RISKS OF CLOUD COMPUTING

RONALD L. CHICHESTER, ESQ.
Law Offices of Ronald Chichester, P.C.

State Bar of Texas
ESSENTIALS OF BUSINESS LAW COURSE:
THE LIFECYCLE OF A BUSINESS
March 6-7, 2014
Houston

CHAPTER 16.1

This paper was originally presented at the Essentials for the General Practitioner Course 2013

Table of Contents

Things to Watch for When Flying Among the Clouds

By Ronald L. Chichester, Esq.
Ron@TexasComputerLaw.com

August 27, 2013

Abstract

Although storing and manipulating data on remote servers via the Internet is not a new technology, it has recently been refashioned into a new service offering, generally referred to as "cloud computing." The pervasive use of cloud computing presents new challenges to lawyers, their clients, and to forensic examiners. For lawyers and clients alike, cloud computing offers many economic benefits. However, recent state legislation and current disciplinary rules impose a duty on the lawyer to maintain the security and the integrity of information stored on the cloud. Lawyers also need to counsel their clients to ensure that their contracts for cloud-based services do not unnecessarily put the client at risk. For forensic examiners, new tools and procedures are needed to identify, collect, preserve, analyze and present electronically stored information ("ESI") that is not within the control of the data custodian. This paper presents identifies various issues related to cloud computing, such as benefits, security, e-discovery, forensics, service contracting and the like.

Keywords: Cloud Computing, Litigation, Electronic Discovery, Digital Forensics, Network Forensics, Internet Service Provider Contracting, Law Enforcement, Privacy, Social Networking

Things to Watch for When Flying Among the Clouds

Things to Know When Your Data (or Your Client's Data) is Stored on the Internet

By Ronald L. Chichester[i]

Introduction

> "[O]ur social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud," on servers owned by internet service providers." *State v. Bellar,* 231 Or.App. 80, 217 P.3d 1094 (Sept. 30, 2009).

There are many benefits to cloud computing. Indeed, the benefits are so many that adoption of cloud services is crossing that tipping point where more adoption leads to yet more adoption. Moreover, certain cloud-based services, such as Gmail, Google+, Facebook, and others take advantage of various network effects that traditional software applications can't match. Consequently, attorneys should know the perils and pitfalls of this not-so-new technology; not only for their own practice, but also for their client's wellbeing.

For this paper, I will adopt the convention of speaking about clients. However, law firms and attorneys must recognize that the issues presented herein apply to you and your firm. As attorneys, you may be involved in securities or malpractice litigation, and the warnings and issues presented in this paper are equally applicable to you.

What is Cloud Computing?

Cloud computing is the placing of data and/or a software application onto a remote (third-party) server that is accessible via a wide area network such as the Internet.[ii] Essentially, the user interacts with their data and/or the software applications used to manipulate that data, typically via a web browser on any device capable of connecting to the World Wide Web of the Internet. Cloud computing will not completely supplant "normal" (PC-based) computing, at least initially. However, more and more services are being accessed online, and the trend is both unmistakable and unstoppable. Indeed, the trend has been likened to rural electrification in the early 20th Century, wherein power generation was centralized and electricity was distributed within a grid to disparate locations, not unlike data distribution via the Internet.[iii]

What are the Benefits?

The benefits to consumers and businesses alike are apparent and substantial. The user does not have to download or install software onto their machine. That eliminates many incompatibilities between the operating system and the software application. The user simply employs one of many (often pre-installed) web browsers that come with their network-capable device.[iv] Moreover, the device that the user *does* use need not be particularly powerful or expensive because the "heavy lifting" can be accomplished on the provider's server. The provider implements security and feature updates to the software in the background without affecting the user's experience. Infrastructure costs are reduced, many full-time IT staff members are furloughed, and training costs are curtailed significantly. More importantly, the tie-ins traditionally imposed by linking office software to operating systems, such as Microsoft Office/Windows, is effectively

broken, making cloud computing a particularly disruptive technology.

What are the Problems?

