INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION

2013 IMLA Mid-Year Seminar

Tuesday, April 16, 2013

Work Session IX – Ethics

20/20 Vision or Short-Sighted? Ethics, Client Data, the Cloud, and Amended Comment 6 to ABA Model Rule 1.1

by

PETER B. HASKEL

City of Dallas
City Attorney's Office
1500 Marilla, 7BN
Dallas, Texas 75201
¶

©2013 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2013 Mid Year Seminar, held April 14-16, 2013 in Washington, DC. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Work Session IX - Ethics 20/20 Vision or Short-Sighted? Ethics, Client Data, the Cloud, and Amended Comment 6 to ABA Model Rule 1.1

PETER B. HASKEL
City of Dallas
City Attorney's Office
1500 Marilla, 7BN
Dallas, Texas 75201

INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION
2013 IMLA Mid-Year Seminar

Tuesday, April 16, 2013, 9:00 - 10:15 AM

¶

Table of Contents

I. INTRODUCTION 1
A. Few if any state lawyer ethics rules explicitly address cloud computing 1
B. Questions 1
1. Inconsistent Standards for Tech Ethics? 1
2. Confuting Lawyer & Technician Responsibilities? 1
3. Must Lawyers Be Technologists? 1
C. This outline addresses only ethical standards. 1
D. Where is the border between UPL and technology when lawyers must apply tech knowledge to legal practice? 2
II. QUESTION: WHAT IS CLOUD COMPUTING? 2
A. Outsourcing of computer resources is not new. 2
B. NIST Definition of Cloud Computing 2
1. Essential Characteristics 2
2. Service Models:[] 3
3. Deployment Models: 4
C. Additional Resources on Cloud Computing Generally 4
III. CLIENT CONFIDENTIALITY IN CONTEXT OF CLOUD COMPUTING – GENERALLY ..5
A. Useful references from NIST on Cloud Security & Privacy 5
B. ABA Ethics 20/20 Commission (Preliminary Issues Identification – Prior to Finalized Model Rules Amendment Adoption by House of Delegates on Aug. 6, 2012) 6
IV. STATE ETHICS OPINIONS 7
A. ABA On-Line Chart of Cloud Ethics Opinions Around the U.S. 7
B. State Ethics Opinions 7
1. Alabama 7
2. Arizona 9
3. California 10
4. Iowa 10
5. Maine 10
6. Massachusetts 11
7. Nevada 11
8. New Jersey 11
9. New York 12
10. North Carolina 12
11. Oregon 13
12. Pennsylvania 13

13. Texas 14

14. Vermont 14

C. There are real risks from using cloud computing. 14

D. Some Developing Though not Uniform Trends in State Ethics Opinions 15

1. investigation of vendor competence & trustworthiness – beyond that required for other outsourcing; 15

2. "Legally enforceable" vendor obligation to preserve confidentiality & make data available back to lawyer; 15

3. Lawyer's obligations may evolve based on technology developments; 15

V. HOW WOULD 2012 REVISED ABA MODEL RULES CHANGE EXISTING ETHICAL STANDARDS? 15

OVERARCHING ISSUE: WHEN AND TO WHAT EXTENT IS A LAWYER SUPPOSED TO HAVE TECHNOLOGICAL COMPETENCE? PUT ANOTHER WAY: WHEN DOES LEGAL COMPETENCE ENCOMPASS TECHNOLOGICAL COMPETENCE 15

A. Competent Representation 15

B. Client Confidentiality 16

C. Safekeeping Property & Respecting Others' Rights 17

D. Responsibility for Cloud Vendors 19

VI. RELATIVISTIC ETHICS: DUE DILIGENCE TO PROTECT CLIENT CONFIDENTIALITY FOR CLOUD COMPUTING COMPARED TO DUE DILIGENCE FOR OTHER OUTSOURCING 20

VII. SOME SECURITY & CONFIDENTIALITY CONCERNS IN NEGOTIATING CLOUD SERVICE AGREEMENTS 21

A. Geographic location of data servers – Privilege, Fourth Amendment, and other protections available under state & federal law but not under some non-U.S. laws; 21

B. Control of data and ability to retrieve at end of agreement or in event of bankruptcy or other demise of provider; 21

C. Assurance that client data will not be negligently leaked and that you will get immediate notice if a leak is discovered; 21

D. Service Level Agreements – Guaranteed Up-time; Redundancy; Firewall and anti-malware protection 21

E. Reliable Search and Production from the data base; 21

F. Assurance that at end of agreement no client data will be retained in backup, archive, or other format 21

VIII. BEYOND ETHICS 21

A. Even when state ethics rules do not impose an ethical duty of technology competence, other authorities do require technological competence, as they should. Should our ethical rules explicitly do so in addition? 21

B. The market will increasingly give a competitive advantage to lawyers with technical knowledge. Perhaps that, rather than ethical rules, will determine how the legal profession deals with technology? 22

IX. ADDITIONAL READING 23

X. SPECIAL BONUS SECTION: METADATA AND SHERLOCK HOLMES: THE ETHICAL CONUNDRUM OF "PAPER METADATA" 23

XI. CITYATTORNEYTECH 23

PETER B. HASKEL
Executive Assistant City Attorney
Dallas City Attorney's Office
Dallas City Hall
1500 Marilla Drive, Room 7BN
Dallas TX 75201
214-670-3038
peter.haskel@dallascityhall.com

BIOGRAPHICAL INFORMATION

BAR ADMISSIONS
Texas, New York, and numerous federal trial and appellate courts.

