ETHICS, CLOUD COMPUTING, AND ENGAGEMENT AGREEMENTS

JOSEPH JACOBSON, Dallas
Law Office of Joseph Jacobson

State Bar of Texas
39th ANNUAL
ADVANCED REAL ESTATE LAW
July 13-15, 2017
San Antonio

CHAPTER 26

©2017 Joseph Jacobson
JOSEPH JACOBSON

Joseph Jacobson has consistently applied his interest in technology to substantive areas of the law. With this background, Mr. Jacobson became one of three attorneys participating in the drafting and legislative process for Texas Antihotnet Bill amending the Texas Business & Commerce Code. Before that it was on the Business Law Section’s legislative committee reviewing UETA and UCITA and preparing Texas versions and commentary for those bills.

A former Chair of the Computer & Technology Section of the State Bar of Texas, Mr. Jacobson currently holds the position as Vice Chair of the Privacy, Data Breach & E-commerce Committee of the Business Law Section. Mr. Jacobson was a founding member of the Dallas Bar Association’s E-Commerce Committee, and a founding member of the E-Commerce Committee of the Business Law Section. Mr. Jacobson is a past Board Member of the Japan America Society of Dallas and a delegate on trade mission to Japan focused on Texas trade. He has represented companies with operations in Europe and Asia.

As an Adjunct Professor at S.M.U. Law School Mr. Jacobson was part of the multidisciplinary team (along with professors and deans from the Engineering, Business, and Law Schools) developing proprietary material for Nortel Networks. The success of this project led to the funding of the Hart eCenter at S.M.U. His practical experience in representing both lenders and borrowers, and in commercial real estate, landlords, tenants, purchasers, and sellers has enabled him to bring an unusual perspective to the nuances of contracting and secured financing, particularly those transactions involving technology. Mr. Jacobson’s representation includes:

- Software developers and contractors;
- Institutional lenders;
- Shopping center and industrial office park developers and investors;
- Franchisees of most major restaurant chains in site acquisition and negotiations;
- Asset acquisitions;
- Electricity contract negotiations;
- General business contracting;
- Producers or creative artists in all media, including photography, music, movies, radio, and television.

Mr. Jacobson’s other business activities include being a founder and chair of a national bank.
TABLE OF CONTENTS

I. SUMMARY ....................................................................................................................................................... 1

II. INTRODUCTION: “SEND IN THE CLOUD. ISN’T IT BLISS?”
(Paraphrasing Stephen Sondheim) ...................................................................................................................... 1

III. HYPOTHETICAL PROBLEMS SOON BECOME REAL CRISIS;
CAN YOU TELL ONE FROM THE OTHER? ................................................................................................ 2
A. Situation 1: A family vacation. ................................................................................................................. 2
B. Situation 2: A law firm. ............................................................................................................................. 2
C. Which fact situation was the hypothetical? ................................................................................................ 2
D. Two more fact situations to consider. ........................................................................................................ 2

IV. IF ADOPTED IN TEXAS, WOULD THE AMERICAN BAR ASSOCIATION’S
NEW MODEL RULE CHANGE THE REQUIREMENTS FOR ATTORNEY
TECHNOLOGICAL COMPETENCE AND COMMUNICATION WITH CLIENTS? .................................. 2
A. A client’s informed consent requires an attorney’s technological competence to identify and communicate procedures, and options, if any. ................................................................. 3
   1. The attorney’s technological sophistication and responsibility to communicate to the client. ....... 3
   2. The law firm’s IT Department and the law firm’s relationship to its CSP, and their impact on the individual attorney. ........................................................................................................... 3
B. The jump from “technological competence” to file encryption ................................................................. 3
C. Texas, arguably, already had encouragement for an attorney’s technological competence before the ABA Commission on Ethics 20/20’s proposed Model Rule ........................................ 5
   1. A law practice is a business and standard statutes and regulations applicable to other businesses apply to firms. .......................................................................................................................... 5
D. Since Texas does not have a Cloud Computing Disciplinary Rule or a Texas Supreme Court
   Professionalism Committee opinion addressing this issue, what can we conclude? .................................. 7
E. Alaska’s approach to Cloud Computing .................................................................................................... 7
   1. The Alaska Bar Association’s Ethics Opinion 2014-3 .................................................................... 7
   2. Implementing the Alaska Bar Association’s Ethics Opinion 2014-3 ........................................ 8
   3. If the Cloud creates opportunities for catastrophic failure, then the attorney’s focus could be directed to his or her control of the environment outside the Cloud. ......... 9

V. IDENTIFICATION OF POSSIBLE RELATIONSHIPS BETWEEN AND
AMONG PARTIES INVOLVED IN CREATING AND USING THE CLOUD. .......................................... 10
A. Outsourcing your IT needs with Software as a Service, Infrastructure as a Service, or simply off-site backup........................................................................................................................................ 10
B. Who finances what and where: from the CSP’s facilities to the equipment holding your software and data, every creditor to every borrower in the chain of transactions wants protection. ............................................................................................................. 10
C. Utility regulation in states outside your jurisdiction may allow destruction of your data................ 11
D. Redundancy of data and software, or “Here, There and Everywhere.” .................................................... 11
   1. Redundancy of your data and software enhances continuity while creating independent security risks ...................................................................................................................................... 11
   2. Filing of security interests and notices of property exempt from security (lien) agreements conflicts with the CSP’s physical security (against terrorism) interests. ........................................................................ 12

VI. RELATIONSHIPS REMAIN UNSETTLED BETWEEN (1) SECURED
PARTIES AND LIEN HOLDERS AND (2) A THIRD-PARTY’S DATA AND
SOFTWARE, PARTICULARLY WHEN PRIVACY ISSUES ARE CONSPICUOUS ...................................... 12
A. Secured lien holders have a duty to prevent the debtor’s asset from wasting ........................................ 12
B. What information must be disclosed to the lien holder about data stored on the secured collateral — and who has that duty? ........................................................................................................ 13
VII. THE SECURED CREDITOR FACES UNRESOLVED CONFLICTING OBLIGATIONS WHEN TAKING POSSESSION OF THE CSP’S COLLATERALIZED EQUIPMENT. ................................................................. 13

VIII. WILL YOUR DATA “TAKE A RIDE ON THE MAGIC BUS.” .......................................................... 14

IX. WHAT ENTITIES ARE GOING TO SAVE YOUR CLIENT OR YOU IN CASE OF LOSS OF DATA? ................................................................. 15

X. “BUT IT’S THE INTERNET, DON’T YOU UNDERSTAND?” ................................................................. 15
A. For those still holding on to the “Too Big to Fail” doctrine for protection in the Cloud-provider discussions, consider Nortel Networks and Dropbox. .................................................................................................... 15
B. Since the Internet may be accessed anywhere, electricity power supply for Cloud computing data centers drives the Internet and Cloud computing. .......................................................................................... 16
   1. Electricity is related not only to energy, but political power and corporations’ branding and profits. ........................................................................ 16
   2. Electricity markets are variable since factoring costs of production and future demands, making corporate planning challenging. .................................................. 16
C. “The Do No Harm” mantra of Internet companies is not universal. ............................................................ 17

XI. “YOUR MONEY OR YOUR DATA, OR BOTH;” OR, “SKIP THE MONEY—JUST GIVE ME YOUR DATA.” ..................................................................................................................... 18
A. Comparing financial safeguards with data protection and control. .......................................................... 18
   1. Banks are monitored, ratings disclosed, and the federal government encourages and provides transition for absorption of customer accounts by a new entity. ........................................................................ 18
   2. If data is as important as money, why isn’t there a government agency that monitors and regulates Cloud Service Providers? .......................................................... 18
B. A CSP’s size may be relevant, but is not controlling for your or your client’s decision, since size creates other risks. ......................................................................................................... 19

XII. KEY INDUSTRY FACTORS EFFECTING YOUR NEGOTIATIONS AND YOUR LIABILITY TODAY: THE CLOUD COMPUTING INDUSTRY BASICS AND TRENDS. .......................................................... 19
A. Economies of scale and facilities planning win the day. ........................................................................ 19
   1. “If you build it, they will come.” ........................................................................ 19
   2. Power availability and cost, even more than contiguous space, dictates the location of CSPs and data centers. ..................................................................................... 20
B. Location, Location, Location; or, why your data center’s location matters. ........................................ 21
   1. Computerized trading governs location for equity and hedge funds. .................................................. 21
   2. Data centers cost money and electricity is the greatest on-going expense. ...................................... 21

XIII. “HOW EXPENSIVE CAN MISTAKES BE?” ..................................................................................... 22

XIV. ETHICS AND STATE REGULATION FOR PINK ELEPHANTS; WHAT IF THERE IS NO CONFIDENTIAL OR PRIVILEGED INFORMATION? ................................................................. 22

XV. IN THE EVENT YOU’RE NOT A CEO, CFO, CIO, OR, MOST POWERFULLY, A CCF YOUR LAW LICENSE, AS A PRACTICING ATTORNEY, MAY BE IN JEOPARDY. ......................................................... 23

XVI. IF CLOUD COMPUTING IS AN INTERNATIONAL TRANSACTION, WHAT OPTIONS EXIST FOR PROTECTION OF CLOUD CONSUMERS? ................................................................. 24
A. Disparate factors such as a highly educated and English-speaking work force to low-cost labor to inexpensive construction costs to green computing branding, all push for internationalization of the Cloud computing industry. .......................................................................................... 24
B. Since IBM is building what may be the world’s largest private data center in China, what would happen if some of these Creditor – Debtor issues arose there? Would the result be different in Hong Kong? ................................. 24
ETHICS, CLOUD COMPUTING, AND ENGAGEMENT AGREEMENTS

I. SUMMARY

This paper begins with an identification of some ethical issues that require or encourage greater technical skills for attorneys. After a brief introduction to technology applications, the technology is applied to both real and hypothetical examples arising from both common business practices and legal ethics compliance issues.

An overview of the Cloud computing industry follows with discussion of the range of services available through the Cloud. Each of these services offer particular contracting challenges, civil liability consequences, and for a law firm using Cloud computing, ethical responsibilities.

Cloud computing through social media has permeated consumer use. Control of Robin Williams’ online identity (digital assets) became national news and a video game devotee had 9,000 attendees at a virtual funeral.

This paper then explores statutory protections and failings, contractual provisions, and case law uncertainty in identifying and protecting interests of Cloud providers, landlords to Cloud providers, lenders to every enterprise associated with the location and equipment used in the Cloud, Cloud consumers, Cloud consumers’ clients and customers (relevant for both attorneys and other businesses using the Cloud), software vendors, and the role attorneys take in representing these parties with their varied interests and goals. This paper concludes with recommendations for Cloud use by businesses and attorneys, and yes, even a suggestion for government regulation.

II. INTRODUCTION: “SEND IN THE CLOUD. ISN’T IT BLISS?” (PARAPHRASING STEPHEN SONDHEIM).

Your client or you has heard about “The Cloud.” Your client or you find IT daunting, an increasing expense, and source of liability. While your client or you may not understand all of the concepts and details of Cloud use, reducing staff, reducing IT expenditures and off-loading direct responsibility for technology support all sound great. How do we get from (A) aggravated with operations and IT (Information Technology) administration to (B) “bliss?” Can it be done?

Stephen Sondheim with amazing prescience asked and answered a question for today:

Isn’t it rich?
Are we a pair?
Me here at last on the ground,
You in mid-air.¹

This paper will help you determine if your client (or your law firm) should be “a pair” with a CSP. Putting these lyrics in context, the lead actress with new self-awareness, and having recognized her part in a failed relationship, ends the song alone and in tears. Will your relationship with your CSP mirror this segment in Sondheim’s play, or mirror the play’s conclusion where the 2 protagonists are united and happy?

III. HYPOTHETICAL PROBLEMS SOON BECOME REAL CRISIS; CAN YOU TELL ONE FROM THE OTHER?

Please consider 2 situations which focus on issues for companies and attorneys using the Cloud.

A. Situation 1: A family vacation.

A Texas family, rents a car in California to vacation along California’s Highway 1. They stop for lunch at a restaurant. When they come out their car (with all the luggage) is gone. The California police didn’t care. No charges were filed, since nothing illegal occurred. How could this be?

The rental car was merely repossessed by the car rental company’s lender. The family’s vacation was ruined. When the family asked the car rental company’s creditor about the luggage left in the car while at the restaurant, they were told all luggage from all the repossessed cars is available for identification in a warehouse in Fargo, N.D. Insurance covered nothing; nothing was stolen or destroyed, just geographically undesirable.

B. Situation 2: A law firm.

A law firm has one-third of its lawyers jump to another firm. The landlord would not negotiate a downsizing of the firm’s space. Following these unsuccessful negotiations, the landlord declares the tenant in default, even though rent is fully paid. Landlord accelerates the balance of the rent, a claim amounting to several million dollars, and asserts a landlord’s lien on the firm’s personal property, including its computers. In addition to the suit for collection of the accelerated rent of millions, and foreclosure on its Landlord’s Lien, the landlord files an action to push the firm into state receivership (suggesting its own receiver). State receivership was to serve only as an intermediate step to having landlord’s choice of receiver place the law firm into federal bankruptcy proceedings.

C. Which fact situation was the hypothetical?

Situation 1? No, not that this author is aware. The reality of Situation 2 (yes, Situation 2 happened) deserves your focus, but the fact situation is not complete for what may happen with Cloud computing.² Let us consider some variations of the two situations and create, yet other hypotheticals.

Consider opportunities to prepare for hypothetical Situations 3 and 4 before they become your reality.

D. Two more fact situations to consider.

Combine the 2 scenarios above and consider the personal property in jeopardy (the computers) and your client’s data residing on the computers of a CSP (luggage in the repossessed car). The computers where the data resides are not in Client’s control. The Client is not aware the CSP has placed financing liens on its equipment (the computers) or that the landlord has a lien on the CSP’s personal property (the computers storing data). Your client is not aware of its CSP’s landlord-tenant dispute. Your client calls and says no one in her company can log on and asks your advice. Your client’s business is in jeopardy.

This scenario sounds challenging for these reasons:

- Your client does not know where the computers are located or how to gain physical control of them and the data.
- Your client does not know what actions if any have been filed against the CSP, or in what jurisdictions. (The computers may be in a location different than the CSP’s headquarters.)
- Your client cannot access anyone at the Cloud Service Provider.
- Your client asks you if any of these problems effect the acquisition it has been planning or its patent applications or its soft drink secret formula.