Instead of buying software and (extra) hardware, the user has to rent space and/or bandwidth on a provider's server. [v] Normally, however, the rental costs are far less than the cost of software and attendant hardware infrastructure – which is why cloud computing is financially compelling. However, with the loss of infrastructure comes the loss of dominion (*i.e.*, both ownership and direct possession) over the data. Loss of dominion over the data can come in several forms, not simply the lack of physical possession.

One problem for the cloud-computing newcomer is vendor lock-in. For example, the service provider may store the information in a proprietary format, making it difficult to "liberate" the data for backup, transfer, or production during discovery. Such tactics are common in the software industry (the proprietary format for Microsoft's Office documents being the most obvious example).

A second problem is that the cloud provider may assert ownership of the data by virtue of contract or copyright. While facts are not copyrightable, the selection and arrangement of facts in a database may qualify for protection under the Copyright Act, and it may be the cloud provider that makes that selection and arrangement, typically as something other than a work-made-for-hire. In general, however, the federal copyright law does not protect databases, which is why service providers may be prompted to include specific data ownership terms in their contracts. If such a clause appears in your user contract, make sure it is on your terms.

A third problem occurs when the service provider interrupts access to your data at any time. Remember, *they* have control over their servers, and they can use that control to their advantage. After all, you're "renting" space on their server. Failure to abide by their rules, or failure to pay the rent can result in termination of access, akin to eviction in real property law.

Finally, there is the issue of data security. For a detailed assessment of the pros and cons of cloud computing (with an eye toward security), see "Cloud Computing Risk Assessment" by the European Network and Information Security Agency ("ENISA"), which is a 125-page critique of available technologies and security issues.[vi] ENISA concluded that:

> "the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective."[vii]

A fourth problem, and perhaps the most prevalent, is financial failure of the cloud provider. What happens when the cloud provider suddenly goes bankrupt or otherwise goes out of business? Do you have to go through a bankruptcy trustee to get at your data? Could the trustee hold your data hostage in order to get money from you? What happens if the cloud provider has to shut its doors immediately, and shut down the servers along with it?

Legal Implications of Cloud Computing

There are several legal implications in the use of cloud computing technology. First, there are the contractual issues between the law firm or client and the provider of the

cloud service. Issues such as corporate compliance (including any attorney-ethics compliance) do not vanish simply by switching the location of the data to the cloud. Secondly, the ramifications of the loss of data (or the loss of the data *and* the provider) can be profound. Finally, there are the electronic discovery issues to be considered.[viii]

Contact Issues

Location of the Servers

While one of the benefits of cloud computing is that you do not have to care where the data is stored – you do need to consider where the data is stored. Many courts are holding that legal jurisdiction over contract disputes involving electronic data take place in the jurisdiction where the data is stored. Moreover, jurisdictional as well as privacy issues may come into play during litigation for electronic discovery, e-commerce and crime investigations. In some jurisdictions, data not within the dominion of the owner can be discovered more easily that data within the owner's direct (physical) control. Similarly, having the data stored in a jurisdiction that is favorable at the termination of the service contract may be desirable for the client or a law firm.

Compliance

"CIOs must understand that data backup and storage in the cloud do not remove a company's responsibility for the legal, regulatory and audit obligations attached to that information." [ix] Law firms and companies often have to account for a variety of privacy laws, such as FERPA,[x] HIPAA,[xi] and others. Industry experts warn enterprises to settle several important compliance issues within the terms of the cloud service agreement.[xii] One of the facts to determine is whether the prospective service provider is *capable* of supporting the audit/legal requirements from a technological standpoint. Compliance audits may require the use of government-sanctioned software applications or techniques. Are the operating systems of the prospective service provider's capable of utilizing the government-required software? Finally, from an administrative standpoint, is the prospective service provider capable of performing the necessary audits in a timely basis. Clauses in the contract can be included that specify the frequency and response time of compliance audits.

