re-negotiate, to ensure they're consistent with ethical obligations. • Evaluate vendor's security measures and backup strategy. • Ensure data can be retrieved if vendor shuts down or lawyer wishes to cancel service.

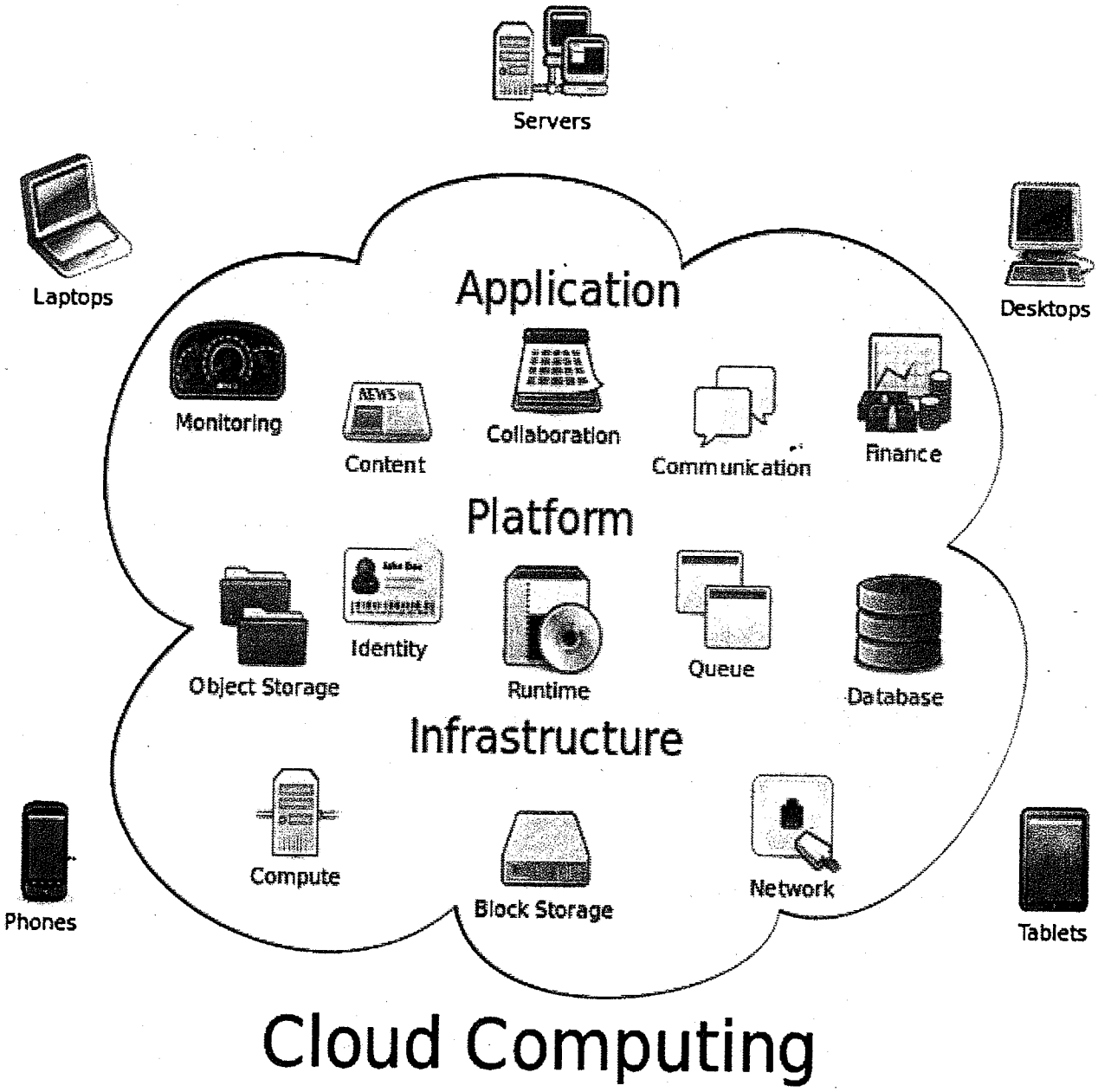
OREGON Opinion 2011-188	Yes	Reasonable Care	• Ensure service agreement requires vendor to preserve confidentiality and security. • Require notice in the event that lawyer's data is accessed by a non-authorized party. • Ensure adequate backup. • Re-evaluate precautionary steps periodically in light of advances in technology.
PENNSYLVANIA Opinion 2011-200	Yes	Reasonable Care	• Exercise reasonable care to ensure materials stored in the cloud remain confidential. • Employ reasonable safeguards to protect data from breach, data loss, and other risk. • See full opinion for 15 point list of possible safeguards.
VERMONT Opinion 2010-6	Yes	Reasonable Care	• Take reasonable precautions to ensure client data is secure and accessible. • Consider whether certain types of data (e.g. wills) must be retained in original paper format. • Discuss appropriateness of cloud storage with client if data is especially sensitive (e.g. trade secrets).

