CLOUD COMPUTING: ETHICAL CONSIDERATIONS OF CONFIDENTIALITY AND DATA SECURITY

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

State Bar of Texas
34th ANNUAL
ADVANCED REAL ESTATE LAW
July 12-14, 2012
San Antonio

CHAPTER 37
PETER B. HASKEL
Chief of Litigation
Litigation Division
General Litigation Section

Peter Haskel joined the Dallas City Attorney's Office in 1999. He is the Chief of the General Litigation Section. In addition, his practice focuses on complex civil litigation, often relating to telecommunications and public utilities controversies and bankruptcy as well as other technological and financial issues.

Education
- Columbia School of Law
  J.D. 1975
- Columbia College
  B.A. 1971

Affiliations & Activities
- Admitted to the State Bar of Texas, June, 1989; Also New York Bar February 1975
- Member Dallas Bar Association and American Bankruptcy Institute
- Also admitted to practice in United States District Courts in the Northern, Western, and Southern Districts of Texas, and Southern and Eastern Districts of N.Y.; U.S. Courts of Appeals for Second, Fifth, District of Columbia, and Military Circuits; and U.S. Supreme Court
- Member, State Bar of Texas Committee for Administration of Rules of Evidence (2004-06)
- Faculty, Texas Municipal Court Education Center

Publications & Presentations
- Complex Litigation (Dallas City Attorney's Office 2000)
- Spurious Petitions (Dallas County Bar Ass'n Gov't Law Working Group 2002)
- Bankruptcy Basics (Dallas City Attorney's Office 2003)
- Some Problems Respecting Evidentiary Privileges (Dallas City Attorney's Office 2005)
- Bankruptcy from a Local Government Perspective (panel presentation; National Association of Attorneys General/States’ Association of Bankruptcy Attorneys Annual Bankruptcy Law Conference, Santa Fe NM 2006)
- Pirating Privacy (panel presentation; National Association of Telecommunications Officers and Advisors Annual Conference, Orlando FL 2006)
- Pretrial Discovery Responses (panel presentation; Dallas City Attorney’s Office 2006)
- Bankruptcy Law for the Municipal Attorney (City Attorney's Association of Kansas 2006)
- Ethics of Communicating with Current & Former Government Officials & Employees (International Municipal Lawyers Association IMLA Regional CLE Employment Law Program Dallas TX 2008)
- Numerous presentations relating to paper terrorism, domestic terrorism, fraud, and related subjects to FBI National Academy, Texas Association of District and County Judges, Texas Association of District and County Clerks, and other organizations (1996 - Present)

Prior Experience
- Public Sector: Assistant Texas Attorney General (deputy chief, financial litigation division and head, anti-domestic terrorism task force), Special Assistant U.S. Attorney (W.D. Texas); Special Prosecutor (various Texas Counties); Supervising Inspector General (NYC); Assistant District Attorney (NYC); Lieutenant Commander, JAGC, US Navy
- Private Sector: Associate Attorney focusing on complex bankruptcy litigation at Weil, Gotshal & Manges and Moore & Peterson, P.C., both in Dallas

© 2011 Dallas City Attorney
# TABLE OF CONTENTS

Introduction

I. Question: What is Cloud Computing?

II. Client Confidentiality in Context of Cloud Computing — Generally

III. What are potentially applicable provisions of Texas Disciplinary Rules of Professional Conduct (“Disc. R.”) To Cloud Computing — And Are They Directly On Point?

IV. ABA Commission on Ethics 20/20 Proposal for New Comment 6 to Model Rule 1.1

V. Relativistic Ethics Due Diligence to Protect Client Confidentiality for Cloud Computing compared to Due Diligence for Other Outsourcing

VI. Some Security & Confidentiality Concerns in Negotiating Cloud Service Agreements

VII. Parting Thoughts
CLOUD COMPUTING: ETHICAL CONSIDERATIONS OF CONFIDENTIALITY AND DATA SECURITY

INTRODUCTION

As detailed below, the only Texas ethics rule directly applicable to protecting client confidential information in connection with cloud computing is the general rule on confidentiality, Tex. Disciplinary R. Prof’l Conduct 1.05.