Security

There is no shortage of data breaches by larger cloud service providers such as Apple[xiii] and DropBox.[xiv] Forty-six states (including Texas) currently have security requirements that are not obviated by the choice of storage mechanism. Cloud-stored data is still subject to Breach/Notification laws, such as Section 521 of the Texas Business & Commerce Code.[xv] Moreover, the storage of sensitive information, such as Social Security Numbers, is also subject to the same protection requirements of all Texas businesses – regardless of whether it is on the cloud or not.[xvi]

Export Controls

Certain categories of electronic data, *e.g.* encryption software and patent applications, are subject to federal export controls. Permission from the federal government must be obtained to transfer the technology outside of the U.S. For example, transfer of certain categories of technology require a special license from the U.S. Patent & Trademark Office (often called "the Blue Sheet") before the patent application can be sent outside the United States. [xvii] Dissemination outside of the U.S. of certain

types of encryption technology requires the approval of the U.S. Department of State.[xviii]

Loss of Data – "SLA's"

Putting your data on the cloud places reliance on the data's integrity and existence in the hands of another party, namely the service provider. Depending upon your information technology infrastructure, such reliance can be sensible or negligent. Many service providers have good records of data retention. However, mistakes are made. For example, in October 2009, Microsoft's cloud storage facility -- aptly named "Danger" -- suffered a catastrophic failure, affecting more than one million T-Moble Sidekick users for weeks.[xix] Microsoft took herculean efforts to retrieve the data, with marginal success. However, the damage was done.

Loss of data need not be permanent in order to affect business operations. Even a temporary loss of access is enough to cripple critical business processes. Large organizations can require certain levels of performance from a service provider, normally in the terms of a *service level agreement* ("SLA"). The SLA can stipulate the amount of "down time" that the provider is allowed, as well as other conditions. Unfortunately, only those organizations with sufficient bargaining power can negotiate adequate SLA's. For the rest of us (and that includes most law firms), the contracts from the service providers are on a "take it or leave it" basis, with terms naturally in the provider's favor. For all organizations, big or small, it behooves the user to identify the frequency and duration of downtime that can be tolerated, and to check the records of the potential service provider to determine their actual record of outages. The SLA's often are written in terms of "uptime" with the number of "9's". An uptime of three 9's means functional operation for 99.9% of a given period of time (usually on a monthly or annual basis). Three 9's is usually sufficient for most companies. Five 9's is expensive, but can be justified for certain critical infrastructure or e-commerce applications.

Loss of Service Provider

Worse than the loss of some data is the loss of the service provider entirely. While striving to appear like the Rock of Gibraltar, many service providers contend with buggy software, unreliable equipment, razor-thin profit margins, and faulty business models. It is a sad fact that some service providers will go out of business – often while they are still servicing contracts.[xx] Specific performance is not always available, even if you have time to run to the courthouse within the meager time between notice and "lights out." It is incumbent upon the

Access / Backup

While one of the many features of cloud computing is the relief of the chore of backing up data, the cloud-consumer should not feel their duties to back up are at an end. Indeed, lack of access – and thus the need for backups – are often provisions that are written into cloud computing contracts. For example, the notion that the disk space where the data is stored is "rented" to the user by the service provider brings up the specter of landlord and tenant, wherein access to the storage space by the user/tenant is regulated by the "landlord," who can withhold access until the rent is paid in full. Contract provisions should stipulate that access not be denied in the event of a contractual dispute. Similarly, the user should backup their data in the event that the service provider suffers a catastrophic failure (such as servers in hurricane zones) or bankruptcy.

Another "gotcha" with respect to access and backup is the *form* of backup that is made available to the user by the service provider. For example, a service provider may uphold a provision that you can download backups of the data, but do so in a *proprietary* format that you cannot use without special software that can only be procured from the service provider. Yes, you get a backup, but one that you cannot use without the permission of the service provider.

Ownership of the Data

Who owns the data? Note, while the Copyright Act often does not help a third-party provider from obtaining ownership of the data, they often turn to contract clauses to obtain the same effect. Some agreements stipulate that the service provider owns the data that is uploaded and stored on their servers. Obviously, there should be a clause in the contract stipulating that the user is the owner of the data, and that in the event that some copyright law says to the contrary, the service provider will be obligated to assign any intellectual property right in the data to the user.