Now, imagine a fourth scenario. You are not worried about these issues because it happened to a client; you are in panic mode because these circumstances happened to your CSP, and no one in your law firm can log on.

IV. IF ADOPTED IN TEXAS, WOULD THE AMERICAN BAR ASSOCIATION’S NEW MODEL RULE CHANGE THE REQUIREMENTS FOR ATTORNEY

¹ STEPHEN SONDHEIM AND HAROLD S. PRINCE, Send in the Clowns in “A Little Night Music” by HUGH WHEELER, STEPHEN SONDHEIM AND HAROLD S. PRINCE, “A Little Night Music” 1973. Music Copyright 1973 Revelation Music Publishing Corp./Beautiful Music, Inc. All rights reserved. This song was made famous by Judy Collins’ recording.

² Situation 2 is discussed in Exhibit A attached to this document.
TECHNOLOGICAL COMPETENCE AND COMMUNICATION WITH CLIENTS?

A. A client’s informed consent requires an attorney’s technological competence to identify and communicate procedures, and options, if any.

1. The attorney’s technological sophistication and responsibility to communicate to the client.

The American Bar Association Commission on Ethics 20/20 broadens a lawyer’s ethical requirements to include an understanding and appreciation of technology.

On February 13, 2013, the American Bar Association’s Commission on Ethics 20/20 issued its proposed recommendation. Rule 1.1 of the Model ABA rules is entitled “Competence.” It states:

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] 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.

This Comment ties not only the use of technology to an attorney’s competence, but apparently requires the attorney to have sufficient understanding of technology to communicate the risks and benefits associated with “relevant” technology.

Following the ABA Model Rule, the client may make a final choice on security procedures required for its communication with a law firm. The attorney would communicate the options to the client. But questions follow this responsibility to communicate risks associated with technology. At issue is not just the risk of technology but the risk of the technology the firm uses.

- Is the attorney obligated to communicate to the client that the law firm does not have encrypted email procedures, but and the risks associated with unencrypted email?
- Does the attorney have an obligation to communicate to the client options which the firm does not offer, i.e., technology the firm doesn’t have or practice, i.e., the firm does not have a procedure for communicating with encrypted email?
- Does the attorney fail the client if the attorney does not have secure options for client communications?

2. The law firm’s IT Department and the law firm’s relationship to its CSP, and their impact on the individual attorney.

This Comment to Rule 1.1 is significant in another way. The ABA Model Rules are applied to individual attorneys. The responsibility these rules impose may not be passed to a firm’s IT Department. Likewise, this author asserts, the responsibility for security may not be delegated to a law firm’s CSP.

At the very least, the attorney should be aware of the basic technology the CSP uses and how the attorney’s procedures or the law firm’s procedures fit into these contractual relationships.

B. The jump from “technological competence” to file encryption.

If a client has a choice to make, such as to send emails encrypted or not; or, to receive emails encrypted or not, then the impact of an attorney’s technological competence can be more easily measured.

- Does the attorney’s explanation of encryption lead to an informed choice by the client?
- Does the client’s behavior change, i.e., does the client choose encryption over unencrypted communication?

Some practicing attorneys have already had to answer questions about whether files are encrypted while stored at a law firm; while in transit from the firm to the CSP or from the CSP to the firm; and, who controls encryption of the files at the CSP. Many of these attorneys are involved in Intellectual Property (IP) work, not surprisingly where both the attorneys and the clients may have more sophistication and appreciation for cybersecurity policies and techniques.

Clients in regulated industries such as health care or finance, or publicly traded companies in any industry have more regulations and potential liabilities for cybersecurity issues than other businesses. Law firms who hope to have and retain these types of clients must adopt rigorous cyber security standards.

Both the federal and state governments regulate health care information as defined in HIPAA, and in state laws and regulations. In medical practices, the control of the keys for cyphering personal health data is critical.

http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf
information is not usually discussed with patients. Yet, because of the types of communications between attorneys and their clients, client involvement at this level of practice is management has already occurred and will be more likely to occur in the future.

Encryption is one level of protection, meaning the file is gibberish without the key to cypher the file. Password access is different, and much less rigorous since the file may be read if accessed, but that access is ostensibly limited to individuals that have the appropriate credentials, i.e., User ID and Password. This limitation is not as restrictive as encryption because if the unencrypted file is accessed, then there is no barrier to reading the file’s contents.

While restricted access to a file offers some protection, it is not the basis for a secure communication. Clients may presume that restricted access would be inviolate, but attorneys may test their client’s expectations by having clients compare their reaction to emails and written letters.

Client expectations for email may be different than that of other written communications. Consider the circumstances of a client writing a letter on paper to the attorney. The client would reasonably believe the letter could be read by any attorney or assistant working on the case.

At issue is whether you, as an attorney are clear to the client, that the emails may be read by others at the firm in the event you are struck by lighting.4

The Texas Disciplinary Rules of Professional Conduct Rule 1.03 Communication holds the lawyer’s obligation to inform a client to this standard:

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

The ABA Model Rule 1.0(e) defines informed consent to occur “... after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.” ABA Commission on Ethics 20/20 Model Rule 1.0 Terminology http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf.

Texas’ Disciplinary Rules appear to have a different standard. The ABA discusses material risks, while the Texas rule is not limited to material matters. Does this variance create a real difference in application? Does the Texas rule require more disclosure?

How would you identify the risks associated with your firm’s use of the Cloud?

- Would you as an attorney have to provide statistics on the general loss of mobile phones or mobile computers5 and passwords or automatic logins for Cloud access to a client’s data, or statistics specific to attorneys in your state or just your law firm?

- Would you as an attorney have to provide information as to the number of law firms and other businesses or just law firms that have been hacked, A test to appreciate a client’s expectations for email privacy as compared to more formal written correspondence (on paper), would be to ask a client contact how he or she would feel if all the emails were in one folder, and any attorney or support staff at the firm could see any email the client contact wrote. This author believes that most clients view email communication as more personal (and more private) than a letter, more like a telephone conversation.

This author has examples of private matters such as health conditions and marital status and availability for other relationships being discussed in emails with client contacts. These discussions in emails have led to litigation.

4 Since a client’s letters or faxes are inserted in a client’s files, does the client have different expectations for privacy in emails? Consider your client contact may communicate personal matters, such as consideration of a new position with another company in an email to you as the company’s outside attorney (and friend). If the client does not take that position, and if you are no longer with the firm, how would the client contact expect the firm to react to her or his emails about possibly accepting another position? If an attorney leaves the firm, should the attorney be allowed to delete or somehow archive more personal emails between the attorney and the client contact? If the client contact leaves the firm, should the client contact have some right to review these emails?

5 “Cell phones, we lose 60 million of them each year. In hotels, 64 million items left behind. And laptops, 600,000 of them left at the airport each year.” Cashing in on the Mother Lode of Lost and Found, ABCNews.com February 2, 2014 http://abnews.go.com/WNT/video/cashing-mother-lode-lost-found-22384309

Asurion, a company insuring mobile devices such as phones, states “29 million phones are lost or stolen each year.” 29 Million Lost & Stolen Smartphones Don't Lie, ASURIONBLOG, DECEMBER 3, 2013 http://blog.asurion.com/more-mobile/dont-left-empty-handed/
i.e., had their computer data compromised?

- Do you as an attorney have to provide to your Client that his, her or its data is stored on computers in California, Virginia, India, and Iceland?

- Do you, as an attorney, even know where the data is stored and the level of encryption of any of this stored data?

Without clear standards, or any guidance, attorneys may want to disclose a firm’s procedures, but be sure to allow the Client to set higher standards.\textsuperscript{6}

C. Texas, arguably, already had encouragement for an attorney’s technological competence before the ABA Commission on Ethics 20/20’s proposed Model Rule.

1. A law practice is a business and standard statutes and regulations applicable to other businesses apply to firms.

   a. Lawyers must follow business laws and regulations — just like a business.

   The Texas legislature has defined personally identifiable information relative to whether the information is encrypted or not. In other words, if the information is encrypted then the data is \textit{not} sensitive personal information; yet, the same information in an unencrypted state is sensitive personal information.\textsuperscript{7}

   This statute was amended in 2009, so every Texas business has had an opportunity to understand the advantages of encryption almost 8 years previous to this paper.

   Every Texas business includes law firms as Texas businesses.

   b. Lawyers should be aware of technology issues to insure their clients’ — and their own — compliance with data privacy issues.

   Texas businesses may reasonably expect their attorneys to have sufficient knowledge of encryption to explain the meaning of this statute and advise them as to whether the company’s procedures are in compliance with safe harbor rules.

   Even if an attorney did not represent businesses, an attorney would easily possess sensitive personal information such as a person’s first name or initial and last name and social security number if the attorney prepared wills for the individual, or represented that person in a divorce, or made a social security disability claim for that person — just to name a few opportunities for a law firm to acquire this information. Attorneys have a good reason to understand the statute for application to his or her own business (i.e., his or her law practice).

   Businesses and law firms may store emails in a backup system (in the Cloud or on their own servers at their offices) separately from their email server system which may be Web based. For example, Google Applications is a commercially available product providing Web-based email access. The emails are on Google’s cloud. The emails, however, may be downloaded to a firm’s server and stored by client or matter or in bulk. These stored emails themselves, may be saved on another server system or backup. Whether these emails are encrypted after being downloaded to the firm or subsequently stored in the firm’s Cloud backup (independent of Google) is relevant to the extent the emails have ethically defined confidential or privileged information, or may contain “sensitive personal information” or other information as regulated by the Texas legislature.

   c. An attorney’s individual responsibility (regulated by the State Bar of Texas) diverges from the law firm’s contractual and business relationship with the client.

   While Texas statutes address the responsibilities for a business, the ethics requirements are personal to the attorney. This tension between

   - Business entity compliance with Texas statutory business records; and,

   - Ethically mandated personal responsibility for an

\textsuperscript{6} An attorney may have to consider his or her understanding and ability to communicate the difference between encryption and password access – and possibly the differences among encryption options.

\textsuperscript{7} \textsc{TEx. BuS.& COM. CODE §521.002 (emphasis added)}

(2) “Sensitive personal information” means, subject to Subsection (b):

(A) an individual’s first name or first initial and last name in combination with any one or more of the following items, \textit{if the name and the items are not encrypted}:

(i) social security number;

(ii) driver’s license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.
attorney

may not be easily assuaged.

If a law firm failed to receive ethically required “informed consent” for the firm’s IT procedures and policies (i.e., Cloud use), then does that failure in ethics effect the engagement agreement? Could the Client argue effectively there was no meeting of the minds (without disclosure sufficient to allow informed consent), or fraud or a deceptive practice of some kind?

Law firms and individual attorneys may face issues such as:

- Whether Texas legal ethics or Texas employment law protect a newly hired attorney or out-voted partner in a “whistle-blower” fact circumstance, where the law firm does not have agreements that properly “explain a matter to the extent reasonably necessary to permit the client to make informed decisions”?

- Is there a way for an attorney to obtain a binding ruling on the disclosures within his or her firm’s professional services agreement without putting his or her employment at risk?

A ruling from a yet-to-be-designated authority may could alleviate an attorney’s concern over proper conduct. A ruling could also be supportive of the law firm if the client were concerned about the disclosures regarding privacy, privilege, confidentiality and Cloud computing.

If an ethical authority existed to issue approval of the attorney’s disclosure, could the ruling be binding in any civil legal action where a client claims the disclosure regarding technology was not adequate? Would the State Bar of Texas in conjunction with the legislature regulate this issue?

A client’s claims against a law firm may arise from

- Disclosure of data protected by statute; or,
- Breach of contract; or,
- Breach of a duty in accordance with tort or fiduciary responsibility.

While violations of the Disciplinary Rules of Professional Conduct in Texas do not give rise to an independent cause of action, in other states, violation of ethics provisions could give rise to a cause of action.

For example, a law firm could hold information about a public offering or an acquisition of a public company. Assume this information were to be accessed (the law firm is hacked) and the offering price changed. Could a claim reasonably be asserted against the law firm for breach of contract, breach of warranty, breach of a fiduciary obligation, or negligence or all four?

A disciplinary action could also be initiated by a client (through a complaint), but if the complaint were sufficient, the action would be brought by the State Bar against the attorney in his or her individual capacity. The State Bar of Texas does not regulate law firms.

d. Should safe harbor rules for business records be modified and adopted for attorneys’ and law firms’ client disclosures regarding technology?

Currently, the State Bar of Texas has a procedure for an advanced ruling from the Advertising Committee as to whether advertising is compliant with State Bar of Texas rules. The Advertising Committee’s ruling is admissible in any action against the law firm or attorney for violation of the advertising rules.

No procedure within the ethics rules grants an attorney or a law firm a safe-harbor provision for satisfactory disclosure enabling a client’s informed consent for the attorney’s or law firm’s use of technology, including encryption or the Cloud. Advertising Review Committee Opinions would always be admissible, but admissibility is a far cry from a safe-harbor provision.

No specific ethics rule or opinion exists in Texas regarding an attorney or law firm’s use of the Cloud for storing client data.

In 2009, the Texas legislature created an incentive for every business which keeps electronic records, including law firms, to have protection against lawsuits based on unauthorized release of these business records. The legislatively created, safe-harbor only requires encryption. No details about the sophistication of encryption were included either in the statute or any regulatory authority or judicial standard. Encryption alone was sufficient to trigger the safe-harbor protection in the event of data loss.

e. The ABA appears to reinforce the concept that a law practice or a law firm is governable distinct from a businesses.

The ABA Committee on Ethics 20/20 does not even use the word encryption in its rule or commentary on the Model rule.

For Texas lawyers, the how-to of encryption is covered by other presentations, particularly those by the Computer & Technology Section of the State Bar of Texas, many of which have been approved for CLE credit.

8 TEX. DISCIPLINARY R. PROF. CONDUCT 1.03(b)
http://www.legalethicstexas.com/Ethics-Resources/Rules/Texas-Disciplinary-Rules-of-

9 West Virginia is one such state allowing causes of actions based on ethics violations.
While the ABA’s emphasis on technical competence would reasonably reach beyond encryption and confidentiality of records, if encryption is so common that Texas passes laws specifying encryption, then why doesn’t the ABA mention encryption in its commentary?