Other states’ ethics rules often differ from Texas ethics rules. However, a recurring theme among those states that have issued 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. This explains the pending proposal being considered by the ABA to add a new comment number 6 to ABA Model Rule of Professional Conduct 1.1 (2004) that would require technical competence as an additional ethical obligation. This proposal is also detailed below.

I suspect that Texas will gradually move in the direction of imposing an ethical duty of technical competence that would include some degree of technological knowledge before a Texas lawyer can put client data “in the cloud.” But we are not there yet. As of now there is no Texas ethics rule that explicitly limits or governs the use of cloud computing by Texas lawyers for client data.

Questions: (1) 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) 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) must acquire or engage another lawyer to provide?

(3) 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?

I. QUESTION: WHAT IS CLOUD COMPUTING?

Answer: OUTSOURCING OF COMPUTER SERVICES, SOFTWARE, PLATFORM, ETC.

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 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 older examples), but technology is recently vastly improved, pricing is becoming affordable and, savings can be realized.

B. Technical Definition From National Institute of Standards and Technology (“NIST”):

NIST Definition of Cloud Computing (Final Oct 21, 2011) (7-page PDF download)
Cloud Computing: Ethical Considerations of Confidentiality and Data Security

Chapter 37

“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.

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.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure[2]. 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 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).
This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.”

**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**

ABA Commission on Ethics 20/20 | ABA Board of Governors / Commission on Ethics 20/20,

Cloud computing resources and information - searchCloudComputing.com,

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.”
http://www.rand.org/pubs/technical_reports/TR933.html

NIST - Cloud Computing Synopsis and Recommendations, Special Publication 800-146 (May 29, 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 a lot of “resolved issues.”

NIST - Cloud Computing Resources Page
http://csrc.nist.gov/groups/SNS/cloud-computing/
II. CLIENT CONFIDENTIALITY IN CONTEXT OF CLOUD COMPUTING - GENERALLY

A. Useful references from NIST


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.”

http://docs.govinfosecurity.com/files/external/SP800-144.pdf


“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 a lot of “resolved issues.”

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

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

“Confidentiality-Related Concerns from Cloud Computing

“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.”

C. State Ethics Opinions


Excerpts:¹ “... 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 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.”

¹ Reproduced with permission of State Bar of Alabama.
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).


Excerpts:

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

- **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.”


Excerpt: “... 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.”


Excerpts: “... 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.

3 Reproduced by permission of State Bar of Nevada.
4 Reproduced by permission of State Bar of North Carolina.
**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).

- **See Texas Center for Legal Ethics - Opinion 572, “... 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?”** (June 2006), [http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-572.aspx](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].”


“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.”

---

III. WHAT ARE POTENTIALLY APPLICABLE PROVISIONS OF TEXAS DISCIPLINARY RULES OF PROFESSIONAL CONDUCT (“DISC. R.”) TO CLOUD COMPUTING — AND ARE THEY DIRECTLY ON POINT?  

Hint: No! The emphases in the text below are mainly intended to demonstrate that existing Texas ethics rules do not explicitly require technical competence, for cloud computing or otherwise.

Disc. Rule 1.01 Competent and Diligent Representation

(a) A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer’s competence, unless:
   (1) another lawyer who is competent to handle the matter is, with the prior informed consent of the client, associated in the matter; or
   (2) the advice or assistance of the lawyer is reasonably required in an emergency and the lawyer limits the advice and assistance to that which is reasonably necessary in the circumstances.

Questions:

Does this rule require technical competence or just legal competence? In modern practice is technical competence sometimes required for legal competence?

Has this rule traditionally been limited to requiring legal (as distinguished from technological) competence? E.g. For e-Discovery?

Official Comments on Rule 1.01 (excerpt):

Accepting Employment

1. A lawyer generally should not accept or continue employment in any area of the law in which the lawyer is not and will not be prepared to render competent legal services. Competence is defined in Terminology as possession of the legal knowledge, skill, and training reasonably necessary for the representation. Competent representation contemplates appropriate application by the lawyer of that legal knowledge, skill and training, reasonable thoroughness in the study and analysis of the law and facts, and reasonable attentiveness to the responsibilities owed to the client.