* Note that in most opinions, the specific steps or factors listed are intended as non-binding recommendations or suggestions. Best practices may evolve depending on the sensitivity of the data or changes in the technology.

** These opinions address issues which aren't directly labeled cloud computing or software as a service, but which share similar technology (e.g.. online backup and file storage).

Table from ABA Law Practice Management Section, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (accessed October 1, 2012).

EXHIBIT B – OVERVIEW AND VISUAL REPRESENTATION OF CLOUD COMPUTING CONCEPTS



**This image, "Diagram showing overview of cloud computing including Google, Salesforce, Amazon, Axios Systems, Microsoft, Yahoo & Zoho" was created by Sam Johnston and is used under the terms of the Creative Commons Attribution-Share Alike 3.0 Unported license.

EXHIBIT C – SAMPLE RELEASE TO ACCESS CLOUD INFORMATION

AUTHORIZATION FOR THE RELEASE OF PRIVATE/CONFIDENTIAL ELECTRONIC RECORDS

I, _____, hereby authorize _____

(Full name of individual) (name of provider)

Pursuant to said provider(s) obligations under the Stored Communications Act of 1986, 18 U.S.C. § 2701-2703, and other applicable state and federal law protecting my private and confidential information, to release my private and confidential records, as specified below, to:

Name _____

Title/Organization_____

I specifically authorize the provider to provide the following personal/confidential information:

_X_ Electronic mail or "instant message" or similar program logs, stored in any folder or format, whether in any inbox, custom folder, sent folder, including any and all such drafts thereof, and any such records that were deleted but are still retrievable.

This authorization shall be valid for a period of one year from the date of signature.

_____ _____

Signature of Individual DATE

EXHIBIT D – SAMPLE REQUEST TO PRESERVE

Dear Opposing Counsel:

By this letter, you and your client are hereby given notice not to destroy, conceal, or alter any paper or electronic files and other data generated by and/or stored on your client's computers and other electronic computing devices and storage media (e.g., flash drives; unique, non-commercial recorded CD or DVD storage media; hard drives or disks, backup tapes), or any other repository for the storage of electronic data. Please note that this notice applies both to computing devices, storage media, and other electronic data in which your client has a personal ownership interest, as well as those of the business(es) in which she has an interest, and those to which your client has access or control but that are otherwise in the possession of a third party.

As you know, your client's failure to comply with this notice can result in sanctions for spoliation of evidence or potential evidence. Through discovery, we expect to obtain from you a number of documents and things, including files stored on your client's computers and on your client's computer storage media.

You will soon receive initial interrogatories and requests for documents and things. We will request that any such data requested by produced in its original format. Electronic information in its native format contains relevant, discoverable information beyond that which may be found in printed documents.

Courts have made it clear that all information available on electronic storage media is discoverable, whether readily readable ("active") or recently "deleted." Accordingly, electronic information subject to our discovery requests and that we believe your client is obligated to maintain (and not alter or destroy), includes but is not limited to the following:

(1) All digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including the drives or disks used by your client's computing devices and backup media (e.g., other drives, backup tapes, data ports, keys, disks, CD-ROM or DVD-ROMs), whether owned by your client or subject to your client's access, custody, or control;

(2) Any and all e-mails, both sent and received, whether internally or externally including any and all attachments thereto;

(3) All electronic files contributed to, produced by, or directed to your client, including word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management, and personal information management software (such as Microsoft Outlook, Google Calendar, or Lotus Notes); all data created with the use of smartphones, personal data assistants, or other Windows-

based, or pocket PC devices; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches, and "cookies" files generated at the workstation of each employee and/or agent in your client's business and on any and all backup storage media; and

(4) any and all other files subject to your client's access, custody, or control, generated by users through the use of computers and/or telecommunications, including but not limited to voicemail.

Further, you and your client are to preserve and not destroy any of the following:

(1) log or logs of network use by your client personally or by him at the business(es) in which the parties' have any right to access, custody, or control;

(2) all copies of backup tapes or drives and the software necessary to reconstruct the data on those tapes, so that there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every computer (and/or workstation) and network server in the client's control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from _____ to the present;

(3) all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view, and (if necessary) reconstruct any discoverable electronic data.

Concerning any electronic data created after the date of delivery of this letter, any discoverable evidence is not to be destroyed, and your client is to take whatever steps are appropriate to avoid destruction of evidence. Any and all media storage devices containing potentially discoverable information should not be disposed of due to upgrades, failures, or any other reason.

To ensure your and your client's obligations to preserve documents and things will be met, please forward a copy of this letter to your client and any and all persons and entities with custodial responsibility for the items referred to in this letter.

Thank you for your attention to this matter.

Very truly yours,

Signing Attorney[32]

32