D. Since Texas does not have a Cloud Computing Disciplinary Rule or a Texas Supreme Court Professionalism Committee opinion addressing this issue, what can we conclude?

In June, 2006, the Texas Supreme Court Professionalism Committee addressed whether an attorney, without the express consent of a client, could deliver material containing the client’s privileged information to an independent contractor, such as a copy services.

Opinion 572 relies on a Michigan case which found that lawyer-client privilege is not lost if a law firm hires an independent contractor necessary in the client’s representation.\(^{10}\)

The Committee concludes that unless the client has instructed the lawyer otherwise, a lawyer may deliver materials containing information subject to the attorney-client privilege to an independent contractor as needed for the client’s representation. The Committee fails to discuss whether the lawyer needs to disclose to the client that it has this option before the lawyer is retained.

The lawyer, however, before making the disclosure to the third-party contractor must reasonably determine that the independent contractor “will not disclose or use the materials or their contents except as directed by the lawyer.”\(^{11}\) The Committee states that “a good basis for such expectations would normally be a written agreement between the lawyer and the independent contractor.”

This last requirement of protections for the client confidentiality in the written agreement with the independent contractor will not work with standard Cloud computing contracts between the law firm and the Cloud Service Provider. Some of the largest and most common providers have form contracts which frustrate any presumption of reasonable expectations of confidentiality or care in handling the information.

The Cloud contracts are designed to confirm the CSP can use the data in any way possible and manipulate it in any way possible, and share it with any of its affiliates, or marketing partners, etc. Furthermore, the CSP obtains from the law firm or lawyer protection and indemnification for any failure or breach by it or its affiliates, or marketing partners.

Exhibit B identifies some of the policies; terms and conditions; terms of service; or legal disclaimers that have been found in recent CSP and IT agreements with third party providers. Some of these same elements would be applicable to storage of physical, paper files, and would raise some of the same issues.

Is delivering a cardboard box with no security mechanism to a storage facility better, the same, or worse than delivering a file to a CSP without having encryption? This question seems as though it is not directly answered by Texas statutes or ethics opinions other than the general reference to a law firm’s hiring independent contractors to perform work for a client.

E. Alaska’s approach to Cloud Computing.


The Alaska Bar Association addressed the question of Cloud computing and concluded:

| A lawyer may use cloud computing for file storage as long as he or she takes reasonable steps to ensure that sensitive client information remains confidential and safeguarded. . . . |
| [Later on in the opinion] |
| While a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where the data are stored and what the service agreement says. . . . |

https://www.alaskabar.org/servlet/content/1934.html

The Alaskan attorney attempting to comply with this opinion will find great challenges.

As noted elsewhere in this paper, information on “where the data is stored” is not available because geographic and physical locations of data centers are often considered proprietary information, and the secrecy justified to protect the data centers from physical attack by terrorists. Even if disclosed, the physical location is subject to automated changes, so the data would be impossible to track, particularly as the CSP would have multiple copies of the same data in different data centers.

The Opinion continues with the admonition that the lawyer “must therefore make reasonable efforts to ensure that the provider will act in a manner compatible

\(^{10}\) **Compulit v. Banctec, Inc.,** 177F.R.D. 410 (W.D.Mich. 1997)

\(^{11}\) Texas Professional Ethics Committee Opinion 572 (June 2006).
with the lawyer’s own professional standards.”12 This direction has several loopholes in its failure to define “reasonable efforts.” The directive does not even state that the lawyer has to be successful, although success would seem to be required. There is a presumption that the lawyer can have a discussion or exchange of emails or letters with the CSP informing them of professional ethics. Of course, this presumption is outside the bounds in contracts of the largest CSPs, unless the law firm is so large as to allow individualized negotiation with the CSP.

The Alaskan Bar creates further confusion by failing to reference the Alaska Statutes covering Breach of Security Involving Personal Information.13 In this next hypothetical, assume a law firm14 has a data breach. There is a statutory duty to notify “each state resident whose personal information was subject to the breach.”15 So, if you as a Texas attorney with an office in Texas, referred a Texas-resident and client of yours to Alaska for an ancillary probate proceeding, and the law firm had a breach, then at least by the relevant statutes, neither you nor your client would have to be notified. Neither of you were an Alaskan resident.

Subsection (a) of AS 45.48.010 does not have a safe harbor provision for encrypted data, just that if the data is stored and there is a breach, then the state resident must be notified.16

Alaska has a “No Harm, No Foul” exception to required breach disclosures. Through an intricate process, the Alaskan attorney general may issue a written opinion that “there is not a reasonable likelihood” of “harm” to the consumers. These opinions are not considered a public record open to inspection by the public. This exception seems to provide for a ruling that a breach of encrypted data (more precisely, sufficiently encrypted data in the opinion of the attorney general) does not trigger notification.

Footnote 7 of the Opinion 2014-3, requires that “the lawyer must notify the impacted client if the lawyer learns that the provider’s [CSP’s] security was breached and the client’s confidence or secret was revealed.” There could be a breach, but if the data was sufficiently encrypted, the “client’s confidence or secret” may not have been “revealed.”17

The crux of the issue is further highlighted in Footnote 7 where the Alaska Bar Association Ethics Committee and the Board of Governors include this suggestion:

Where highly sensitive data are involved, it may behoove a lawyer to inform the client of the lawyer’s use of cloud computing and to obtain the client’s informed consent.

The use of cloud computing is deemed so complicated and has so many problems woven into it, that the attorney has an obligation to inform the client the attorney is using cloud computing. There is no discussion as to whether this obligation to inform may be provided by the CSP, or an independent consultant acting on the lawyer’s behalf.18

The takeaway for the Alaskan lawyer seems to be a three step process:

1. Read the agreements without having to become an expert in cloud data storage
2. Disclose to the client that you (as an Alaskan attorney) are not an expert in Cloud computing, but you read the contract, and cannot obtain any better terms.
3. Have the client agree in writing to your Information Technology business practices. These steps for protecting clients may not be what the opinion wanted to encourage.


Let’s imagine we’re Alaska-licensed attorneys and we desire to implement Cloud computing for our practice consistent with Alaska’s opinion.

(c) Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public. AS 45.48.010

If encryption is properly accomplished with sufficiently complex encryption, then the information would be undecipherable.

The Opinion states, however, “the lawyer need not be an expert in cloud storage.” Opinion 2014-3

---

14 AS 45.48.090 (2) “covered person” means a (A) person doing business; (B) government agency; or, (C) person with more than 10 employees.” http://www.casemakerlegal.com/eliteBrowse.aspx?state=AK&sessionyr=2016&dataType=S&filename=akstatc2016Title45Chapter4548Article01.htm&categoryAlias=Statistics&cat=STAT
15 AS 45.48.010.
16 (c) Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public. AS 45.48.010
17 If encryption is properly accomplished with sufficiently complex encryption, then the information would be undecipherable.
18 The Opinion states, however, “the lawyer need not be an expert in cloud storage.” Opinion 2014-3
a. **We must first identify a CSP which is a “reputable organization.”**

There is no definition or example of “reputable” or “irreputable” in Alaska’s Opinion.\(^\text{19}\)

Using an easy-to-justify maxim, that biggest is the best, then we can begin our analysis. Amazon’s Cloud computing service is known as AWS. This Cloud service is the largest in the world.

In 2016, Oracle a giant among software and hardware companies had over $3 billion in sales of Cloud computing services.

In 2016, AWS had profits of over $3 billion dollars. AWS’ profits accounted for over 50% of Amazon’s total profits; yet, amounted to only 9% of Amazon’s total sales.\(^\text{20}\)

Let’s assume the attorney chose Amazon’s Cloud services entity known as AWS to provide Cloud services for his or her firm. This seems like a reasonable choice of a reputable supplier.

b. **If an attorney “need not become an expert in data storage,” what information is relevant for the attorney?**

The Alaska Ethics Rule is clear that attorneys do not have to become data storage experts, but the level of competence and expertise is not defined. The ABA Model Rule is not particularly helpful in this regard either.

If there is some awareness in specialized literature, should that awareness be enough to trigger an attorney’s further investigation or action? Consider the following reviews of Amazon’s AWS security.

- **“If you use Amazon, HP or GoGrid for Cloud-based server services you’ll need to take extra steps to secure the environment. “Bkav corporation, a security vendor . . . uncovered a lack of security best practices . . . for Amazon . . . HP and GoGrid.”**\(^\text{21}\)
- **“Wednesday’s demise of Code Spaces is a cautionary tale, not just for services in the business of storing sensitive data, but also for end users who entrust their most valuable assets to such services. . . . People who host their services on Amazon should avail themselves of the full spectrum of multifactor protections.”**\(^\text{22}\)
- **“[A]ttackers were able to gain full access and delete all of One More Cloud’s AWS instances, knocking both the company’s Websolr and Bonsai services offline.”**\(^\text{23}\)

Major, credible industry-specific media contained notices of the security issues with AWS, the largest CSP in the world. Few Alaska or Texas attorneys would review these sources to be aware of the warnings and know how to interpret them.

Would the attorney attempting to comply with Alaska’s Cloud computing ethics rule be expected to employ a consultant to monitor the industry trade journals, provide warnings, and recommend solutions?

If the largest CSP in the world has security issues and hacking problems, is there no hope in using a smaller company?

3. **If the Cloud creates opportunities for catastrophic failure, then the attorney’s focus could be directed to his or her control of the environment outside the Cloud.**

The attorney is responsible for encrypting and controlling the material that is delivered to the CSP; so, disclosure of confidential or privileged information is less likely even if the data is lost.

Use of the Cloud and the possibilities for its backups does not abrogate the attorney’s responsibility to exercise proper backup procedures off-site with the attorney’s control; so, the client’s files and attorney’s data are not with the sole control of a single provider.

---

\(^{19}\) “Prior to engaging with a cloud computing service, a lawyer should determine whether the provider of the services is a reputable organization.” Alaska Bar Association Ethics Opinion No. 2014-3, https://www.alaskabar.org/servlet/content/1934.html


V. IDENTIFICATION OF POSSIBLE RELATIONSHIPS BETWEEN AND AMONG PARTIES INVOLVED IN CREATING AND USING THE CLOUD.

A. Outsourcing your IT needs with Software as a Service, Infrastructure as a Service, or simply off-site backup.

CSPs are third-party entities that minimally store data, and may provide software licenses for an enterprise’s data creation and manipulation needs, including Web hosting, and more generally, IT services (accounting, recording keeping, court filing systems). These services may be complete encompassing all your fully outsourced, or as little as an off-site backup resource.

Terminology in the industry may also reference these same companies as “SaaS,” or “Software as a Service” providers. Another term that is frequently used is “IaaS” or “Infrastructure as a Service.” The SaaS or IaaS designation highlights the use of the CSP’s versatility and capability of providing more than remote data storage. The CSP may take responsibility for the Cloud customer’s software licenses since the software is run on the CSP’s computers. The “sale” or licensing of software is turned from a single transaction for each software used, into an environment where all IT activities are supplied by a third-party vendor, and are maintained off-site.

Realizing the breadth of a CSP’s activities, including providing software licenses and sublicenses to companies, this paper will use “loss of data,” to mean all the services and data enumerated in the customer contract.

The use of “you” or “your” within context, means the Cloud customer (the entity contracting for Cloud services), the IT professional reading this paper, or the professional advisor to Cloud customers. Many, but not all of the references in this paper focus on “you” the lawyer with a firm representing the Cloud customer, CSP, lenders landlords or tenants, as will be identified within this article.

B. Who finances what and where: from the CSP’s facilities to the equipment holding your software and data, every creditor to every borrower in the chain of transactions wants protection.

CSPs may own their servers and data centers. A CSP could also lease a facility from which to run its servers. The CSP with which you contract may even subcontract its storage and computing needs to third parties, and you as a CSP customer are even more removed from your data.

The CSP’s data is stored on a storage device. You may commonly think of a storage device as a hard drive or an optical drive (like a CD, DVD, or Bluray disk), or even a flash or thumb drive that plugs into a USB port. All these items are storage devices.

A Cloud customer’s use of a CSP located within the United States could be subject to some or all of the following:

- Equipment and software security agreements
- Software licensing agreements
- Liens created and filed by lenders to both landlords and tenants
- State constitutional and statutory liens, filed by either the tenant’s or landlord’s contractors
- Government tax liens

Priorities and both formal and informal relationships may govern how these entities work to achieve their goal: getting paid. Bankruptcy proceedings may make further adjustments among the parties, and their relative bargaining strengths. Ultimately, your client’s data is caught in the middle of these negotiations.

Entity barriers exist between your data and you, and all potentially have claims that interfere with access and control of your data: developers, landlords, CSP-tenants, Cloud customers, and lenders and mortgagees at every step.

The facility owner is considered the landlord in this paper. The landlord may develop its own facility, in which case it may have a construction lender until the landlord moves to a long-term financing lender. A landlord may purchase an existing industrial facility with help from an acquisition financing lender.

These lenders are all related to the landlord and potentially adverse to the CSP and your data.

---

24 “A storage device is any computing hardware that is used for storing, porting and extracting data files and objects. It can hold and store information both temporarily and permanently, and can be internal or external to a computer, server or any similar computing device. A storage device may also be known as a storage medium or storage media.” TECHOPEDIA, April 25, 2017, https://www.techopedia.com/definition/1119/storage-device

25 Other possibilities exist where an owner-operator becomes a tenant. For example, ByteGrid offers data center owners the opportunity to “Monetize your Real Property and Mission-Critical Infrastructure Assets – Enabling you to redeploy capital into your core business operations.” Sale/Leaseback, http://www.bytegrid.net/saleleaseback.php (last viewed by author on ____________).
The CSP is considered a tenant for the purposes of this paper. The CSP as a tenant has the most tenuous of relationships, since its rights in a lease agreement are usually inferior (or subject to) all other parties involved in development (landlord, construction companies, mechanics and material supplier lien holders, and lenders). As we’ll review later, your software and data on the CSP’s servers are similarly inferior in rights to the CSP and all of its relationships.

Cloud customers enter into agreements, physical or online, regarding their use of the Cloud. Some companies provide free use of Cloud services. Whether free use or paid, and whether online or on paper, these agreements (often called Terms of Service or Privacy Policies, etc.) in this article are called Cloud customer contracts.