2. In determining whether a matter is beyond a lawyer’s competence, relevant factors include the relative complexity and specialized nature of the matter; the lawyer’s general experience in the field in question, the preparation and study the lawyer will be able to give the matter, and whether it is feasible either to refer the matter to or associate a lawyer of established competence in the field in question. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more elaborate treatment than matters of lesser consequences.

3. A lawyer may not need to have special training or prior experience to accept employment to handle legal problems of a type with which the lawyer is unfamiliar. Although expertise in a particular field of law may be useful in some circumstances, the appropriate proficiency in many instances is that of a general practitioner. A newly admitted lawyer can be as competent in some matters as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge.

* * *

Disc. Rule 1.05 Confidentiality of Information

(b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e), and (f), a lawyer shall not:[8] knowingly reveal confidential information of a client or a former client:

7 N.B. — no mention of retaining a computer engineer or other non-lawyer consultant.
8 What about negligent or reckless disclosure of confidential information to cloud provider? Without checking provider’s security measures or employees’ reliability? Without determining where provider’s servers are located? Other states’ legal ethics rules for using the cloud seem to impose a higher standard than “knowingly” for a duty not to disclose client information.

Official Comments on Rule 1.01 (excerpt): Accepting Employment

1. A lawyer generally should not accept or continue employment in any area of the law in which the lawyer is not and will not be prepared to render competent legal services. Competence is defined in Terminology as possession of the legal knowledge, skill, and training reasonably necessary for the representation. Competent representation contemplates appropriate application by the lawyer of that legal knowledge, skill and training, reasonable thoroughness in the study and analysis of the law and facts, and reasonable attentiveness to the responsibilities owed to the client.

2. In determining whether a matter is beyond a lawyer’s competence, relevant factors include the relative complexity and specialized nature of the matter; the lawyer’s general experience in the field in question, the preparation and study the lawyer will be able to give the matter, and whether it is feasible either to refer the matter to or associate a lawyer of established competence in the field in question. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more elaborate treatment than matters of lesser consequences.

3. A lawyer may not need to have special training or prior experience to accept employment to handle legal problems of a type with which the lawyer is unfamiliar. Although expertise in a particular field of law may be useful in some circumstances, the appropriate proficiency in many instances is that of a general practitioner. A newly admitted lawyer can be as competent in some matters as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge.

* * *

Disc. Rule 1.05 Confidentiality of Information

(b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e), and (f), a lawyer shall not knowingly[8] reveal confidential information of a client or a former client:

[8] What about negligent or reckless disclosure of confidential information to cloud provider? Without checking provider’s security measures or employees’ reliability? Without determining where provider’s servers are located? Other states’ legal ethics rules for using the cloud seem to impose a higher standard than “knowingly” for a duty not to disclose client information.

All emphases and footnotes in Disc. Rules text & comments are added.
(i) a person that the client has instructed is not to receive the information; or
(ii) anyone else, other than the client, the client’s representatives, or the members, associates, or employees of the lawyer’s law firm.\(^9\)

* * *

(c) A lawyer may reveal confidential information \(^{10}\):

\(^9\) What about disclosure to a cloud service provider of the lawyer without consent of the client? Cf., Texas Center for Legal Ethics - Opinion 572, “. . . 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?” (June 2006), 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. In these circumstances, the independent contractor owes a duty of confidentiality both to the lawyer and to the lawyer's client. See generally Restatement (Second) of Agency sections 5, 395, 428 (American Law Institute 1958).”

\(^{10}\) None of these circumstances apply to cloud providers unless the lawyer specifically gets client consent to disclose to a cloud provider. But see Texas Center for Legal Ethics - Opinion 572 “. . . 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?” (June 2006) 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. . . .”).

(1) When the lawyer has been expressly authorized to do so in order to carry out the representation.
(2) When the client consents after consultation.
(3) To the client, the client’s representatives, or the members, associates, and employees of the lawyers firm, except when otherwise instructed by the client.
(4) When the lawyer has reason to believe it is necessary to do so in order to comply with a court order, a Texas Disciplinary Rule of Professional Conduct, or other law.