EDUCATION
B.A. in American History, Columbia College
J.D. Columbia University School of Law

PROFESSIONAL ACTIVITIES
Head, Dallas City Attorney's Office General Litigation Section
Chair, International Municipal Lawyers Association Technology Section
Chair, International Municipal Lawyers Association e-Discovery & Legal Hold Working Group
Co-Chair, Dallas Bar Association Legal Ethics Committee
Member, Sedona Conference Working Group 1 - Electronic Document Retention and Production
Past member, State Bar of Texas Administration of Rules of Evidence Committee
Past member, Texas Supreme Court Unauthorized Practice of Law Dallas Subcommittee
Runs "wildly popular" Yahoo Discussion Group: CityAttorneyTech:
(www.cityattorneytech@yahoogroups.com)

Frequent speaker including speaker for programs sponsored by the FBI National Academy, University of Texas Law School, State Bar of Texas, International Municipal Lawyers Association, Texas City Attorneys Association; Texas County and District Clerks Association; Texas Municipal Court Education Center; Dallas Bar Association; Dallas City Attorney's Office, City Attorneys Association of Kansas, Arkansas City Attorneys Association, and Tennessee Municipal Attorneys Association; and panelist for programs sponsored by the American Bar Association, National Association of Attorneys General, and National Association of Telecommunications Officers and Advisors.

CLOUD COMPUTING: ETHICAL CONSIDERATIONS OF CONFIDENTIALITY AND DATA SECURITY

I. INTRODUCTION

A. Few if any state lawyer ethics rules explicitly address cloud computing

A recurring theme among state ethics opinions on attorney use of cloud computing (their opinions are discussed below) is their attempt to impose an ethical duty of technical competence on attorneys by expanding beyond their plain meaning the existing ethics rules on attorney competence, client confidentiality, care of client property, and obligation to supervise non-lawyers. The ABA has to some extent acted similarly by amending comments to require technological expertise without changing the text of the Rules of Professional Conduct, which do not contain any such requirements. This explains the ABA's addition in August 2012 of a new comment number 6 to ABA Model Rule of Professional Conduct 1.1 that would require technical competence as an additional ethical obligation. This change is also detailed below.

I suspect that most states will gradually move in the direction of imposing an ethical duty of technical competence that would include some degree of technological knowledge before a lawyer can put client data "in the cloud."

B. Questions

1. Inconsistent Standards for Tech Ethics?

Are we developing higher standards for outsourcing computer technology than for other outsourcing relationships as to protection of client confidences? Are such distinctions wise? Necessary? Beneficial to clients?

2. Confuting Lawyer & Technician Responsibilities?

As standards for legal ethics in cloud computing and other technological areas develop, should there be a clearer distinction between what responsibilities a lawyer can delegate to retained technical experts and the type of expertise that the lawyer (or perhaps at least one lawyer in a firm or law office) must acquire, or engage another lawyer to provide?

3. Must Lawyers Be Technologists?

Fundamentally, should lawyers ethically be required to have technical knowledge as well as legal knowledge for the general practice of law? If so, what are the parameters for such requirements?

C. This outline addresses only ethical standards.

Lawyers should not for a moment forget that substantive legal standards do apply to the protection of client information when an attorney uses the cloud — just as when an attorney uses filing cabinets, secretaries, or couriers for paper documents, or uses e-mail (which is often cloud-based anyway). Those standards include malpractice liability, sanctions for violations of court rules, and civil and criminal penalties under laws and regulations such 42 U.S.C. § 17935 (Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format).

D. **Where is the border between UPL and technology when lawyers must apply tech knowledge to legal practice?**

If legal competence encompasses technology (and this is the trend), where is the boundary for unauthorized practice of law when non-lawyers advise others about technology issues related to contracts, e-discovery, or other matters about which lawyers traditionally provide advice and other legal services?

II. QUESTION: WHAT IS CLOUD COMPUTING?

Answer: **OUTSOURCING** OF COMPUTER SERVICES, SOFTWARE, PLATFORM, ETC., TO BE HOSTED ON A CONTRACTOR'S SERVERS AND MANAGED BY THE CONTRACTOR

This explains the potential benefits and the risks of cloud computing. Think of how cloud computing resembles other outsourcing. There are savings in salary, benefits, capital investment, and upkeep, etc. There are increased risks including loss of direct control over the data and over security of the data, and over maintenance and upkeep, etc.

A. **Outsourcing of computer resources is not new.**

Westlaw, GoToMeeting, and EDS data storage are some examples of earlier technology used for outsourcing computer data or activities. But technology is recently vastly improved, pricing is becoming affordable and, savings can be realized.

B. **NIST Definition of Cloud Computing:** Peter Mell & Timothy Grance, Technical Definition From National Institute of Standards and Technology ("NIST")**: NIST Definition of Cloud Computing (Final Oct 21, 2011) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (7-page PDF download last accessed Aug. 17, 2012).**

"The NIST Definition of Cloud Computing

"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.

1. Essential Characteristics:

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.

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[1] 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.

[1] Typically this is done on a pay-per-use or charge-per-use basis.

2. Service Models:**[[1]]**

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure

[1]. 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.

[2] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

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.

[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

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

[1] Vendors continue to invent terms that purport to describe additional cloud deployment models. The most recent that I have seen is "DaaS" (data as service), which ties into the recent sales pitch for "big data" cloud support." The lesson: To be tech-savvy, a lawyer needs to watch his aas. Pete Haskel

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).

[4] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources."

3. **Deployment Models**:

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)."

C. **Additional Resources on Cloud Computing Generally**

ABA Commission on Ethics 20/20 | ABA Board of Governors / Commission on Ethics 20/20, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited Aug. 23, 2012) (links history of proposals, discussions, and events on legal ethics relating to technology and to final changes to ABA Model Rules of Professional Conduct stemming from the Commission's work approved on August 6, 2012, by the ABA House of Delegates [see below]).

Cloud computing resources and information - searchCloudComputing.com, http://searchcloudcomputing.techtarget.com/resources (last visited May 6, 2012).

Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony G. Thompson-Starkey, Hans Graux, Sadie Creese, &Paul Hopkins, The Cloud: Understanding the Security, Privacy and Trust Challenges - Rand Paper (Apr. 2011) - 0.8 MB (122 pages) Free PDF Download or read online, http://www.rand.org/pubs/technical_reports/TR933.html (last visited Aug. 23, 2012).

Abstract: "The overall objective of The Cloud: Understanding the Security, Privacy and Trust Challenges study is to advise on policy and other interventions which should be considered in order to ensure that European users of cloud environments are offered appropriate protections, and to underpin a world-leading European cloud ecosystem. Cloud computing is increasingly subject to interest from policymakers and regulatory

authorities. The European Commission's recent Digital Agenda highlighted a need to develop a pan-European 'cloud strategy' that will serve to support growth and jobs and build an innovation advantage for Europe. However, the concern is that currently a number of challenges and risks in respect of security, privacy and trust exist that may undermine the attainment of these broader policy objectives. Our approach has been to undertake an analysis of the technological, operational and legal intricacies of cloud computing, taking into consideration the European dimension and the interests and objectives of all stakeholders (citizens, individual users, companies, cloud service providers, regulatory bodies and relevant public authorities). We undertook literature and document review, interviews, case studies and held an expert workshop to identify, explore and validate these issues in more depth. The present paper represents the final consolidation of all inputs, suggestions and analyses and contains our recommendations for policy and other interventions."

NIST - Cloud Computing Synopsis and Recommendations, Special Publication 800-146 (May 29, 2012), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075 (81-page PDF file last accessed May 31, 2012).

"Open issues" identified by this recent special report include computing performance, reliability, network dependence, cloud provider outages, safety-critical processing, economic goals, risk of business continuity, service agreement evaluation, portability of workloads, interoperability between cloud providers, disaster recovery compliance, lack of visibility, physical data location, jurisdiction and regulation, support for forensics, information security, risk of unintended data disclosure, and data privacy." *Id*, at 8-1 *et seq*. *That does not leave many "resolved issues."*

NIST - Cloud Computing Resources Generated by NIST Web site search engine from search term "cloud computing," NIST Search Results, http://www.nist.gov/search-results.cfm?q=cloud+computing&btng=Search&num=10&sortType=L&scopeType=0&datefrom=&datet0= (last visited Aug. 23, 2012).

Daniel Ward, Cloud Computing: A Brief Overview: E-Discovery Law Review (July 13, 2010), http://www.ediscoverylawreview.com/2010/07/articles/cloud-computing-a-brief-overview/ (last visited June 1, 2012).

III.CLIENT CONFIDENTIALITY IN CONTEXT OF CLOUD COMPUTING – GENERALLY

A. Useful references from NIST on Cloud Security & Privacy

NIST Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144) (Dec. 19, 2011). http://docs.govinfosecurity.com/files/external/SP800-144.pdf (last accessed Aug. 17, 2012).

Self-Described: "Cloud computing can and does mean different things to different people. The common characteristics most share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a

certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment."

NIST - Cloud Computing Synopsis and Recommendations, Special Publication 800-146 (May 29, 2012), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075 (81-page PDF file last accessed May 31, 2012) (also cited above).

From Executive Summary at ES-2:

" . . . Service Agreements, including Service Level Agreements. Organizations should understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers. An organization should understand customer responsibilities, and those of the service provider, before using a cloud service.

"Security. Organizations should be aware of the security issues that exist in cloud computing and of applicable NIST publications such as NIST Special Publication (SP) 800-53 "Recommended Security Controls For Federal Information Systems and Organizations." As complex networked systems, clouds are affected by traditional computer and network security issues such as the needs to provide data confidentiality, data integrity, and system availability. By imposing uniform management practices, clouds may be able to improve on some security update and response issues. Clouds, however, also have potential to aggregate an unprecedented quantity and variety of customer data in cloud data centers. This potential vulnerability requires a high degree of confidence and transparency that cloud providers can keep customer data isolated and protected. Also, cloud users and administrators rely heavily on Web browsers, so browser security failures can lead to cloud security breaches. The privacy and security of cloud computing depend primarily on whether the cloud service provider has implemented robust security controls and a sound privacy policy desired by their customers, the visibility that customers have into its performance, and how well it is managed.

"Inherently, the move to cloud computing is a business decision in which the business case should consider the relevant factors, some of which include readiness of existing applications for cloud deployment, transition costs and life-cycle costs, maturity of service orientation in existing infrastructure, and other factors including security and privacy requirements."

B. ABA Ethics 20/20 Commission (Preliminary Issues Identification – Prior to Finalized Model Rules Amendment Adoption by House of Delegates on Aug. 6, 2012)

ABA Ethics 20/20 Comm'n, Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology, at 3-4 (Sept. 20, 2010),

http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/clientconfidentiality_issuespaper.authcheckdam.pdf (last visited June 1, 2012)
Cloud Computing: Ethical Considerations of Confidentiality and Data Security
Chapter 37

"Lawyers in different practice settings have taken advantage of cloud computing's many benefits, but cloud computing also raises several specific

issues and possible concerns relating to the potential theft, loss, or disclosure of confidential information. They include:

- unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet
- the storage of information on servers in countries with fewer legal protections for electronically stored information
- a vendor's failure to back up data adequately
- unclear policies regarding ownership of stored data
- the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business
- the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information
- policies for notifying customers of security breaches
- policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms
- insufficient data encryption
- the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information."

IV. STATE ETHICS OPINIONS

A. ABA On-Line Chart of Cloud Ethics Opinions Around the U.S.

Cloud Ethics Opinions Around the U.S., Legal Technology Resource Center, ABA Law Practice Management Center, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Mar. 10, 2013)(table & interactive map with links to opinions). *Caution, this is a superb research starting point but do not rely on the summaries of "specific requirements or recommendations" in the ABA table – read the actual opinions for substantive content.*

Note that practice varies from state-to-state as to whether opinions are binding or advisory, and as to whether the opining entity has any legal authority.