C. Utility regulation in states outside your jurisdiction may allow destruction of your data.

State utility regulations commonly include electricity. In addition to those regulations, special legislation may grant or deny powers or rights outside of utility regulators’ purview. Regardless of the competing claims on the equipment on which your data and software resides, your data’s survival may depend upon utility regulation or legislative approach within the state where your data is maintained.

Cloud customers may not assume the regulatory and statutory provisions for utilities are applicable to the Cloud agreement for many reasons. The easiest to imagine, however, is the storage of data in another state or jurisdiction. Utility regulations or statutory fiat may control your CSP’s access to power. What if power is intentionally interrupted—not by a utility, but by a CSP’s creditor or even its subcontractor where the server is physically located—all within the governing state’s laws, and all without recourse by your client for its damages?

Utility interruption in accordance with state laws and many commercial leases may be allowed or, if not statutorily allowed, waived, by the entity closest to servers holding your data. Utility interruption may prevent your client’s or your access to data and may also jeopardize the data itself. A sudden power outage alone may destroy data or interrupt business operations.26

An issue closely aligned with this potential interruption is whether business interruption insurance would cover this type of catastrophe.

The insurance would be obtained in a policy approved by one state (assume Texas for this example), but construed to be applicable to data centers and power facilities located in another state.

- Is this cross-state border business interruption insurance foreseeable?27
- What if the CSP switches data center locations from Washington State to Virginia – does your cyber insurance company need to know?
- What if the CSP does not notify its Cloud customer where the data is located? (Data transportability is a security policy as well an efficiency mandate for some CSPs. This topic is discussed in more detail later.)

D. Redundancy of data and software, or “Here, There and Everywhere.”28

1. Redundancy of your data and software enhances continuity while creating independent security risks.

Redundancy, the storage of all data and applications you use from the CSP, protects data, but places it out of your control, and maybe in a foreign country.29 Redundancy may mean storage on multiple

26 Tex. Prop. Code §93.002(a) governing commercial leases provides:

A landlord or a landlord's agent may not interrupt or cause the interruption of utility service paid for directly to the utility company by a tenant unless the interruption results from bona fide repairs, construction, or an emergency. Section 93.002(h) states that a lease may supersede this provision. In the author’s experience the vast majority of commercial leases include a waiver of §93.002(a).

27 Compare to business interruption for a leased premises.

The insurance underwriter can examine the property and confirm that safety codes are being met. The insurance company is also familiar with building inspection procedures in the state in which the policy was obtained. With data distributed through the Cloud, none of these geocentric safeguards are available to the underwriter.

28 Copyright words and music John Lennon and Paul McCartney 1966.

29 CSP Syncplicity discloses a minimum of information about its redundancy standard in a Web page few customers may not normally read entitled “Syncplicity Reseller Program” with, “Data is stored in quadruplicate across three geographically dispersed data centers to deliver 99.999999% durability of data.” Many consumers would not think the “Syncplicity Reseller Program” page would have information valuable to him or her as a consumer.

http://www.syncplicity.com/partners/resellers (last viewed by author on ____________).

There is no disclosure of whether the locations are in the same state or international or some mix of international and national sites. The representation seems to set a minimum standard of “quadruplicate” storage, and would allow more than 4 locations. Having several locations, creates more difficulty for your client or you to have access to and control the data. Having more than one location in a single state or in a single country
devices where all the devices exist at one geographical location. For example, your data resides on a server with serial number 135 and a server with serial number 246, both located in the same building 400 Gates Drive, Billingsly, Montana. Server 135 may not be subject to a security interest under a UCC-1, while server 246 may be subject to a security interest by a lender to a CSP. Should you have a concern if others hold security interests in servers holding your data? This level of detail could have implications we will discuss later.

If the CSP offers redundancy in the form of your data stored in multiple locations, then secrecy may both add protection and reduce your control over information. Your information is not in one place but in several—all at once—and some locations may be outside the United States. Your client's or your data could be stored in Billingsly, Montana and India. The redundancy is minimal, but valuable. An earthquake in Billingsly, Montana would not effect data in India, while a tsunami in India would not impact data and computational ability in Billingsly, Montana. The data in India, however, is less within your control and independently susceptible to attack.

2. Filing of security interests and notices of property exempt from security (lien) agreements conflicts with the CSP's physical security (against terrorism) interests.

Your challenge to identify your data and assert ownership rights in the data becomes not only an interstate, but potentially an international nightmare. Even your access to your CSP’s geographical locations is not certain. Secrecy is integral to the Cloud industry for both vendors and consumers of Cloud services. Your client or you may be unaware of the international connection to your data until you face a crisis or until the data is breached.

Our state-by-state public records filing system poses challenges to Cloud industry vendors, lenders, landlords, and consumers. If you do not know the location of your data (Austin, Texas or Billingsly, Montana), you cannot see

- If any prior liens exist on the equipment; or,
- If there are claims to funds from contracts; or,
- If a recorded instrument assigns to another party your Cloud contract; or, certain specified interests in your Cloud contract; or, your contractual payments to your CSP.

VI. RELATIONSHIPS REMAIN UNSETTLED BETWEEN (1) SECURED PARTIES AND LIEN HOLDERS AND (2) A THIRD-PARTY’S DATA AND SOFTWARE, PARTICULARLY WHEN PRIVACY ISSUES ARE CONSPICUOUS.

A. Secured lien holders have a duty to prevent the debtor’s asset from wasting.

Generally, a lien holder has a duty to the debtor to prevent an asset’s wasting. If any prior liens exist on the equipment; or, if there are claims to funds from contracts; or, if a recorded instrument assigns to another party your Cloud contract; or, certain specified interests in your Cloud contract; or, your contractual payments to your CSP. Proceeds from the asset’s sale would be applied to the existing debt, but the secured creditor could continue to seek the deficiency. This greater deficiency (greater than it would be otherwise) was proximately caused as a result of the creditor’s willfulness or negligence while the asset was in the creditor’s possession. To the extent the asset’s undiminished value would more than pay for the secured creditor’s debt, then other creditors (second lien holders or unsecured creditors) are also harmed by the first secured creditor’s action. Punishing a debtor or subsequent creditors because of the first secured creditor’s actions does not make sense.

---

Amazon’s Web Services, called Amazon Simple Storage Service (Amazon S3) is among the most transparent of CSPs allowing customers options for geographical regions for data storage. The regions are defined as US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo, Brazil) and GovCloud (US) Regions. The US Standard region allows routing to either Northern Virginia or the Pacific Northwest. Amazon S3 states an object “stored in a Region never leaves the Region.” This representation is critical because of European Union (EU) financial, employment, and personal privacy policies, which are very different from the United States, yet critical to international companies and international transactions. “Amazon S3 Functionality,” Amazon Web Services, http://aws.amazon.com/s3/, (last viewed by author on ____________).

30 “The owner of a facility doesn’t necessarily want to have the address or name of the building out in the world, because what they’re doing is very secretive,” said Brett Boncher, project manager at Cupertino Electric, which installs data center electrical systems.” SAN JOSE MERCURY NEWS (CA) VIA ACQUIRE MEDIA

B. What information must be disclosed to the lien holder about data stored on the secured collateral — and who has that duty?

If a lien holder owes the CSP-debtor a duty to protect an asset from waste, how far does that duty extend and what cooperation may be expected from the CSP-debtor and third-parties which have a relationship with the CSP-debtor? Does it go beyond the asset to data on the asset? If so, then the lien holder would expect to have notice of the asset to be protected, including the data.

The challenge is for the CSP-debtor (or the CSP-User – possibly an attorney) to provide information about the data held on the server enabling the secured creditor can take steps to protect the collateral.

The data changes constantly. How would a CSP-debtor know what is on its servers at any one moment? The CSP-User does not have an obligation to update the CSP; the CSP-User operates independently of the CSP. But it is possible the CSP-User could voluntarily update the CSP about data stored on the CSP’s servers. If the data was unencrypted, then the CSP could be aware of the nature of the data or relationships between the attorney and his or her clients. Encryption creates a presumption of the attorney’s intent to keep the information privileged and confidential, and not available to the public.

Assume the CSP-User is an attorney.

For an attorney disclosing the nature of the data, e.g., a patent, a merger, or information regarding a real estate acquisition may involve disclosing the name of the client or the nature of the client (Example, “Blackacre offers”).

There are times when even an attorney’s disclosing the client’s name may indicate some special type of relationship or hint at future activity. For example, a firm known for family law matters, or one representing employees in discrimination claims, or a criminal defense firm may have Jane Doe as a client. That information alone may be valuable to third parties. The client’s confidentiality is clearly at risk with disclosures of relationships.

VII. THE SECURED CREDITOR FACES UNRESOLVED CONFLICTING OBLIGATIONS WHEN TAKING POSSESSION OF THE CSP’S COLLATERALIZED EQUIPMENT.

Assume you, as an attorney, represents a secured lien holder that has just taken possession of the CSP’s equipment. What do you do to advise your client of its duty to the collateral? The answer to this question involves an analysis of these issues:

- Does data become part of the collateral?
- Is data an “after-acquired” asset considered as part of the collateral (like cash in the proverbial cash register)?
- Is the addition of data in storage considered a modification of the asset?
- Are there some contractual obligations owed to the CSP-user or third-parties as a result of the data’s storage on the secured collateral?

Basically, do you tell your client the secured lien holder to protect data on the servers or to destroy the data? Protecting the data would contribute to the CSP’s continuity. It would make the servers and storage devices more valuable if part of an ongoing business. Alternatively, the data on storage devices must be protected from breaches and that creates liability for the secured lien holder.

If the data is critical, such as a health care record (for example, indicating an allergy to peanuts), just unplugging the equipment (from electrical power or from the Internet) and denying access may cause harm. Is that harm foreseeable?

Does a secured creditor have to maintain electricity and Internet access to protect the data and prevent the asset (the data on the servers) from wasting?

Texas has a statute prescribing destruction of business records containing personal identifying information. The statute is addressed only to “customers” of a business. Cloud Customers’ agreements are between the CSP and the Cloud Customer. The secured lien holder’s business relationship is with the CSP, on which the secured lien holder has foreclosed. There is no identifiable contract or direct relationship between the Cloud Customers and the secured lien holder. The secured lien holder does not owe a contractual obligation to Cloud Customers.

Moreover, in anticipation of these issues, every CSP agreement this author has reviewed includes waivers of the “Warranties Against Interference And Against Infringement.” There may be debate as to whether a Cloud Customer is leasing equipment or contracting for a service, but the CSPs construct the agreements so they appear, in part, as a traditional lease.

Can any notice to the CSP by the CSP Customer that personal identifying information or health care information of third parties is being stored at the CSP be effective as to the secured lien holder? This author doubts it.

32 TEX. BUS. & COM. CODE § 72.04
33 TEX. BUS. & COM. CODE § 2A.211
“(a) There is in a lease contract a warranty that for the lease term no person holds a claim to or interest in the goods that arose from an act or omission of the lessor other than a claim by way of infringement or the like, which will interfere with the lessee’s enjoyment of its leasehold interest.”
Is stored data part of the business records of the CSP or of the CSP Customer? If the CSP’s Customer is an attorney is the data the CPS’s Customer’s Customer’s data (the client’s business record)? Does the CSP Creditor acting have a right to destroy the data without harming the equipment?

If the your client is a Secured Lien Holder and it takes possession of the equipment and data residing on the storage devices?

- How is notice for access provided when data, not necessarily copyrighted nor displaying appropriate confidentiality notices, is part of the protected asset?
- What examination may a creditor conduct to determine ownership?
- If the data is encrypted, and since many encryptions are easily broken, does the secured lien holder have an obligation to attempt to decrypt the data to determine ownership?
- What examination may the secured lien holder allow a Cloud Customer in order to access its data? [This question focuses on the situation where a server holds the data of more than one CSP customer, a likely incident.]
- Does the secured lien holder have an obligation to release the data on the storage devices if a CSP Customer tells a secured lien holder that it does not have access to copies of the data?

Assume your client or you place data with a CSP, and the CSP loses control of the data to a creditor of the CSP. 34

- Would your client or you be responsible for data breach notices to your client's customers or your clients?
- Does a foreign state’s breach notification law apply to your client’s data merely because
  - the CSP’s place of business is controlling for data breach; or,
  - the data contains information about citizens of other states or countries?

Not all these questions have answers at this time, but the abundance of data centers and CSPs make these questions likely to occur.

CSPs may have automated systems that move your data, for administration purposes, among the hundreds or even hundreds of thousands or even millions of servers it owns. Some of these services are in this country while some may not be. Geographical proximity to the Cloud Customer is not necessarily controlling in the transfer of data and the manipulation of the information.

Even if you knew data storage locations and the storage locations were stable, you as a CSP Customer may not want to disclose that information. Public filings' disclosure could lead to attacks on your data. Some Cloud Customers may not want the CSP with which they do business identified.

CSPs often are secretive about their own data center locations. Undisclosed locations provide security by preventing physical terror attacks (bombings, etc.) or cyber attacks (which in the future may include computer-based power-grid interruptions targeted at geographical areas).

High value information, often held by law firms, may become a target. China is alleged as the source of attacks successfully breaching security at law firms in the United States and Canada. These security concerns are not for the future because the incidents have occurred. These security concerns exist now.

**VIII. WILL YOUR DATA “TAKE A RIDE ON THE MAGIC BUS.”**

The author’s personal tale may be instructive as to some possibilities related to data storage and IP address location. The story begins at the Infomart in Dallas, Texas.

I registered a domain with a company called Verio in the late-1990s. I knew the owners and if I had a problem, I could come down the Dallas North Tollway and visit with them. I could have face-to-face meetings. I could see the servers on which my domain and data were stored. They could make changes as I watched.

Verio, a Texas corporation with principal place of business in Dallas, Texas was acquired by Nippon Telephone and Telegraph. The owners disappeared to a

---

34 While this paper discusses many ways in which the CSP may lose control of data, consider foreclosure on a CSP’s servers used as collateral for a lender or a landlord asserting a lien on personal property for violations of a lease agreement. Both lender and landlord could litigate priority of liens.


happier place. Verio wrote that some of its data was going to be transferred to its servers in Florida. It advised where the server with my IP address could be found. Verio could have transferred the data without notice to me, but at the time, it was a company sensitive to customer relations.