Disc. Rule 1.14 Safekeeping Property
(a) A lawyer shall hold funds and other property\(^{11}\) belonging in whole or in part to clients or third persons that are in a lawyer’s possession in connection with a representation separate from the lawyer’s own property.\(^{12}\) Such funds shall be kept in a separate account, designated as a trust or escrow account, maintained in the state where the lawyers office is situated, or elsewhere with the consent of the client or third person. Other client 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.\(^{13}\)

(b) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this Rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive\(^{14}\) and, upon request by the client or third person, shall

\(^{11}\) Does “other property” include data? Several subsequent terms in this rule & the associated comments cast doubt on that gloss.

\(^{12}\) Would it be feasible for a lawyer segregate client’s data from the lawyer’s own work product, as perhaps with separate data bases? If so, would that benefit the client in any way?

\(^{13}\) An indication that “other property” does not include data, because so many substantive laws and regulations govern records retention.

\(^{14}\) Another indication that “other property” does not include data — a client is always entitled to an attorney’s records concerning the client; could the attorney keep copies or duplicates of the data if the attorney had to turn it over to the client whenever received? The rule just does not fit the “data” situation. Indeed, I question if it even makes sense to treat paper documents as “other property” within the meaning of this rule.
promptly render a full accounting regarding such property.

* * *

Official Comment on Disc. R. 1.14 (Excerpt):

1. A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property which is the property of clients or third persons should be kept separate from the lawyer’s business and personal property and, if monies, in one or more trust accounts. Separate trust accounts may be warranted when administering estate monies or acting in similar fiduciary capacities. Paragraph (a) requires that complete records of the funds and other property be maintained.)

Question: If “other property” is intended to include electronic data, how can the strict accountability of a fiduciary for property be reconciled with the duty of merely not “knowingly” disclosing client information under Disc. R 1.05(b)?

Rule 5.03 Responsibilities Regarding Nonlawyer Assistants

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the persons conduct is compatible with the professional obligations of the lawyer; and

(b) a lawyer shall be subject to discipline for the conduct of such a person that would be a violation of these rules if engaged in by a lawyer if:

(1) the lawyer orders, encourages, or permits the conduct involved; or

(2) the lawyer:

(i) is a partner in the law firm in which the person is employed, retained by, or associated with; or is the general counsel of a government agency’s legal department in which the person is employed, retained by or associated with; or has direct supervisory authority over such person; and

(ii) with knowledge of such misconduct by the nonlawyer knowingly fails to take reasonable remedial action to avoid or mitigate the consequences of that person’s misconduct.

Comment:

1. Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants act for the lawyer in rendition of the lawyer’s professional services. A lawyer should 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 non-lawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.

2. Each lawyer in a position of authority in a law firm or in a government agency should make reasonable efforts to ensure that the organization has in effect measures giving reasonable assurance that the conduct of nonlawyers employed or retained by or associated with the firm or legal department is compatible with the professional obligations of the lawyer. This ethical obligation includes lawyers having supervisory authority or intermediate managerial responsibilities in the law department of any enterprise or government agency.

IV. ABA COMMISSION ON ETHICS

20/20 PROPOSAL FOR NEW COMMENT 6 TO MODEL RULE 1.1

Proposed Comment 6 to ABA Model Rules of Professional Conduct (2004) ("Model Rules"), Rule 1.1 would include a requirement that a lawyer be aware of “the benefits and risks associated with relevant technology” as a component of legal technology:

Model Rule 1.1 Competence

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

Proposed Comment 6

“Maintaining Competence

* * *

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

* * *
American Bar Association
Commission on Ethics 20/20
Report to the House of Delegates,
Resolution at 3.

Report accompanying and in same online PDF File as 20/20 Commission Resolution, for Proposed Comment 6 on Model Rule 1.1, at 3-4:

“Model Rule 1.1 (Competence)
“Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today’s environment without knowing how to use email or create an electronic document.

Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase “including the benefits and risks associated with relevant technology,” would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

V. 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 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?

VI. 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

VII. PARTING THOUGHTS

A. Although existing Texas 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, the civil procedure rules respecting e-discovery, Tex. R. Civ. P. 192.3(b), 196.4; the evidence rules respecting contents of writings, etc. Tex. R. Evid. 1001-03, 1006.

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

I suspect that land use attorneys are generally expected, even if not ethically required, to have a working knowledge of technologies such as online research, electronic filing, and the ability to read and interpret plats, topographic maps, and, perhaps, even the sending and receiving of e-mail. With attachments!

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?

Additional Reading