Loss of Dominion

In the context of cloud computing, dominion is the ability to control data, either by being able to place it with other data, to read it, modify it or erase it. Placing data on the server of a data provider necessarily entails that the service provider has access to that data, and can do with it that which you yourself could do. Moreover, by storing the data on the service provider's server, you give that service provider the ability to interrupt your access to that data – another loss of dominion. With loss of dominion comes a certain loss (or change) of responsibility. Who is responsible for the loss of data? Who indemnifies whom for a loss? Both of these questions are often addressed in the contract between the service provider and the author of the data (the client). However, in many contracts, the risks are not adequately addressed or allocated within the contract. For these reasons, some industry experts caution clients from relying too heavily upon cloud providers.[xxi]

Worse, with the loss of dominion come increased problems with the preservation of documents relevant to litigation, and the corresponding problems with responding to discovery requests during litigation.

Electronic Discovery Issues

Electronic documents and other electronic information are central to every legal matter – even for those matters that do not involve litigation.[xxii] Lawsuits are an inevitable cost of doing business. Consequently, production of electronically stored information ("ESI") is also inevitable. Prudent shoppers of cloud resources should conduct a "dry run" of the production capabilities in order to test the provider's capabilities and shortcomings, as well as what resources are needed within your organization (or third party expertise).

For matters involving litigation (potential or real), an extra duty – preservation – is imposed upon the party.[xxiii] Spoliation of evidence, when there is a duty to preserve it, can prompt a court to impose sanctions on you (the attorney) and/or your client under FRCP Rule 37 (or the state equivalent).[xxiv] Sanctions are often monetary,[xxv] but other sanctions include: the striking of pleadings,[xxvi] default judgment,[xxvii] dismissal of the case[xxviii] or the imposition of an adverse inference instruction to the jury.[xxix] Preservation efforts can be especially difficult when the data is on the cloud, and preservation of metadata (or the data itself) is difficult.[xxx] Fortunately, Rule 37 has some

safe harbor provisions, and the general rule is that sanctions will apply to intentional/willful misconduct, not mere negligence.[xxxi] However, willful blindness allowing for destruction of evidence is not a viable solution.

Computer forensics

Cloud computing complicates computer forensics (the traditional "first step" in electronic discovery). While there are excellent forensic tools for imaging[xxxii] and searching data, storing the data on the cloud renders many of those tools obsolete. In addition, *multiple* organizations are involved in the typical Internet presence, such as web server provider, Internet service provider, email provider, telecommunications companies, router providers and others. Consequently, forensic examiners and attorneys must attempt to gather information from disparate organizations (often outside their normal jurisdiction) via subpoena or warrant. Unfortunately, by placing another organization in the e-discovery loop – with the data stored outside the direct control of the responding party – the discovery process is inhibited.[xxxiii]

An example of complicated e-discovery involving cloud computing is a litigant whose server may in fact be a "virtual" server that is running on a large machine shared by multiple organizations, making the acquisition of a forensic image difficult, if not problematic.[xxxiv] Moreover, the fact that the data is stored on the cloud can complicate admissibility of the evidence.[xxxv] The attorney *must* understand any extra cloud-based problems before conducting the Rule 26(f) [xxxvi] conference with opposing counsel.

For the computer forensics examiner, the shift will be from traditional examination of "dead" personal computers to gathering data from "live" servers for later analysis and presentation. More in-person testimony is likely because the evidence will need to be authenticated using (ironically) the older rules of evidence, specifically Rule 901(b)(1). Examiners can expect to see criminals (and their tech-savvy civil counterparts) use volatile RAM applications to avoid leaving traces of their activities. The key problem for the examiner, however, is the same one that so bothers lawyers – the lack of control over the data/machines that are to be examined. This puts a greater emphasis on logging information about user-activities for subsequent investigation. In general, however, the forensic examiner/ expert witness will have to:

- Identify the parties involved with the litigant's Internet presence;
- Systematically collect and time-stamp the evidence which identifies those parties;
- Save and package the evidence;
- Create a cryptographic hash value of the evidence packet to ensure its integrity; and
- Create a verifiable report that presents the identities of the parties (and any contact information) for presentation at trial or to counsel.