Later Verio, still a subsidiary of NTT acquired other companies including a company in Utah. Verio determined that the laws of Utah were unfavorable for ISPs such as Verio, and removed all the data from Utah. At around this time, all Verio’s data in the United States was consolidated in either California or Virginia.

Eventually, I learned that Verio purchases its domains through a company named MelbourneIT. MelbourneIT is located in Melbourne, Australia. In order to continue to operate my domain, at one point, I had to open an account at MelbourneIT in Melbourne, Australia. There was no way, at that particular time for me to renew my domain name registration without opening an account in Australia. I had no idea that Verio did not acquire its domain names directly.

The liabilities for some businesses to open an account and have their domain operated in a foreign country could be very significant.

Australia has a provision in its privacy laws that if a subsidiary is obligated to handle data in accordance with Australian law, and the data is transferred to the parent, which is outside Australia, then the parent of that subsidiary is required to handle the data as though the data was still in possession of the subsidiary. Instead of limiting liability by a parent entity creating a country-specific subsidiary, liability actually increases by extending to the parent.38

The lesson to take from this author’s series of transactions is that your client’s data or your data may unexpectedly find itself in another state or country’s jurisdiction, and subject to other laws.

IX. WHAT ENTITIES ARE GOING TO SAVE YOUR CLIENT OR YOU IN CASE OF LOSS OF DATA?

If the entity’s CSP or an entity further down the chain from your provider is responsible for the data loss or business interruption, then coverage issues and replacement costs and loss of business will be important. The threshold question is whether these coverages exist, do these organizations have such coverage, and are the amounts sufficient.

If you are a professional, and a client’s data is lost or transactions using software inaccessible for the failure, then the focus becomes:

- Does your general liability or professional liability insurance provide coverages for loss of client data where the data is held by a third party (your CSP)?
- Does the defaulting CSP or its defaulting subcontractor have insurance that would cover your client’s or your law firm’s damages?
- For professionals, does your data loss alone violate an ethical cannon? In some states, violations of ethical regulations create causes of action for malpractice from clients and awards of monetary damages.

X. “BUT IT’S THE INTERNET, DON’T YOU UNDERSTAND?”

A. For those still holding on to the “Too Big to Fail” doctrine for protection in the Cloud-provider discussions, consider Nortel Networks and Dropbox.

The bankruptcy judge in March, 2012, described Nortel’s fortunes succinctly.

In 2000, Nortel reported approximately $30 billion of annual revenue, employed nearly 93,000 people, and had a market capitalization of over $250 billion. Nortel’s business was essentially two-fold: the supply of physical hardware with embedded or bundled software and the deployment and support of that hardware.

Competition for innovation in the telecommunications industry, high operating expenses, the deterioration of the global economy and a general decrease in demand for some of Nortel’s products, in addition to previously described difficulties, caused Nortel to confront a full-blown liquidity crisis and the insolvency proceedings in Canada and here.

These economic conditions and market forces may describe the Cloud-provider industry, just as they described the telecommunications and networking industry in 2004. According to the judge’s description, how much different is a CSP’s activities than Nortel’s? A CSP supplies hardware (rented or purchased) with

bundled software. Consider this recent description of Dropbox, a CSP:

“Dropbox Inc. followed the Internet start-up playbook to a tee last year.

“The online file-sharing company became a hot property in Silicon Valley and snagged a [sic] $250 million in venture capital at a $4 billion valuation. It even secured celebrity investments from U2’s Bono and his bandmate, The Edge. . . .

“At all that valuation, five-year old Dropbox is worth as much as companies with multibillions in revenue, such as Cablevision Systems Corp. and Expedia Inc.

“Dropbox is now racing to keep up with that growth and prove its business is sustainable. The 100-person company recently moved into an 87,000-square-foot office in San Francisco where it plans to hire hordes of engineers and product managers.”


For comparison and to appreciate Nortel Networks’ capitalization of $250 billion, at the end of the fourth quarter (Q4) of 2001, here are some comparisons:

Apple at $6.84 Billion;  On April 25, 2017, $758.33 Billion
Microsoft at $336.66 Billion; On April 25, 2017, $524.85 Billion
Cisco at $132.76 Billion. On April 25, 2017, $167.36 Billion

All of the companies listed above remain in business, but the valuations are very different now. The Internet is fluid.

B. Since the Internet may be accessed anywhere, electricity power supply for Cloud computing data centers drives the Internet and Cloud computing.

1. Electricity is related not only to energy, but political power and corporations’ branding and profits.

Electric supply contracts are complex and touch practical and philosophical business goals. Some businesses strive to have a green designation, and the source of electricity may be part of that arrangement. These companies may seek wind, hydro, or solar generation in whole or in part in order to fulfill a larger business ethic. There may be a divergence in corporate goals between

1. Being green, and for example locating to Iceland and using the cold waters there for cooling; and,
2. Being a “good” United States corporate entity and maintaining jobs in the United States.

Electricity contracts may not be about electricity supply, but about branding and marketing factors unrelated to cost of goods.

2. Electricity markets are variable since factoring costs of production and future demands, making corporate planning challenging.

To the extent electricity contracts are about the supply of electricity, there are opportunities for purchase through long-term contracts. These long-term contracts provide a target usage and a variance of for example 15% more or less during any billing cycle. This variance is subject to negotiation. Charges may be dependent upon facilities, and for example certain types of businesses may anticipate closing existing facilities and adding new ones. The contract, separately from the 15% variance to the target use, may allow for other locations or facilities to be added to the contract at the same rate as the original contract.

There is a futures market in electricity supply and while suppliers may use the futures market to arrange
for actual delivery of electricity some electricity consuming companies may use the futures market to arrange for hedges to the volatility of electric pricing.

C. “The Do No Harm” mantra of Internet companies is not universal.

Consider this case regarding a data center transaction for those of you who still believe the computer industry is populated with good and honorable people running good and honorable companies.

Calling the plaintiffs/counterclaim defendants collectively, “Sterling,” and the defendants/counterclaim plaintiffs, collectively, “Digital,” we can discuss the sale of Sterling’s 350,000 square foot data center facility (the Property) in Phoenix, Arizona, to Digital, along with SNS, the entity operating the data center. SNS “sold” space and power to third party customers. Digital bought the building and SNS, so there was a real estate component and a securities (stock transaction) component to the purchase/sale agreement. At 12 times the Net Operating Income (NOI) of SNS, Digital paid $171,703,038 for the property and SNS, combined.

One of the closing agreements selected Arizona law as applicable, while another selected Delaware. All the parties agreed that there was no significant difference between Arizona and Delaware laws on the subjects, and agreed Delaware law would apply.

Digital asserts it was not granted full access to the property prior to closing, and the power supplier would not discuss with Digital its current contract without consent from the property owner (Sterling), which consent apparently was not forthcoming. Digital asserts Sterling falsely represented that the capacity of the utility services at the property was adequate. Additionally, Sterling over-committed the available power capacity at the property by signing 120 new contracts soon before closing. The power was inadequate to serve the existing Sterling (now Digital) customers and the new 120 (Sterling, now Digital) customers. Sterling promised customers a performance impossibility right before closing.

Digital alleges the last 120 new customer agreements entered into before the sale were designed to increase the purchase price at 12 times NOI. Digital’s problem was not only did they pay 12 times the added value of these contracts to the NOI, but Digital asserts these last 120 new customer agreements required more power to operate than could be accessed at the Data Center. Sterling argues the contract and closing documents required only that it deliver power to the existing “tenants and customers.”

The court quotes Digital’s assertion:

“... Property is, in general, an improperly engineered building, not enough generator capacity, not enough UPS [Uninterruptable Power Supply] systems, and not enough cooling infrastructure.”

Digital alleged $20 million in damages to meet these new customer commitments.

The what-ifs are worth noting:

• What if Digital could not “cover,” in contract remedy terms? What if Digital could not have afforded to honor SNS’s agreements for the last 120 customers by paying the allegedly $20 million in extra costs for power and infrastructure, and potentially temporary relocation of client data and computing power and software to other facilities? In other circumstances the excess infrastructure and power charges could have forced the entity acquiring SNS to go into bankruptcy. Without the rent stream, the property owner (if a separate entity) may have defaulted on its mortgage. This effect cascades through other parties in interest and their mortgagees or lenders. Maybe, the assets, including the servers on which your client’s data may reside would be sold at auction.

• What if you, as a lawyer, represented Digital in the acquisition? Do your firm’s examinations in a real estate transaction include detail representations and warranties by utilities and other parties to the transaction regarding capacity to a property? Does this case help establish a new standard for due diligence for attorneys in real estate cases, especially in data center cases?

• What if Digital is accurate in asserting the power capacity to the property was inadequate because of the last 120 new customers, and SNS could not meet its obligation to the new customers, and your law firm or you represented one of these 120 customers who asked you to “just glance at this...

---

47 Id. 7.
48 Id. 8.
49 Id. 10. There is no discussion of the difference between “tenants” and “customers” and how priority of their claims on power would be managed, in the event Digital could not have afforded the extra power costs.
50 Id. 8.
IT agreement to be sure it’s okay?” Does this case help establish a new duty lawyers owe clients in a Cloud transaction?

XI. “YOUR MONEY OR YOUR DATA, OR BOTH;” OR, “SKIP THE MONEY—JUST GIVE ME YOUR DATA.”

A. Comparing financial safeguards with data protection and control.

Which would cause the greatest disruption to your personal and professional life: access to your bank account or access to your all your data? The answers vary upon scheduling. Is today payroll? Are trust funds missing? Must a brief or tax return or 10Q report be completed and filed today?

Let’s examine and compare sudden failure in both instances and see the recovery options available for both.

1. Banks are monitored, ratings disclosed, and the federal government encourages and provides transition for absorption of customer accounts by a new entity.

Acquired banks have a smooth transition from the failed entity to the new bank, complete with instant temporary vinyl signs. Your checks and ATM cards work just as they did on Friday before the acquiring bank’s opening in your old bank’s location.

The Federal Deposit Insurance Corporation (FDIC) closed 92 banks in 2011, 2 of which did not have “acquiring bank” arrangements. For 2012, the FDIC closed 51 banks of which 2 had “no acquirer.” There were 8 bank failures in 2015.

You may compare a “no acquirer bank failure” to a bankruptcy liquidation. Where there is no acquiring bank, the insured deposit limits are as established by the FDIC which varies over time. Thanks to government regulation, depositors apply to receive their insured funds. Even in cases where there are acquiring banks, things change dramatically. For uninsured funds, there is no timetable for access, and they are lost. But as a bank customer, you’re aware of the risks of uninsured funds, and you have a free market choice to risk uninsured funds or not.

For the 4th Quarter of 2015, of the 6,270 reporting institutions with FDIC insured deposits, there were 183 “Problem List” banks, with assets of $46.8 billion.

In these instances of bank failures, if there are interim findings, and a public disclosure of agency regulated operating agreements, customers receive warnings. The FDIC has put the bank on notice and works diligently to find an acquiring institution. The FDIC encourages a resolution prior to receivership.

2. If data is as important as money, why isn’t there a government agency that monitors and regulates Cloud Service Providers? Does the federal government devote any resources to encouraging resolution of CSP bankruptcies prior to the closing of the company in order to protect the CSP’s customers? No. The Cloud customer is left to the vagaries of the market.

Is there any industry organization that emphasizes the importance of having secure data in our commerce and has the resources and authority to take steps to protect Cloud customers? No.

Your client and you are on your own. It is not only a free market, but it is a market in a territory that’s not a state.

You may think these business arrangements are different than banks because they occur through the Internet. In 2012, 2 Internet banks failed. The Internet does not make transactions safer.

If banks can fail, do you really believe CSPs cannot and will not fail?

---

51 Clients often begin requests for document examination with this phrase when the client does not have much time for examination, the client has only a small amount of money allocated to the examination, or both. Also, the client often works on the documents thinking she, he, or the entity, already knows enough about the subject matter to operate successfully without advice from attorneys. In this instance, if the IT department already approved and negotiated the contract, the client’s confidence may be high. Client’s are rarely interested in fine points such as access to electrical power.


55 FDIC, EDIE Estimator, Welcome to the FDIC’s Electronic Deposit Insurance Estimator (EDIE), https://www.fdic.gov/edie/

56 You may lose your banking relationship with lending officers and other bank contacts.

57 FDIC QUARTERLY BANKING PROFILE, FOURTH QUARTER 2015, downloadable at http://www2.fdic.gov/qbp/qbpSelect.asp?menuitem=QB P

You may think you're protected with a CSP, that you'll receive notice or understand if things are not going well, and you'll be able to move your account. You may be wrong as is discussed later.

If you have a problem with your bank's, closing, the FDIC gives you a toll-free number: 877-ASKFDIC and TDD access at 800-925-4618.

Do you have an emergency toll-free number independent of your CSP for when your CSP does not answer its phones?

In your business, if you make arrangements with a CSP you may face unlikely events in crisis, or you may recognize risks and guard against them with careful planning.

B. A CSP’s size may be relevant, but is not controlling for your or your client’s decision, since size creates other risks.

Just as big banks have economies of scale that pressure smaller competitors, large CSPs and data centers have a similar advantage. Large high-tech firms have traditional advantages in purchasing (or designing and making their own) servers, storage, and cooling and power equipment.

The largest data center companies have another and distinct advantage in operations: they can control electricity cost. Apple is building 20 megawatt solar farm on 100 acres and a 5 megawatt fuel cell plant across from its data center in North Carolina. In assessing this competitive advantage, one commentator noted, “Adding a lower cost of electricity to the mix just makes it much harder for small and medium-sized data center companies.”

Building facilities in climates that are advantageous to cooler temperatures creates another option to lowering electricity costs for cooling. Only very large companies are capable of managing logistics of building and operating facilities in, for example, Iceland; so, again, size plays a large part in the data center economics.

There have been bank failures in a highly regulated industry; and, and for the most part, customers have been protected. Protection of our money is supervised by our government. Large banks, however, have been in trouble.

In our service economy, in “The Information Age,” access and manipulation of data is money. There is no governmental safety net. Cloud customers are all on their own. CSP and data center failures may be as likely as bank failures in a regulated and highly supervised industry.

This paper next examines Cloud transactions, protections, and liabilities and risk shifting negotiated in the market or established under current law.

XII. KEY INDUSTRY FACTORS EFFECTING YOUR NEGOTIATIONS AND YOUR LIABILITY TODAY: THE CLOUD COMPUTING INDUSTRY BASICS AND TRENDS.