B. State Ethics Opinions

1. Alabama

Alabama State Bar, Office of Gen'l Counsel, Ethics Opinion 2010-02, **[Retention, Storage, Ownership, Production and Destruction of Client Files]** (undated but PDF version has "last modified date of Nov. 2, 2010), http://www.alabar.org/ogc/PDF/2010-02.pdf (last visited Mar. 11, 2012).

Excerpts:[2] ". . . The lawyer must have reasonable measures in place to protect the integrity and security of the electronic file. This requires the lawyer to ensure that only authorized individuals have access to the electronic files. The lawyer should also take reasonable steps to ensure that the files are secure from outside intrusion. Such steps may include the installation of firewalls and intrusion detection software. Although not required for traditional paper files, a lawyer must "back up" all electronically stored files onto another computer or media that can be accessed to restore data in case the lawyer's computer crashes, the file is

[2] Reproduced by permission of the State Bar of Alabama.

corrupted, or his office is damaged or destroyed. A lawyer may also choose to store or "back-up" client files via a third-party provider or internet-based server, provided that the lawyer exercises reasonable care in doing so. These third-party or internet-based servers may include what is commonly referred to as "cloud computing." According to a recent ABA Journal article on the subject, "cloud computing" is a "sophisticated form of remote electronic data storage on the internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored 'in the cloud' is kept on large servers located elsewhere and maintained by a vendor." Richard Acello, Get Your Head in the Cloud, ABA Journal, April 2010, at 28-29. The obvious advantage to "cloud computing" is the lawyer's increased access to client data. As long as there is an internet connection available, the lawyer would have the capability of accessing client data whether he was out of the office, out of the state, or even out of the country. In addition, "cloud computing" may also allow clients greater access to their own files over the internet. However, there are also confidentiality issues that arise with the use of "cloud computing." Client confidences and secrets are no longer under the direct control of the lawyer or his law firm; rather, client data is now in the hands of a third-party that is free to access the data and move it from location to location. Additionally, there is always the possibility that a third party could illegally gain access to the server and confidential client data through the internet. However, such confidentiality concerns have not deterred other states from approving the use of third-party vendors for the storage of client information. In Formal Opinion No. 33, the Nevada State Bar stated that: "[A]n attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third party declines to agree to keep the information confidential, then the attorney violates SCR 156 by transmitting the data to the third party. But if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent.

* * *

The Disciplinary Commission agrees [with ethics opinions from Arizona & Nevada] and has determined that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so. The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider. In whatever format the lawyer chooses to store client documents, the format must allow the lawyer to reproduce the

documents in their original paper format."

(Emphases added).

2. Arizona

Arizona Ethics Op. 09-04, [Confidentiality; Maintaining Client Files; Electronic Storage; Internet] (Dec. 2009) http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 (last visited Mar. 11, 2012).

Excerpts:[3] "This Committee has already determined that electronic storage of client files is permissible as long as lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." Ethics Op. 05-04.

* * *

"Other bar associations have recognized that the duty to take reasonable precautions does not require a guarantee that the system will be invulnerable to unauthorized access. See, e.g., N.J. Ethics Op. 701 (Apr. 10, 2006). Instead, the lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access." Id. See also 2008 N.C. Formal Ethics Op. 5 ("law firm must enact appropriate measures to ensure that each client only has access to his or her own file [and] that third parties cannot gain access [to] any client file").

"It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field. The competence requirements of ER 1.1 apply not only to a lawyer's legal skills, but also generally to "those matters reasonably necessary for the representation." Therefore, as a necessary prerequisite to making a determination regarding the reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security.

"Based on the facts supplied by the inquiring lawyer, the proposed online client file system appears to meet the requirements set forth by ER 1.6 and interpreted in Ethics Op. 05-04. [1] The lawyer has taken the preliminary step of having the files protected by a Secure Socket Layer (SSL) server, which encrypts the files, and also applied several layers of password protection. The fact that the system also utilizes unique and randomly generated folder names and passwords appears to satisfy the requirement of taking reasonable measures to protect client confidentiality and prevent unauthorized access. The further measure of converting each document to PDF format and requiring another unique alpha-numeric password to review its contents enhances the security of the proposed system.

"However, the Committee also recognizes that technology advances may make certain protective measures obsolete over time. Therefore, the Committee does not suggest that the protective measures at issue in Ethics Op. 05-04 or in this opinion necessarily satisfy ER 1.6's requirements indefinitely. Instead, whether a particular system provides reasonable protective measures must be "informed by the technology reasonably available at the time to secure data against unintentional disclosure." N.J. Ethics Op. 701. As technology advances occur, lawyers

[3] Reproduced by permission of the State Bar of Arizona.

should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information. . . ."

3. California

California Formal Opinion No. 2010-179, " … using technology to transmit or store confidential client information…" http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836 (last visited Mar. 11, 2012)

DIGEST: "Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications."

Draft California Formal Opinion Interim No. 10-0003, 2010 WL 8435841 (2010). ". . . may an attorney maintain a virtual law office practice ("VLO") and still comply with her ethical obligations, if the communications with the client, and storage of and access to all information about the client's matter, are all conducted solely through the Internet using the secure computer servers of a third-party vendor (i.e., "cloud computing")"

"DIGEST: As it pertains to the use of technology, the Business and Professions Code and the Rules of Professional Conduct do not impose greater or different duties upon a VLO practitioner operating in the cloud than they do upon an attorney practicing in a traditional law office. While an attorney may maintain a VLO in the cloud where communications with the client, and storage of and access to all information about the client's matter, are conducted solely via the internet using a third-party's secure servers, Attorney may be required to take additional steps to confirm that she is fulfilling her ethical obligations due to unique issues raised by the hypothetical VLO and its operation. Failure of Attorney to comply with all ethical obligations relevant to these issues will preclude the operation of a VLO in the cloud as described herein."

4. Iowa

Iowa State Bar Ass'n, Ethics Op. 11-01 [Use of Software as a Service – Cloud Computing] (Sept. 9, 2011), http://iowabar.org/associations/4664/files/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf (last accessed Mar. 10, 2013).

Suggests considerations before using SaaS for client data and due diligence steps for investigating cloud vendor.

5. Maine

Maine Prof. Ethics Comm'n, Bd. of Overseers of the Bar, Op. 194 [Client Confidences: Confidential firm data held electronically and handled by technicians for third-party vendors] (June 30, 2008), http://www.maine.gov/tools/whatsnew/in

dex.php?topic=mebar_overseers_ethics_opinions&id=86894&v=article (last accessed Mar. 10, 2013).

6. Massachusetts

Massachusetts Bar Ass'n Ethics Op. 12-03 (May 17, 2012), http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03 (last visited Mar. 10, 2013).

"Summary: A lawyer generally may store and synchronize electronic work files containing confidential client information across different platforms and devices using an Internet based storage solution, such as "Google docs,"[4] so long as the lawyer undertakes reasonable efforts to ensure that the provider's terms of use and data privacy policies, practices and procedures are compatible with the lawyer's professional obligations, including the obligation to protect confidential client information reflected in Rule 1.6(a). A lawyer remains bound, however, to follow an express instruction from his or her client that the client's confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client's express consent to do so.

7. Nevada

Nevada Formal Op. 33 [Storage of Client Files], http://nvbar.org/sites/default/files/opinion_33.pdf (last visited May 31, 2012)

Excerpt:[5] ". . . the lawyer must act competently and reasonably to safeguard confidential client information and communications from inadvertent and unauthorized disclosure. This may be accomplished while storing client information electronically with a third party to the same extent and subject to the same standards as with storing confidential paper files in a third party warehouse. If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate SCR 156 simply by contracting with a third party to store the information, even if an unauthorized or inadvertent disclosure should occur."

8. New Jersey

New Jersey Advisory Committee on Professional Ethics, Op. 701 [Electronic Storage And Access of Client Files] (undated, but PDF version indicates last modified on May 20, 2011 – refer to publication date in NJLJ for further information), http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf (last visited Mar. 11, 2013).

Excerpt: "With the exception of "property of the client" within the meaning of RPC 1.15, therefore, and with

[4] The opinion refers to several SaaS providers in addition to GoogleDocs, although the summary happens only to mention GoogleDocs. The opinion observes that GoogleDocs and several other SaaS providers' Privacy Policies seem to comport with lawyers' duties as to encryption, password protection and other safeguards. However, the policy ignores the need, clearly stated in GoogleDocs' Privacy Policies, for the customer to ensure that that customer's privacy settings provide the desired level of protection. *See* Privacy Policy – Policies & Principles – Google, http://www.google.com/intl/en/policies/privacy/ (last visited Mar. 10, 2013).

[5] Reproduced by permission of State Bar of Nevada.

the important caveat we express below regarding confidentiality, we believe that nothing in the RPCs prevents a lawyer from archiving a client's file through use of an electronic medium such as PDF files or similar formats. The polestar is the obligation of the lawyer to engage in the representation competently, and to communicate adequately with the client and others. To the extent that new technology now enhances the ability to fulfill those obligations, it is a welcome development.

"This inquiry, however, raises another ethical issue that we must address. As the inquirer notes, the benefit of digitizing documents in electronic form is that they "can be retrieved by me at any time from any location in the world." This raises the possibility, however, that they could also be retrieved by other persons as well, and the problems of unauthorized access to electronic platforms and media (i.e. the problems posed by "hackers") are matters of common knowledge. The availability of sensitive client documents in an electronic medium that could be accessed or intercepted by unauthorized users therefore raises issues of confidentiality under RPC 1.6.

* * *

"We do think, however, that when client confidential information is entrusted in unprotected form, even temporarily, to someone outside the firm, it must be under a circumstance in which the outside party is aware of the lawyer's obligation of confidentiality, and is itself obligated, whether by contract, professional standards, or otherwise, to assist in preserving it. Lawyers typically use messengers, delivery services, document warehouses, or other outside vendors, in which physical custody of client sensitive documents is entrusted to them even though they are not employed by the firm. The touchstone in using "reasonable care" against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has the lawyer has come to the prudent professional judgment he has satisfied both these criteria, then "reasonable care" will have been exercised."

(footnote omitted).

9. New York

NYS Bar Ass'n Committee on Professional Ethics,Opinion 842 [Using an outside online storage provider to store client confidential information] (Sept. 10, 2010)**"**

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege."

10. North Carolina

North Carolina Formal Ethics Op. 6, "Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client

Property" The North Carolina State Bar, http://www.ncbar.gov/ethics/ethics.asp (last visited Mar. 11, 2012) (search by opinion number in appropriate search box or click on search by title & scroll down alphabetical list of opinions to "Subscribing …")

Excerpts:[6] ". . . a law firm may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.

* * *

"Some recommended security measures are listed below.

• Inclusion in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.

• If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor's software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.

• Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.

• Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.

• Evaluation of the extent to which the SaaS vendor backs up hosted data.

(Endnotes omitted).

11. Oregon

Oregon State Bar Formal Ethics Op. No. 2011-188 [Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials], (Nov. 2011), http://www.osbar.org/_docs/ethics/2011-188.pdf (last visited Mar. 11, 2013).

Excerpt: "Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology "available at the time to secure data against unintentional disclosure." As technology advances, the third-party vendor's protective measures may become less secure or obsolete over time. Accordingly, Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials." (footnotes omitted).

12. Pennsylvania

Pennsylvania Bar Ass'n Comm. On Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 [Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property] (undated but PDF

[6] Reproduced by permission of State Bar of North Carolina.

version dated Nov. 23, 2011 as last modification), http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf (last visited Mar. 11, 2013).

Excerpt: "An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks."