The number of data centers is not easily calculated and the estimates vary greatly.

There are lenders and debtors at every level in providing Cloud facilities. A facility owner-provider would not have these same levels of claims at that facility, that may be most common to the data center industry. The emphasis on “at that facility” is to highlight that with redundancy, data could be stored in a facility owned by a CSP and in a separate facility the CSP leases from a landlord. So, the same data at the same time, may be on different machines in different states with different laws regulating control of the equipment on which your data resides. You often would not know your data’s location.

A. Economies of scale and facilities planning win the day.

Servers and data storage facilities are filled with racks of computers. These computer facilities are centralized for maintenance, management, and security control. A server center needs a low-cost power source, as well as, backup power storage, and if necessary, electrical generation capabilities. Efficiency in keeping the hardware cool and at operationally optimal temperatures is critical. Once a location has been deemed satisfactory, the investment is long-term and substantial.

1. “If you build it, they will come.”

The Cloud center industry finds a 20,000 square foot facility notable enough for press coverage. But that size is small in comparison to international corporations and their delivery of Cloud services. Apple constructed a 500,000 square foot, $1 billion data center in North Carolina. IBM plans a 6,200,000 square foot

60 See discussion in VI, B.
61 Paraphrase of “If you build it they will come,” from the 1989 movie Field of Dreams, screenplay by Phil Alden Robinson.
62 Kelli Davis, TekLinks Announces Opening of Third Data Center, Press Release, April, 8, 2011,
Facebook recently announced the opening of its own facility in Prineville, Oregon, and construction of another in North Carolina. Facebook acquired 120 acres for the Prineville Facility. Within 15 months construction completed on the first 150,000 square feet and the first building opened. Construction on another 150,000 square feet in the second portion of the first building has begun. Major companies, such as Apple, not only have their own facility, but lease data center facilities.

2. Power availability and cost, even more than contiguous space, dictates the location of CSPs and data centers.

Power is critical to a data center facility location, and its cost may be the most significant single factor in choosing a location.

Data centers in the United States used 2% of all electricity in 2014, and the predictions are that this energy consumption could increase by 40%.

The largest single-building data facility currently in the United States is the 1.1 million square foot location in Chicago. This facility houses 79 entities affiliated with the Chicago futures markets. For Con Edison, the 350 E. Cermak building’s electricity use is second only to Chicago’s O’Hare Airport.

To help understand power’s importance you’ll want to note the description of Apple’s leasing data center space in a May 18, 2011, description in Theflyonthewall.com.

DuPont Fabros signs Apple as a tenant, Data Center Knowledge reports. In April, Apple (AAPL) signed a seven-year lease for 2.28 megawatts of critical power load in a new data center being built in Santa Clara, Calif. By DuPont Fabros Technology (DFT), a leading developer of wholesale data center space, according to Data Center Knowledge.


Data Center Knowledge reports. In April, Apple (AAPL) signed a seven-year lease for 2.28 megawatts of critical power load in a new data center being built in Santa Clara, Calif. By DuPont Fabros Technology (DFT), a leading developer of wholesale data center space, according to Data Center Knowledge.

The press release did not highlight the square footage that Apple leased, but the megawatt of critical power load. DuPont Fabros, a REIT (Real Estate Investment Trust), composed the press release used by the media, since other sources had the same description. DuPont Fabros and Apple, decided the most important element of the lease was the data center’s available power in watts. Square footage was literally irrelevant, and not even mentioned.

The square footage of a lease agreement may be misleading as an indicator of the size of a facility. As processors become smaller and designs more sophisticated, more computing power (more wattage use, more heat generation), will be stacked in smaller spaces. The amount of space servers occupy may decrease, while the data storage capacity increases. More data in less space drives the industry.

Real estate, power, and personnel may cost less overseas. Remote server management allows for
international location of servers reducing costs and increasing flexibility. Economic and redundant solutions achieve catastrophe planning goals and are consistent with the Internet’s operation where any computer can find any other computer, and there is no singular way to get from computer Alpha to computer Omega.

B. Location, Location, Location; or, why your data center’s location matters.

1. Computerized trading governs location for equity and hedge funds.

   The world’s largest data center (as of this writing) is 350 E. Cermak, not even 3 miles from the Chicago Mercantile Exchange (which is the entity that includes derivatives trading. The CME trades agricultural, metals, energy, foreign currency, and equity index, and futures and options trading products. All these products allowed the world-wide subprime lending crash.

   Why consider location for data centers? Light travels at 186,000 miles per second.

   • The distance from Downtown Dallas to the CME at 20 South Wacker Drive, Chicago, Illinois 60606 USA is 968 miles (by car). Time: 0.00520430108
   • The distance from Downtown Dallas to the CME at 20 South Wacker Drive, Chicago, Illinois 60606 USA is 968 miles (by car). Time: 0.00001505376
   • Trading time difference: 0.00518924731

   If transaction speeds are not as critical as in stock trading, then more options to reduce cost exist. There are other trade-offs to consider.

   The placement of the center so it requires less cooling is obvious. Place the data center in a cooler climate. Since the external environment is already cool, then the internal environment has to be cooled less. Temperature and direct energy consumption is not the only consideration.

   The Intelligence Community Comprehensive National Cyber-security Initiative (IC CNCI) data center’s location matters.

   For computerized derivatives trading, speed is everything. If you’re not first, then the price at which you want to buy or sell, may disappear after someone beats you to the trade. Data centers need to be close to where “the action is” to be most effective.

2. Data centers cost money and electricity is the greatest on-going expense.

   If electricity is the data center’s greatest expense then within the geography of acceptable times for transaction speeds, the CSP wants to reduce cost. This cost reduction may be accomplished by 2 direct means:

   1. Reduce the direct cost of electricity.
   2. Reduce the need for electricity by placing the data center in a location that requires less cooling.

   If transaction speeds are not as critical as in stock trading, then more options to reduce cost exist. There are other trade-offs to consider.

   The placement of the center so it requires less cooling is obvious. Place the data center in a cooler climate. Since the external environment is already cool, then the internal environment has to be cooled less. Temperature and direct energy consumption is not the only consideration.

   The Intelligence Community Comprehensive National Cyber-security Initiative (IC CNCI) data center’s location matters.

   For computerized derivatives trading, speed is everything. If you’re not first, then the price at which you want to buy or sell, may disappear after someone beats you to the trade. Data centers need to be close to where “the action is” to be most effective.
or each fingerprint

Violation is provides for a civil penalty of $25,000 per “violation.”

a fingerprint or iris scan) compromised, Texas law necessarily an employee’s) biometric identifier (such as

constituting statute-defined “personal identifying

number compromised or a combination of other data

being defined.81 There is no certainty if “business record”

includes $500 per “business record,” without “business record”

information,” then your company could be liable for

penalties. For an individual’s loss of data, Iowa

provides for individuals to bring actions and receive compensation of 3 times actual damages or $5,000 (Five thousand dollars) (whichever is greater).82

These penalties are exclusive of any requirement for notification to effected parties of breach or wrongful access to their data. These notifications can easily reach a cost of $250,000. Even if no damage claims were made, the notification process could be damaging to a company’s long-term viability.

- Does the Cloud Provider form contract include a provision that your company indemnify the Cloud Provider for any actions brought against it for loss of data?
- Are all these liabilities properly shifted to your company by the contract, when the goal was to place your company’s data in the hands of an expert dedicated solely to managing servers and data?

You may wonder what are the chances of your company’s data getting shuffled around so other than Texas law could apply. The answer is very good. You’ll find data centers and cloud providers in Texas, Illinois, Ohio, New York, Washington (state), Virginia, and California. The single largest operating data center is in Chicago, and this one building uses more electricity than any other user in Chicago, except one: O’Hare International Airport.

One of the author’s clients was working with a software development company in Texas that shifted its server use to Lansing, Michigan. When my client decided it did not want to defend suits in Michigan or have a court hold Michigan law would apply to its transactions, it moved the domains, data, and software to a different Texas cloud provider; yet, allowed the software developer to continue to work and maintain the software and financial transaction data.

XIV. ETHICS AND STATE REGULATION FOR PINK ELEPHANTS; WHAT IF THERE IS NO CONFIDENTIAL OR PRIVILEGED INFORMATION?

If privacy protection from the government is futile, do protective measures even matter or does the likelihood of spying encourage vigilance? Consider the following information from the NSA through the Intelligence Community Comprehensive National Cyber-security Initiative ICCNCI:

center is located in Utah.78 This data center is easier to protect physically79, and the climate is not so adverse that it would be difficult attracting employees. Compare this Utah location to Antarctica (which the United States does not control nor is it part of the United States) or the Arctic in Alaska, where finding and supporting employees may be more difficult. The IC CNCI data center in Utah does have the advantage of potentially using solar energy for power as the technology develops to be more cost efficient.

The direct cost of electricity has another variable, which unrelated to government security needs, may encourage location of data centers in other countries. Pollution controls may factor into the cost of electricity. Therefore, a location with fewer pollution controls may be warmer initially than a geographically cooler climate, but the difference in greater electricity use may be narrowed when considering the cost of electricity.

Global climate change and world-wide treaties to address issues of climate change may impact electricity pricing in ways that have not been considered. There could be carbon taxes, carbon neutral activities related to electricity consumption, and even new technologies developed in order to comply with country and world-wide global carbon-use mandates. These choices may effect CSP data center location and applicable laws.

XIII. “HOW EXPENSIVE CAN MISTAKES BE?”

CIO and IT consultants do not have the perspective or to identify legal risks and liabilities.

Texas is a business-friendly state. Tort reform and limitation of damages for pain and suffering are old news in Texas. So, surely, one may conclude, Texas has favorable laws regarding privacy and data protection. But that conclusion would be wrong.

If your company were to have a person’s (not necessarily an employee’s) biometric identifier (such as a fingerprint or iris scan) compromised, Texas law provides for a civil penalty of $25,000 per “violation.” Violation is not defined as whether it applies to one file or each fingerprint within a file.80

If your company were to have a social security number compromised or a combination of other data constituting statute-defined “personal identifying information,” then your company could be liable for $500 per “business record,” without “business record” being defined.81 There is no certainty if “business record” means all the information in a single file or each individual’s personal identifying information.

Let’s take Iowa as another example of data loss penalties. For an individual’s loss of data, Iowa

81 TEX. BUS. & COM. CODE §72.004
80 TEX. BUS. & COM. CODE §503.001
82 IOWA STATUTES 714.16B IDENTITY THEFT — CIVIL CAUSE OF ACTION.
79 The area around and above the IC CNCI can have a no-fly zone excluding all aircraft.
Your Data: If You Have Nothing to Hide, You Have Nothing to Fear

. . . What if we could build a national data warehouse containing information about every person in the United States? Thanks to secret interpretations of the PATRIOT ACT, top-secret Fourth Amendment exceptions allowed by the Foreign Intelligence Surveillance Court, and broad cooperation at the local, state, and federal level, we can! 83

[The exclamation point after “we can” is on the NSA Web site.]

The IC CNCI data center advertises to fulfill this position (below), with this notable qualification, (below):

**Job Title:** Domestic Intelligence Specialist
**Job ID:** 6662013
**Location:** Utah Data Center . . . Strong curiosity and inquisitive nature when examining highly personal information

This qualification was not number one in its list. Maybe individuals can develop this trait once they are an employee.

Even if government knows everything, an attorney or even a business or individual may have an interest in other individuals or companies not knowing everything. A business may have competitors, a person may have nosy neighbors or relatives, etc. The attorney’s obligation is not diminished.

**XV. IN THE EVENT YOU’RE NOT A CEO, CFO, CIO, OR, MOST POWERFULLY, A CCF YOUR LAW LICENSE, AS A PRACTICING ATTORNEY, MAY BE IN JEOPARDY.**

C-level abbreviations are common, but you’ll find this legend below for convenience.

- CEO: Chief Executive Officer
- CFO: Chief Financial Officer
- CIO: Chief Information Officer
- CCF: Chief Control Freak

If you do not have any of these titles, then your law license may be in jeopardy even if you have the best of intentions regarding technology adoption and disclosure.

A law license is given to an individual attorney. A firm does not receive a law license. Yet, as an individual attorney, you may identify issues and solutions to problems, but be unable to implement them because of technology intransigence in your firm. The solution you may want to implement may be no more than disclosure to clients of your IT practices and receiving approval, or even just asking clients for their direction on how to handle certain information. Your solution may be correct. But correctness is rarely a reason a course of action is adopted.

How do you protect yourself? Ethics rules do not have whistle-blower provisions. There are no ways for you to register your concerns (even secretly), and escape consequences of ethical violations.

If the law has not kept up with technology, then just as surely, law firms have not kept up with technology or the impact of technology on substantive matters. The ABA Ethics 20/20 report referenced earlier just now addresses technology use 30 years after computers were widely adopted by lawyers.

If you bring a client to a firm, and if your firm’s engagement agreement does not include disclosure about encryption or even that your firm allows encryption as an option, and the firm suffers a breach which negatively impact your client, to whom will the client blame or have recourse? The individual attorney is the disciplinary target. In Texas, violation of a Disciplinary Rule, alone, does not give rise to a cause of action. Other states have different rules. But there are no rules for firms in Texas.

You as an individual do not have a “safe harbor” provision in the ethics provisions. The ethics rules encourage your leaving the firm to protect your license, when you may be the attorney best capable and most needed to institute change.

If the State Bar of Texas were to adopt rules applicable to firms or set minimum standards applicable to all attorneys (just as the federal government did for all physicians with HIPAA’s passage), then all firms will comply. A competent voice will not be perceived as a trouble-maker wanting adoption of cost-increasing administrative burdens, but will be seen as a valued asset.

Innovative and clear technological standards for all attorneys do not exist now and none appear on the horizon. No safe harbor provisions exist protecting individual attorneys who may not be in a position to set firm policy or arrange for variance for his or her clients. While patients perceive HIPAA as protecting their rights, then the State Bar of Texas has not seen that technology and privacy provisions are aimed at protecting client rights.

83 Domestic Surveillance Directorate, *Defending the Nation. Securing the Citizens.* “Your Data: If You Have Nothing to Hide, You Have Nothing to Fear,”

https://nsa.gov1.info/data/index.html
XVI. IF CLOUD COMPUTING IS AN INTERNATIONAL TRANSACTION, WHAT OPTIONS EXIST FOR PROTECTION OF CLOUD CONSUMERS?