13. Texas

Texas Center for Legal Ethics - Opinion 572 (June 2006) [". . . may a lawyer, without the express consent of a client, deliver material containing privileged information of the client to an independent contractor, such as a copy service, hired by the lawyer to perform services in connection with the lawyer's representation of the client?] http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-572.aspx (last visited May 30, 2012).

" . . . The Committee is of the opinion that a lawyer's delivery of materials containing privileged information to an independent contractor providing a service, such as copying, to facilitate the lawyer's representation of a client (and not for the purpose of disclosing information to others) does not constitute 'revealing' such privileged information within the meaning of Rule 1.05, provided that the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information. . . . [But the lawyer should not do this if the client expressly prohibits it]."

14. Vermont

Vermont Bar Ass'n Advisory Ethics Op. 2010-6, https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx (last visited Mar. 10, 2013).

Excerpt: "Vermont attorneys may use SaaS systems for storing, processing, and retrieving client property, as long as they take reasonable precautions to ensure the property is secure and accessible. The nature of the precautions depends on the circumstances. The ability to engage in Cloud Computing is not limited by the specific location of the remote server, although some of the factors noted above, including choice of law clauses, and concerns about access to data in the event of a service interruption or an emergency, may be implicated by the location of the storage server and the extent of backup service provided by the vendor.

"Depending on the circumstances, there may be limits on systems that can be used and client property that can be stored with an SaaS vendor, and lawyers must assess each situation based upon the specific facts and circumstances."

C. **There are real risks from using cloud computing.**

- Human Error & Dishonesty – this single greatest security risk, just as it is outside the cloud
- Hacking & leaks through inadequate technical security measures
- Death of the Delete Key
- Loss of data or of data access – particularly if vendor goes out of business

Question: Who will pay for the due diligence to avoid these risks? Do benefits in cost-savings, accessibility, flexibility out-weigh the risks? Who

makes that decision – the lawyer or the client? Or does each have veto power?

D. Some Developing Though not Uniform Trends in State Ethics Opinions

1. **investigation of vendor competence & trustworthiness – beyond that required for other outsourcing;**
2. **"Legally enforceable" vendor obligation to preserve confidentiality & make data available back to lawyer;**[7]
3. **Lawyer's obligations may evolve based on technology developments;**

[7] What does "legally enforceable" mean in this context? Does the lawyer need to attempt to insulate the agreement from potential assignment or rejection in bankruptcy? If "enforceable" would money damages suffice if client data lost?

V. HOW WOULD 2012 REVISED ABA MODEL RULES[8] CHANGE EXISTING ETHICAL STANDARDS?

OVERARCHING ISSUE: WHEN AND TO WHAT EXTENT IS A LAWYER SUPPOSED TO HAVE TECHNOLOGICAL COMPETENCE? PUT ANOTHER WAY: WHEN DOES LEGAL COMPETENCE ENCOMPASS TECHNOLOGICAL COMPETENCE?

A. Competent Representation ABA Model Rule (as amended 2012) Rule 1.1 Competence

[8] Text from August 2012 Amendments to ABA Model Rules Of Professional Conduct, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_house_action_compilation_redline_105a-f.authcheckdam.pdf (28-page PDF file last visited Aug. 23, 2012), unless otherwise noted. Footnotes are mine, but underlining and strike-throughs denoting deleted and added text is from the ABA. N.B., I do not here reproduce or discuss all ABA Model Rules of Professional Conduct or comments changes approved by the ABA House of Delegates on August 6, 2012. My reproductions are limited to directly relevant excerpts and constitute "fair use." However, the linked PDF document does set out the full set of amendments to the rules and to the comments. The full current Model Rules with comments are online at Model Rules of Professional Conduct | The Center for Professional Responsibility, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visited Nov. 9, 2012).

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment

* * *

Maintaining Competence

[~~6~~ 8] 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,[9] engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Pete Haskel Suggestions:

- If a state considers adopting a version of this comment, consider clarifying scope of technology about which the attorney needs to be competent as to risks and benefits.
- This and other ABA changes strongly suggest that attorneys, even government attorneys, need to include in terms and scope of engagement and administrative directives about their duties some clear and appropriate limits and allocation of responsibilities for technology expertise. *See* Tex. Disc. R. Prof'l Conduct 1.02(b) (lawyer may limit scope of representation if client consents after consultation).

B. Client Confidentiality

ABA Model Rule 1.6 (as amended 2012) Confidentiality of Information

* * *

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment

Acting Competently to Preserve Confidentiality

[1~~8~~6] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ 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,[10] the cost of employing**

[9] Does this mean only the benefits and risks associated with technology used by a lawyer in the lawyer's practice? Does this requirement extend to being able to advise a client about the benefits and risks associated with technology that the client may use, at least in transactions relevant to the subject of a lawyer's engagement?

[10] The language "the likelihood of disclosure if additional safeguards are not employed" is troublesome. If applied to the lawyer's use of outside contractors including cloud providers, does this text imply an ethical duty for the lawyer to review such

additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].[11]

Pete Haskel Suggestions:

- If Texas considers adopting versions of this rule and comment, and even if not, it is becoming prudent to obtain written client approval before sharing client information with cloud providers and other outside contractors based on a written discussion/disclosure addressing the factors listed in ABA comment 18 to Rule 1.6(c).
- This discussion in the engagement letter or related documents would include any client requirements for special security precautions or explicit client approval of existing security measures as sufficient.
- Government lawyers (and other in-house counsel) can consider achieving similar results via adopted organizational policies addressing the sufficiency of security measures for protecting organizational data.

C. **Safekeeping Property**

ABA Model Rule 1.5 Safekeeping Property [unchanged]

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client

---

things as the vendor's security policies, effectiveness of those policies as actually applied and/or personnel backgrounds for vendor employees and subcontractors? Who will pay for these steps? How often must they be repeated? The comment has one virtue: Unlike the language of several state ethics opinions addressed above, the ABA standard at least applies consistent standards to all outside vendors, from the high-tech cloud provider to the lower-tech temp secretarial service and the document courier or archive company.