A. Disparate factors such as a highly educated and English-speaking work force to low-cost labor to inexpensive construction costs to green computing branding, all push for internationalization of the Cloud computing industry.

While arguments for ethics and a lawyer’s control over data suggest lawyers could demand Cloud computing contracts tailored to their goals, many Cloud Customers may not have these restrictions in negotiation. These nonlawyer Cloud Customers will have other goals and parameters for negotiations with a Cloud Provider.

Many CSPs use data storage facilities in foreign countries. Your client or you may not be able to control where data is held, nor should your client or you presume U.S. law is applicable to data storage or transfer.

Facebook, even before its users were at 800 million, recognized it has more users outside the United States than within. Facebook is built a server facility in Sweden. While this data center will provide a node for better communications for European users, there is recognition the data traffic is subject to surveillance by Sweden’s National Defense Radio Establishment, known by Swedish initials as FRA. The constructions costs are estimated at $760 million and the total size of the 3 buildings is about 904,000 square feet.

Google turned a paper mill in Haminam, Finland, into a data center using Baltic Sea water for its cooling systems.

Every country seeks to exploit its advantage of workforce, Internet connectivity, and clean power. For example, Iceland has renewable energy in a temperate climate. Olafur Olafsson, CEO of Green Earth Data expects 5% to 10% of the world’s data to flow through Iceland. The reliability and cost of power is low at less than one-half the price of electricity in the United States. This pricing makes foreign location attractive.

The marketing aspects of being “green” may make alignment with Facebook an advantage not apparent by price alone. The more commerce conducted over and through a Facebook page as compared, for example, to a Web site hosted by Amazon (which may not have renewable energy facilities in Iceland or the U.S. or wherever it claims the Web site is stored), makes the consumer feel as though his or her or its choice has made an impact.

B. Since IBM is building what may be the world’s largest private data center in China, what would happen if some of these Creditor – Debtor issues arose there? Would the result be different in Hong Kong?

The government response among private parties in China seems similar to the response of an orderly transition in a bank take-over as structured by the FDIC and the Comptroller of the Currency here in the United States.

If a CSP (as a debtor) owes money to a lender or a landlord (as a creditor), then the procedures do not involve self-help. In quick review, secured interests, perfected by UCC-1s or Deeds of Trusts do not exist in China. So, the approach is much different.

The expectation is the CSP / Debtor (as holder of the personal property, the computers in this instance) would approach the Administration of Industry and Commerce (AIC). Depending on the circumstances this entity may take possession of the computers, or may meet with the parties and then determine which administrative action to take. If the AIC rules in favor of the creditor, then the AIC would supervise an orderly turnover of the property to the Lender / Landlord. This orderly transfer would include supervising the personal property owner’s (again, the Lender / Landlord) transfer
of all the data, and then deleting the data before taking final control of the equipment.

If a party to the dispute were to receive a preliminary injunction before the AIC hears the case, then the AIC will “almost always” enforce the injunction, even though the AIC has the power to make and enforce its own independent and conflicting decision.

Additionally, in a court proceeding, the owner of the data could sue for damages related to the loss of data and costs incurred.

The proceeding in Hong Kong would be different. Hong Kong retains English common law concepts of liens, pledges, and the perfection of security interests. If there is a “charge” against “movable property” then the charge can be registered with the HK Companies Registry. Failure to register may prevent the lienholder from asserting its secured interest in the personal property. The consequences of failure to register in the HK Companies Registry would, in general, not completely bar the lien. The consequences would be less severe than failure to follow lien registration procedures in the United States.

CONCLUSION: MODELS FOR INTERSTATE AND INTERNATIONAL RELATIONSHIPS GOVERNING CLOUD COMPUTING PROVIDERS.

Corporate laws are individual by state. Yet, Delaware, a state with a small population has captured most of the incorporations of Fortune 500 companies. The state of incorporation does not have an impact on the headquarters of a company, or its principal place of business. New York state has 57 Fortune 500 Companies, while Texas 52 and California has 50.88

Within the United States, each state could adopt laws designed to protect businesses or consumers using Cloud computing.

These laws may include an entity’s declaring it is a Cloud Service Provider thereby triggering government protections.

These protections may include the following:

• No landlord or utility company could interrupt any utility service until cleared by either a Bankruptcy Trustee or a Receiver in a state administrative proceeding.

• Creditors would be given access to servers only through a judicial proceeding, and with appointment of an ombudsman responsible for protecting a cloud consumer’s data.

• Data auctions would be prevented.

• Data destruction would be prevented.

• Acquiring creditors interested in maintaining the business relationship with customers for at least one year, could be given incentives through the government agency.

• No government authority, as a result of a bankruptcy or receivership proceeding would have any additional access to the data that it already possessed, unless through a court order in the matter.

• The bankruptcy or receivership administrators would not have authority to grant waivers for access to data.

These ideas may be interesting but you’ll want to know who will pay for them? A reserve could be established with “insurance fees” similar to the FDIC or the Pension Benefit Guaranty Corp. so the Trustee could have access to resources enabling an orderly transfer of data. Additionally, the Trustee may need these funds to initiate and maintain adverse proceedings from government agencies or other entities claiming access to the data. The answer is all of us will pay for them through a tax (like the FDIC tax on banks) based upon the CSP’s gross revenues. The tax could be calculated based upon Gigabytes of storage or transmission bandwidth or both. Programming or operational charges could be included or excluded as well.

While each state could adopt these types of measures individually, the United States could decide that access to information coupled with privacy create a public interest to all citizens of the United States. Accordingly, the Commerce Clause of the Constitution could be used to enact preemptive federal legislation.

Now that domestic CSP issues are resolved (see preceding paragraph), let’s examine options for addressing these issues in an international forum.

The World Trade Organization determined electrical energy is subject to its regulations. The authority comes from The International Convention on The Harmonized Commodity Description and Coding System. “Mineral fuels, mineral oils and products of their distillation; bituminous substances; mineral waxes” are subject to regulation, and electricity is derived from fuels. Countries have regulated the international trade of electricity.89 This regulation enabled the United


89 Leonardo Macedo, Electricity energy and the WTO customs valuation agreement, WORLD TRADE ORGANIZATION, ARTICLE, RESEARCH AND ANALYSIS, JULY 2, 2010
States to lodge a complaint against India for its alleged requirement for domestic-sourced solar cells for power generation and for advantages for long-term and favorable electricity tariffs for the purchase of electricity by these generating companies.90

The United States is not leading in these proceedings since the European Union has requested consultations with Canada regarding Canada’s alleged laws and regulations favoring the use of domestic-sourced items for the “renewable energy generation facilities.”91

So far, there have been no WTO actions about the pricing violations of Cloud computing or data center access. The WTO may not consider cloud services a “good.” Have you prepared your client for the impact of WTO regulation on its CSP contracts?

Japan’s government has a Cloud Computing plan.

- Does our federal government?
- Does any state government?

Does your firm have a cloud computing policy consistent with the industry’s practices and client expectations?

Are Cloud legal ethics appropriately regulated in your state?

Have you adequately warned your clients about the problems and uncertainties of Cloud computing?

Could your clients be reasonably disappointed you didn’t discuss these issues with them in greater detail?

Most favorably, you could view issues associated with Cloud computing as an opportunity for you to provide unexpected value to your client. The client may have focused only on the technical aspects of the contract and left the decision-making to the IT department. You now have an opportunity to intervene and warn of business uncertainties and both resolved and unresolved legal issues associated with the Cloud technology. You have an opportunity to grab the client before he or she falls to earth.

---

90 India — Certain Measures Relating to Solar Cells and Solar Modules, Request for Consultations by the United States, Addendum, WORLD TRADE ORGANIZATION FEBRUARY 10, 2014

https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009- DP.aspx?language=E&CatalogueIdList=122489&CurentCatalogueIdIndex=0&FullTextSearch=


https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=116589&CurentCatalogueIdIndex=0&FullTextSearch=
EXHIBIT A:
Cloud customers lose, along with landlords, lenders, and debtor-tenants, if all parties do not cooperate.

Professionals may relate to a dispute involving a law firm’s dissolution when approximately one-third of the partners left. What’s unusual in the following example, is the law firm Weinstock & Scavo announced cessation of continuing representation of clients. The landlord declared them in default of the lease. A large section of the firm left, and remaining members and associates of Weinstock & Scavo sought other positions. The property management firm declared Weinstock & Scavo in default under the lease provisions, accelerated the lease payments approximately $9 million, and sued to have the firm placed in state receivership.

Weinstock & Scavo asked for a renegotiated rent for the floor vacated when Scavo and 11 other lawyers left the firm to join another. With a relatively new landlord and management company, twenty-four years in the building did not hold much sway when Weinstock & Scavo sought modification of the lease and lease terms. Its space needs were less (with about one-half of a floor fewer attorneys), and the market value of rents had fallen substantially from when the firm entered into its last lease. Unsatisfactory lease negotiations led the landlord to sue the law firm Weinstock & Scavo in a fight to control the law firms’ accounts receivables and other assets.

The landlord asserts liens for unpaid rent in the amount of $7 million, while challenging liens the firm granted remaining attorneys up to the amounts of their salaries in an effort to hold the firm together. Subsequently, the lawyers with those security interests withdrew the liens granted in their favor. In a situation which resembles a default in a Cloud computing case, the landlord is left trying to collect on its lease agreement using the receivables of the now disbanded law firm. As founding attorney Michael Weinstock, questioned, “How many of the accounts receivables could be collected by a landlord who sues and gets a judgment from an abandoned corporation?” The remaining lawyers in the firm took their practices to other firms.

As of May 31, 2011, the firm removed its personal property from the leased premises. According to the law firm’s counsel, Jim Cifelli and Greg Ellis, of Lamberth, Cifelli, Ellis Stokes & Nason, P.A., the landlord’s lien covered the personal property (i.e., computers and storage devices) and there was no financing lien that covered personal property, although the law firm did have financing through SunTrust. SunTrust’s financing was covered by a lien, but the lien did not extend to the firm’s personal property.

The landlord’s attorney brought an action in state court, which among other relief, sought to have the law firm placed in receivership. The landlord’s attorneys specifically requested that the state court-appointed receiver have authority to place the company in federal bankruptcy. The judge denied the motion. The firm may be solvent on a current cash flow basis, but its contingent liabilities, including the $7 million accelerated under the lease agreement, made the situation precarious.

SunTrust, a lender, filed liens as security, including ones that appeared to reach accounts receivables. Michael Weinstock, a shareholder of Weinstock & Scavo and personal guarantor on the SunTrust note, purchased the debt and the security from SunTrust. He therefore assumed SunTrust’s priority, ahead of the landlord. The landlord claimed the conveyances and transfers from SunTrust were fraudulent, but these claims were rejected by the court.

The adverse positions and claims among the landlord, lender, and debtor-tenant mirror positions that may be taken in a Cloud computing case. The failed Cloud computing entity’s clients are no more likely to pay outstanding invoices than a law firm’s clients. Here there was a dispute over control of the computers, the software, and data which are contained on the law firm’s computers, just as if the debtor-tenant would be a Cloud computing entity. The landlord did not succeed in having a receiver appointed for the law firm; which left the lender (now Michael Weinstock), the landlord, and the defunct firm to have individual actions challenging priorities when a coordinated solution may have been more beneficial.

Counsel for Weinstock & Scavo distinguished the business aspects of a CSP’s failure from the law firm’s handling of its data. The files held by the law firm (and the data on the computers) belong to the firm’s clients. The law firm has a legal obligation to protect and return the files (both electronic and nonelectronic) to the clients. The clients can direct transfer of their files to other law firms.

93 Telephone interview with Jim Cifelli and Greg Ellis, partners of Lamberth, Cifelli, Ellis, Stokes & Nason, P.A., counsel for Weinstock & Scavo (July 5, 2011).
A lawyer formerly with Weinstock & Scavo created a special purpose company to manage the winding down of the firm including collecting receivables, payment of on-going liabilities, return of files to clients, and any other outstanding matters. As with a Cloud computing debtor-tenant entity, each client may have maintained copies of its data.
EXHIBIT B:

Provisions in Cloud Contracts undermining a Texas attorney’s “reasonable expectation . . . the independent contractor will not disclose or use materials or their contents except as directed by the lawyer.”

The quotation reference above is from Texas Committee on Professionalism Op. 572.

The provisions below are excerpted from various clauses in Terms and Conditions, or Service Agreement applicable to Amazon’s various products and services — all relevant to Cloud use.

Individually, any of these clauses defeat the criteria established in Texas Supreme Court Committee on Professionalism Opinion 572 for a lawyer’s ethically contracting with third-party, independent support staff or entities. Combined, these clauses in interrelated agreements and governing documents remove any doubt as to who is in control of the relationship. While a form contract is not inherently one-sided, the ethical challenge to the practicing attorney is to maintain that the CSP is cognizant of the lawyer’s ethical responsibilities. In this instance, AWS may be cognizant of the lawyer’s ethical responsibilities, but AWS makes clear it will do nothing to help the attorney accomplish his or her goals, and given the opportunity will work against compliance.

This author has reviewed many CSP contracts, and while all these provisions relate to services and products Amazon offers, this same approach is used by many other providers.

The approach is not unique to CSPs. Many of these same clauses are found in third-party, off-site, physical storage agreements for legal documents. So, the same caution should be exercised in examining any storage agreement or agreement affecting your storage, including your firm’s lease agreement with its landlord.

The following clauses have references to the document, and the effective date of the last changes, as well as links to the online version of the document.

AWS Customer Agreement Provisions

8.1 Your Content. As between you and us, you or your licensors own all right, title, and interest in and to Your Content. Except as provided in this Section 8, we obtain no rights under this Agreement from you or your licensors to Your Content, including any related intellectual property rights. You consent to our use of Your Content to provide the Service Offerings to you and any End Users. AWS Customer Agreement, 8. Proprietary Rights, 8.1 Your Content, Last updated March 18, 2016, http://aws.amazon.com/agreement

8.3 Adequate Rights. You represent and warrant to us that: (a) you or your licensors own all right, title, and interest in and to Your Content and Your Submissions; (b) you have all rights in Your Content and Your Submissions necessary to grant the rights contemplated by this Agreement; and (c) none of Your Content, Your Submissions or End Users’ use of Your Content, Your Submissions or the Services Offerings will violate the Acceptable Use Policy. AWS Customer Agreement, 8. Proprietary Rights, 8.3 Adequate Rights, Last updated March 18, 2016, http://aws.amazon.com/agreement

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS Customer Agreement, 4. Your Responsibilities, 4.1 Other Security and Backup, Last updated March 18, 2016, http://aws.amazon.com/agreement

9.1 General. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from . . . (including reasonable attorneys’ fees) arising out of or relating to any third party claim concerning: AWS Customer Agreement, 9. Indemnification, 9.1 General., Last updated March 18, 2016, http://aws.amazon.com/agreement

13.2 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including AWS Customer Agreement, 13. Miscellaneous, 13.2 Force Majeure, Last updated March 18, 2016, http://aws.amazon.com/agreement

AWS Service Terms Agreement Provisions

13.7 You will retain title to any Media and Data we receive from you and store on an AWS Service . . . You supply us with Media and Data entirely at your own risk. . . . We are not responsible for and will not be held liable for any damage to Media or any loss of Data. . . .


94 What if you do not have title to the Data? What does “title” to Data mean?
13.8. You represent that you have all necessary rights to (a) provide the Media and/or Data to us for upload into supported AWS Services and (b) authorize our transfer of any Data specified by you to the Media or Appliance and to you. Without limiting the foregoing, if your Data includes personal information, personally identifiable information, personal data, or any information about a person or individual covered by applicable law or regulation, you represent that you have obtained all necessary rights to transfer such Data to or from the AWS region you select, and you will comply with all of your obligations with respect of such Data as required by applicable law or regulation, which may include obtaining consent of the subjects of such Data. We may reproduce Data as necessary to transfer it between Media or Appliances and supported AWS Services.


13.9 . . . WE HEREBY DISCLAIM ANY DUTIES OF A BAILEE OR WAREHOUSEMAN, AND YOU HEREBY WAIVE ALL RIGHTS … (WHETHER ARISING UNDER COMMON LAW OR STATUTE), RELATED TO OR ARISING OUT OF ANY POSSESSION, STORAGE OR SHIPMENT OF MEDIA OR DATA BY US OR OUR AFFILIATES OR ANY OF OUR OR THEIR CONTRACTORS OR AGENTS. YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA . . . .


13.10 [Y]ou agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims . . . .


Exhibit C Sample Language for Attorney Engagement Agreements re: Breach and Cloud Use.

A law firm not based in Texas he following language in an engagement agreement.

11. EMAIL AND ONLINE CLOUD SERVICES. Attorney Firm endeavors to take appropriate precautions to protect private information. In order to work efficiently Attorney and Firm will communicate with Client via telephone, email, and Internet-based video conferencing.

Attorney and Firm may also store files in secure, encrypted, online services. Client hereby agrees to:

(a) receive certain documents via email or other online services, unless Client states otherwise;

(b) communicate with Attorney using online media and video technologies;

(c) allow Attorney and Firm to store client documents and billing information on reputable third-party online services, commonly known as the “Cloud”; and (d) be billed via email and other online services. Client acknowledges and agreed agrees that no form of communication is completely secure. Therefore, a breach of security that was not caused by negligence on the part of Attorney and or Firm shall not constitute a negligent breach of the attorney-client privilege.
“Cloud Computing, Ethics & Engagement Agreements”

By: Joseph Jacobson
214-207-8819
joseph@jacobsonlawyer.com

Or

“No One Is Here To Help You”

By: Joseph Jacobson
214-207-8819
joseph@jacobsonlawyer.com
Walk out now; Trouble is inevitable. You will
- Feel compelled to redraft client engagement letters
- Learn the unthinkable happens
- Find Governments [all governments everywhere] and legal ethicists are not helping you

Cloud (Data Center) Industry
- Goals
- Strategy
- International inevitability
“Show me the data”
- Your client’s data / Your data and 3rd Party Rights
- Data around the world
 Modified from “Show me the money,” said by the character Rod Tidwell in the film, *Jerry Maguire*

“You can’t handle the truth.”*
- Federal / State conflicts
- International trade issues

* Col. Jessup from the movie *A Few Good Men*
Is my data at risk?

- I’m not important.
- My clients aren’t important.
- Want a job at the Intelligence Community Comprehensive National Cyber-security Data Initiative?

The IC CNCI data center advertises to fulfill this position (below), with this notable qualification, (below):

**Job Title:** Domestic Intelligence Specialist  
**Job ID:** 6662013  
**Location:** Utah Data Center  
[Listed job qualifications include]

“**Strong curiosity and inquisitive nature when examining highly personal information**”
IC CNCI Internship Program

Joseph’s Mom’s Voice Mail

- Big Data Analysis of your unencrypted data
- Google Voice
- Data analysis means advertising revenue
Alaska Cloud Ethics Opinion

Before hiring a CSP (like ISP), “a lawyer should determine whether the provider of the services is a reputable organization. The lawyer should specifically consider whether the provider offers robust security measures.”

Who is the biggest & best?

AWS has 10 times the computing capacity in use than the Next 14 largest cloud companies Combined. Including (Yes) Google, Microsoft, etc.
Industry Alert April 24, 2014

“[L]ack of security best practices from . . AWS . . HP and GoGrid.”

Rod Trent, WindowsITPro

AWS Failure < 60 days later June 18, 2014

“[N]o way to restore the data, Code Spaces . . . winding down the operation and helping customers migrate any remaining data to other services.”

Dan Goodwin, Ars Technica
AWS Failure 1 day later
June 19, 2014

Websolr and Bonsai reported “similar AWS infrastructure compromises in what may be a series of attacks against AWS-based cloud providers.”

Brandon Blevins, *TechTarget.com*

Was the Alaskan Law Firm Compliant?

Industry publications indicated trouble.

Who reads them?

What do they mean?
Texas Supreme Court
Professionalism Committee
Opinion 572

Q: Without client’s express permission may a lawyer deliver client’s privileged material to an independent contractor (copy service) hired by lawyer?

Copy Service Op. 572

A: Delivery of privileged material is not “revealing” [DR1.05(c)] provided “the lawyer reasonably expects independent contractor will not disclose or use materials or their contents except as directed by the lawyer.” (emphasis added)
Opinion 572 into Action

Cloud Contract Clauses

Just a few tweaks to the form contracts . . .

8.1 Your Content

http://aws.amazon.com/agreement/

As between you and us, you or your licensors own all right, title, and interest in and to Your Content. [Do you?] . . . You consent to our use of Your Content to provide the Service Offerings to you and any End Users. We may disclose Your Content to provide the Service Offerings to you or any End Users or to comply with any request of a governmental or regulatory body (including subpoenas or court orders).
Bailor (not the Waco kind) & Bailee

13.10. IN ADDITION TO THE DISCLAIMERS IN THE AGREEMENT, WE HEREBY DISCLAIM ANY DUTIES OF A BAILEE OR WAREHOUSEMAN, AND YOU HEREBY WAIVE ALL RIGHTS ... (WHETHER ARISING UNDER COMMON LAW OR STATUTE), RELATED TO OR ARISING OUT OF ANY POSSESSION, STORAGE OR SHIPMENT OF MEDIA OR DATA BY US OR OUR AFFILIATES OR ANY OF OUR OR THEIR CONTRACTORS OR AGENTS.

YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA.

AWS Service Terms

13.7  You represent that you have all necessary rights to (a) provide the Media and Data to us . . . and (b) authorize our transfer of any Data . ... You represent that import or export of the Media or Data to or from us does not require a license under the laws or regulations of any country.
"Danger, Will Robinson, Danger"*

Your data and programs are going to a foreign country.

* "Lost in Space" TV Series

http://aws.amazon.com/agreement/

9.1. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys’ fees) arising out of or relating to any third party claim concerning:
You tell vendor about privilege; but,

Vendor tells you there is no privilege.

Engagement Agreement Disclosures

- Firm uses the Cloud;
- Client data in foreign countries;
- Client’s will obtain extended Cybersecurity Insurance for firm;
- CSP protected against claims;
- Client can only sue you.
Ignoring Data Control Problems Is No Solution

Bank failure story and toxic data.  
[Bank = Data Center]

Bank’s Computer Lessor Cleans the Hard Drives
Other Third-Party Vendors

Lease a photocopier?

- Law firm photocopy machine and “lyin’, cheatin’ vendors.”
- Hard drive storage 250 – 512 MB = 125,000 to 250,000 pages

Photocopy Hard Drive Solution

https://www.semshred.com/

hard drive destruction services solutions
Jeopardy

Answer: Encryption

Jeopardy

What allows Cloud use to be both ethical and a solution to IT challenges?
Encryption Risks

Attorneys Justifying Ignoring Encryption with Clients

- “Clients don’t want it, why bother?”
- Compare to physicians and HIPAA
  - Federal mandatory requirement
  - Level playing field
  - Encryption use not a physician differential
ABA Model Rule 1.0

(e) "Informed consent" denotes the agreement . . . after the lawyer has communicated adequate information and explanation about the *material* risks of and reasonably available alternatives to the proposed course of conduct.

Texas Ethics Informed Consent

Rule 1.03(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.
Texas v. ABA

- ABA: “material risks”
- Texas: disclosure of risks necessary to make an informed decision.
- Hacking into email is a federal offense; exposure presumes a criminal act.
- Did criminal acts help Sony???
- Material or Not Material?
Explaining Encryption to Attorneys

- What's *not* encryption:
  User ID & Password access
  [Data is readable, but only slightly difficult to access.]
- Scrambled eggs

Encryption for Attorneys

- You provide *Public Key* to client.
- Posted on Web site; delivered by a trusted method.
- Client uses your *public key* (21) and encrypts file and sends to you.
- You cypher file with your private key (3 x 7)
Encryption for Attorneys

- Client and you must use same program.
- Free Cross-platform programs (Windows, OSX, Linux, iOS, Android) exist.

Pop Test: Warranties in U.C.C., CSP Contract, and Client Disclosures

“Warranties Against Infringement and Against Interference” (Tex. Bus. & Com. Code §2A.211) refers to this protection.
Pop Test Answers

A. No fire during performance from dangling leather strips worn by CW artists
B. Guaranty a bribed referee **IGNORES PASS INTERFERENCE.**
C. Anything to do with IP law (Really, *anything at all*)
D. None of the above.

Answer To Pop Test

No person through act or omission of Lessor will have an interest that would interfere with Lessee’s enjoyment of leasehold interest.
AWS Disclaims Warranties

AWS AND ITS AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING . . . NON-INFRINGEMENT, OR QUIET ENJOYMENT . . .

https://aws.amazon.com/service-terms/

§2A.211 Waiver in Cloud Service Provider Contracts

- CSP’s Equipment
  - Bank financing for equipment
  - Leased equipment
- CSP’s Landlord
  - CSP assigns rents to Landlord
  - Landlord’s lien
  - CSP’s Landlord assigns rents to Mrtg Co.
§2A.211 Waiver in Cloud Contracts

- CSP purchases building it occupies.
  - CSP’s rents assigned
- Trustee / Creditors in Bankruptcy.
- Landlord (if renting, then assignment of rents issue).

§2A.211 Waiver in Cloud Contracts

- Utility companies interrupting Cloud Service Provider’s service.
  - Electricity
  - Internet access
Wave “Bye-Bye” to Client: Indemnification and Waiver

- Client knows you waived everything?
- Client knows you indemnify your CSP?
- Your client’s cyberinsurance carrier approve your waivers?
- Your cyberinsurance carrier approve all these waivers and indemnification?

True Story: Landlord Forecloses on Law Firm

- Law firm splits but PAYS RENT
- Landlord feels insecure; declares default; accelerates $8 million rent
- Landlord asserts lien on computers
- Landlord seeks State receiver
Law Firm Lease Negotiations

- Client files & data exempt from Landlord’s creditor claims
- Same issues with CSP, but you have no privity with CSP’s creditors
  - CSP’s Landlord
  - CSP’s equipment lien holder

Electrical Power

“In April, Apple (AAPL) signed a seven-year lease for 2.28 megawatts of critical power load in a new data center being built in Santa Clara, Calif. by DuPont Fabros Technology (DFT) . . .”
Largest U.S. Data Center in Chicago 3 miles from CME

- 1.2 million square feet
- Only O’Hare International Airport uses more power
- .0052204301 (Dallas)
- .0000155914 (3 miles)

Inevitable Internationalism

- Google to Finland
- Facebook to Sweden
- Any company to Switzerland to escape U.S. and EU spying
Iceland

- 100% renewable energy
- Hydroelectric and thermal
- Goal: 10% of the world’s Internet traffic
- Highly educated, underemployed English-speaking workforce

Pop Test: Who, Where, Why

- 6.5 million sq. ft. Data Center
- Largest in the world
- Who? Where? Why?
### Pop Test Answers

- **Who:** IBM
- **Where:** China
- **Why:** Speed to Asian market
- **Why:** Less expensive labor
- **Why:** Less expensive electricity

### Advantages of Chinese Adverse Proceedings

- No UCC-1 interests
- No self-help
- Administration of Industry and Commerce
- Most likely result: Safe transfer of data before computers are taken
“Don’t you know each cloud contains pennies from heaven.”

Financial Cloud since 1970s
Government Regulation of the Financial Cloud

- CU regulatory liability protection
- CSPs (banks)
  - Audits
  - Federal Supervision of Insolvency

Government Regulation of the Financial Cloud

- Standards make inter-bank access easy. [Compare to HIPAA and physician access across networks.]
- Federal preemption since FDIC, Comptroller Regulation
- 3rd party retailers are at risk
**Unregulated Data Cloud**

- CSPs not insured; not audited
  - State creditor rights apply
  - State laws protect Cloud Users
- Cloud users have full risk
- Contracts prohibit 3rd party beneficiaries [Your law firm’s clients]

**U.S. sees as trade barriers**

- Australia health care law
- Canadian lawyer restrictions
- More international, then less certainty in dispute resolution
- Less certainty, then insurance unavailable
10 Words Businesses Fear Most

“I’m from the government and I’m here to help you.”

Remember:

CIOs: Don’t trust your computers to lawyers.

Lawyers: Don’t trust your law license to IT pros.
Cloud Computing, Ethics & Engagement Agreements

By: Joseph Jacobson
214-207-8819
joseph@jacobsonlawyer.com