[11] Emphasis added. How useful is a rule such as this that enumerates factors to be weighed without a bright-line standard if the result of a violation can be disciplinary sanctions?

or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

* * *

ABA Model Rule 4.4 (as amended 2012) Rule 4.4 Respect for Rights of Third Persons[12]

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

Comment

* * *

[2] Paragraph (b) recognizes that lawyers sometimes receive a documents or electronically stored information that were was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the document or electronically stored information original document, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been wrongfully inappropriately obtained by the sending person. For purposes of this Rule, ''document or electronically stored information'' includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data

[12] I include ABA Rule 4.4 here even though it does not necessarily involve cloud computing (though it often could) mainly to note the "hot" ethics issues regarding the inadvertent disclosure of electronic data including metadata that are drawing attention in many states. The often divergent approaches to ethical and substantive obligations respecting inadvertently disclosed electronic data, particularly metadata, are addressed in such sources as "The Sedona Conference® Commentary on Ethics & Metadata (March 2012 Public Comment Version) March 2012" Publications | The Sedona Conference®, https://thesedonaconference.org/publications (last visited Aug. 23, 2012) (free PDF download but registration required); Metadata Ethics Opinions Around the U.S., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html (last visited Aug. 23, 2012). *See also* Special Bonus Section, *infra*.

(commonly referred to as "metadata"), that is ~~email or other electronic modes of transmission~~ subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.

[3] Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving ~~it~~ the document that it was inadvertently sent ~~to the wrong address~~. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.

* * *

D. **Responsibility for Cloud Vendors**

ABA Model Rule 5.3 (as amended 2012) Responsibilities Regarding Nonlawyer Assistan~~ce~~ts ~~:~~:

Comment

[~~2~~1] Paragraph (a) requires lawyers with managerial authority within a **law firm**[13] to make reasonable efforts ~~to establish internal policies and procedures designed to provide~~ to ensure that the firm has in effect measures giving reasonable assurance that nonlawyers in the firm and nonlawyers outside the firm who work on firm matters will act in a way compatible with the professional obligations of the lawyer. ~~with the Rules of Professional Conduct.~~ See Comment [6] to Rule 1.1 (retaining lawyers outside the firm) and Comment [1] to Rule 5.1~~.~~ (responsibilities with respect to lawyers within a firm). Paragraph (b) applies to lawyers who have supervisory authority over ~~the work of a nonlawyer.~~ such nonlawyers within or outside the firm. Paragraph (c) specifies the circumstances in which a lawyer is responsible for the conduct of ~~a nonlawyer~~ such nonlawyers within or outside the firm that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer.

Nonlawyers Within the Firm

[~~1~~2] Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.

Nonlawyers Outside the Firm

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, **hiring a document management**

---

[13] Model Rule 1.0 (Terminology) includes this definition : "(c) "Firm" or "law firm" denotes a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the **legal department of a corporation or other organization**." (Emphasis added). I think that his covers government legal departments.

company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.[14] See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). **When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.**[15]

[4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

[14] Emphasis added.

[15] Emphasis added.

VI.RELATIVISTIC ETHICS: DUE DILIGENCE TO PROTECT CLIENT CONFIDENTIALITY FOR CLOUD COMPUTING COMPARED TO DUE DILIGENCE FOR OTHER OUTSOURCING

When it is suggested that a lawyer take special care to protect client data when negotiating cloud service agreements, might it be useful to compare the recommended steps to steps that reasonable attorneys take when entering into other "outsourcing" relationships, *e.g* ---

A. Office lease: Do we check on operational status of building's centralized fire and burglar alarms? Do we conduct background checks on landlord's security guards, or demand to read existing personnel background reports? Do we sweep for electronic listening devices? Do we investigate possible organized crime ties of the landlord or of the building's janitorial company or waste disposal company?

B. Temporary secretarial/clerical staff: Do we rely on background checks by temp agencies of the employees that they send to us?

C. Internet service providers: How closely do we audit their firewall and malware measures? Do we demand background checks on their staff? Do we demand right to control their subcontracting or outsourcing?

D. Computer hardware vendors: Do we check for keystroke monitors or other spyware on newly-received devices?

VII. SOME SECURITY & CONFIDENTIALITY CONCERNS IN NEGOTIATING CLOUD SERVICE AGREEMENTS

A. **Geographic location of data servers – Privilege, Fourth Amendment, and other protections available under state & federal law but not under some** non-**U.S. laws;**

B. Control of data and ability to retrieve at end of **agreement** or in event of bankruptcy or other demise of provider;

C. Assurance that client data will not be negligently leaked and that you will get immediate notice if a leak is discovered;

D. Service Level Agreements – **Guaranteed Up-time; Redundancy; Firewall and anti-malware protection**

E. Reliable Search and Production from the data base**;**

F. Assurance that at end of agreement no client data will be retained in backup, archive, or other format

VIII. BEYOND ETHICS

A. **Even when state ethics rules do not impose an ethical duty of technology competence, other authorities do require technological competence, as they should. Should our ethical rules explicitly do so in addition?**

1. Existing rules other than ethical rules already explicitly or by necessary implication impose requirements for technological competence. For example, Tex. R. Civ. P. 196.4.[16]

---

[16] This passage from a 2009 Texas Supreme Court case is illustrative:

> Weekley argues that HFG failed to comply with Rule 196.4 because it never specifically requested production of "deleted emails." Rule 196.4 provides that, "[t]o obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced." Tex. R. Civ. P. 196.4. As we have said, email communications constitute "electronic data," and their characterization as such does not change when they are deleted from a party's inbox. Thus, deleted emails are within Rule 196.4's purview and their production was implied by HFG's request. However, for parties unsophisticated in electronic discovery, such an implication might be easily missed. Rule 196.4 requires specificity, and HFG did not specifically request

deleted emails. HFG counters that it did not know how Weekley's computer system and electronic information storage worked, and thus did not know what to ask for. But it is a simple matter to request emails that have been deleted; knowledge as to the particular method or means of retrieving them is not necessary at the requesting stage of discovery. Once a specific request is made the parties can, and should, communicate as to the particularities of a party's computer storage system and potential methods of retrieval to assess the feasibility of their recovery.6 But even though it was not stated in HFG's written request that deleted emails were included within its scope, that HFG thought they were and was seeking this form of electronic information became abundantly clear in the course of discovery and before the hearing on the motion to compel. The purpose of Rule 196.4's specificity requirement is to ensure that requests for electronic information are clearly understood and disputes avoided. Because the scope of HFG's requests *315 was understood before trial court intervention, Weekley was not prejudiced by HFG's failure to follow the rule and the trial court did not abuse its discretion by ordering production of the deleted emails. To ensure compliance with the rules and avoid confusion, however, parties seeking production of deleted emails should expressly request them.

In re Weekley Homes, L.P., 295 S.W.3d 309, 314-15 (Tex. 2009) (From WestlawNext. Text of footnotes omitted).

2. Lawyers practicing in specialized fields such as patent law or medical records law necessarily must now have an understanding of relevant technology issues.

3. Generalist lawyers will increasingly be called on by the market and by professional competence standards to obtain some proficiency in technology matters. The issues will always be how much competence the lawyer must have personally and when and to what extent the lawyer can permissibly rely on employed or retained technical experts, or the client, for technical knowledge. There has never been and probably never will be a simple answer, for purposes of ethics or otherwise, to those questions.

B. **The market will increasingly give a competitive advantage to lawyers with technical knowledge. Perhaps that, rather than ethical rules, will determine how the legal**

profession deals with technology?

IX. ADDITIONAL READING

John W. Amberg, Jon L. Rewinski, New Technologies Add a Wrinkle to the Ongoing Ethical Concerns of the Legal Profession, 2005 Ethics Roundup, 29-APR L.A. Law. 35 (2006), supposedly online at www.lacba.org/Files/LAL/Vol29No2/2246.pdf but online file not accessible on May 31, 2012

William Freivogel, Technology And The Lawyer's Duty Of Confidentiality, Practical Real Estate Lawyer 9 (Nov. 2007), online at http://files.ali-aba.org/thumbs/datastorage/lacidoirep/articles/PREL0711-Freivogel_thumb.pdf (last accessed May 31, 2012)

Ellie Margolis, Surfin' Safari—why Competent Lawyers Should Research On The Web, 10 Yale J. L. & Tech. 82 (2007)

Dan Rowinski, Computer Programming for All: A New Standard of Literacy, ReadWriteWeb (May 17, 2012), http://www.readwriteweb.com/hack/2012/05/computer-programming-for-all-a-new-standard-of-literacy.php (last visited May 31, 2012).

Sarah Salter, Storage and Privacy on the Cloud: Enduring Access to Ephemeral Messages, 32 Hastings Comm. & Ent L.J. 365 (2010).

Martha Sperry, You May Be Illiterate If You Can't Program, Advocate's Studio (May 28, 2012), http://advocatesstudio.com/2012/05/28/you-may-be-illiterate-if-you-cant-program/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+advocatesstudio%2FHnQs+%28Advocate%27s+Studio%29 (last visited May 31, 2012)

Michael Whiteman, The Impact Of The Internet And Other Electronic Sources On An Attorney's Duty Of Competence Under The Rules Of Professional Conduct, 11 Alb. L.J. Sci. & Tech. 89 (2000)

X. SPECIAL BONUS SECTION: METADATA AND SHERLOCK HOLMES: THE ETHICAL CONUNDRUM OF "PAPER METADATA"

Paper metadata: Fingerprints, watermarks, blood traces, DNA, traceable indentations; folds, anything that Sherlock Holmes might have considered a "clue" if associated with a paper document.

What ethical standards would preclude a receiving attorney from inspecting a paper document for such clues?

What ethical standard requires a producing attorney to scan for possible "paper metadata" absent special facts (except perhaps in criminal cases)?

Why should electronic metadata be treated differently from paper metadata in respect of legal ethics?

XI. CITYATTORNEYTECH

http://groups.yahoo.com/group/CityAttorneyTech/

A forum for attorneys who represent local government units and their IT staff to discuss tech issues relating to their practice, including research, software, office management, hardware, regulatory, and communications issues. Any views expressed are solely those of the posting individuals, and not of any government unit, legal office, or law firm. Moreover,

no posting represents fully researched, authoritative, or binding legal opinion for any purpose. This group is a spin off from and has overlapping membership with listservs associated with IMLA, but City Attorney Tech is not affiliated with or sponsored by any organization or listserv. Any reference or link to any vendor of goods or services is purely informational and implies no sponsorship or endorsement. Posting of any link or excerpt does not imply agreement with anyone else's views; only that the material might be useful to know. NO REQUEST FOR INFORMATION OR FOR DOCUMENTS THAT IS POSTED, REPRODUCED, OR CITED ON THIS SITE IS INTENDED AS A REQUEST UNDER ANY FEDERAL, STATE OR LOCAL LAW, RULE, REGULATION, OR ORDINANCE REQUIRING THE DISCLOSURE OF ANY GOVERNMENT INFORMATION OR DOCUMENTS.

Group Email Addresses

Post message: **CityAttorneyTech@yahoogroups.com**

Subscribe: **CityAttorneyTech-subscribe@yahoogroups.com**

Unsubscribe: **CityAttorneyTech-unsubscribe@yahoogroups.com**

List owner: **CityAttorneyTech-owner@yahoogroups.com** or **peter.haskel@dallascityhall.com**