Fortunately, there are many Unix-based tools that lawyers and forensic experts can use to identify parties with potentially relevant evidence.[xxxvii]

Case law

An early case regarding cloud-held information subject to discovery is *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008). The opinion was related to a

wrongful death suit, where the City was accused of covering up a murder of the plaintiff's relative. Earlier, the Court had allowed production of text messages held by a SkyTel, a third party provider. In this particular decision, the Court ruled upon motions to prevent the discovery of the text messages from going forward. The moving defendants argued that the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., wholly precludes the production in civil litigation of electronic communications stored by a non-party service provider (SkyTel). The court rejected this proposed reading of the SCA, observing that "[d]efendants' position, if accepted, would dramatically alter discovery practice, in a manner clearly not contemplated by the existing rules or law, by permitting a party to defeat the production of electronically stored information created by that party and still within its control – information that plainly is subject to civil discovery, see Fed. R. Civ. P. 34(a)(1) – through the simple expedient of storing it with a third party." Because the Court felt that the SCA did not require the preclusion of discovery in such a situation, he allowed the discovery to proceed.

Another case that highlights the potential pitfalls of cloud computing is *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261 (E.D. Mich. Sept. 28, 2006). In this corporate espionage case, an employee of the defendant purposefully inactivated his cloud-based Yahoo! email account which "resulted in the destruction of Yahoo records concerning his computer use." As a result of this act and some other misconduct, the Magistrate in that case recommended an adverse inference instruction as a sanction.

If there is one case that highlights the distinction between "traditional" email and cloud-based email, that case would be *United States v. Weaver*, 2009 WL 2163478 (C.D. Ill. July 15, 2009) (Not Reported). In *Weaver*, the Court ruled that previously opened emails that were stored for less than 181 days in *web-based* email account could be obtained using only a trial subpoena, rather than a warrant. The Federal government sought to obtain emails and other information from a defendant's Hotmail account via a trial subpoena seeking production of "'the contents of electronic communications (not in 'electronic storage' as defined by 18 U.S.C. § 2510(7)' and specified that the '[c]ontents of communications not in 'electronic storage' include the contents of previously opened or sent mail.'" Microsoft, however, felt that a warrant, rather than a trial subpoena, was necessary to compel production, citing their local Ninth Circuit precedent *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003). In distinguishing *Theofel*, the *Weaver* court pointed out the differences within subsections of the Stored Communications Act that were affected by the choice of web-based and traditional email systems – and thus disserving of disparate treatment. This case highlights the lower standards necessary to obtain someone's web-based email records.

In those cases where a warrant is obtained, does the owner of the account need to be notified when the warrant is served on the ISP? That question was addressed in *In re United States*, — F.Supp.2d —-, 2009 WL 3416240 (D.Or. 2009). In that case, the Court concluded that "[i]n this third party context, the Fourth Amendment notice requirement is satisfied when a valid warrant is obtained and served on the holder of the property to be seized, the ISP. In this case, the ISPs were served with the warrants to obtain the relevant e-mails. The requirements of the Fourth Amendment were satisfied." As Orin Kerr observed, "Judge Mosman concluded that Rule 41 and

18 U.S.C. 2703(a) required the notice to be served on the ISP, not the account holder, as a statutory matter," although he did not question that the Fourth Amendment applied to email.[xxxviii]

Social networking sites in litigation

Personal blogs and social networking sites such as Facebook, [xxxix] Twitter [xl] and MySpace, [xli] are treasure troves of information about individuals. Users place pictures of themselves, and often very personal information on these sites. Companies have begun to use the sites as screening tools for job candidates.[xlii] Law enforcement agencies have used the sites repeatedly during investigations.[xliii] Lawyers access these sites to gather evidence for lawsuits, [xliv] or to screen potential jurors during *voir dire*.[xlv]

There are several ethical considerations with respect to social networks. Recently, the Philadelphia Bar Association's Professional Guidance Committee released an opinion on the matter, specifically about posing as someone (a "friend") in order to secure evidence for litigation. [xlvi] A recent conference highlighted the legal and ethical problems with certain aspects of cloud computing, namely the Boalt School of Law at the University of California, Berkley held a seminar entitled "Social Networks: Friend or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking". The law school graciously posted audio excerpts of the presentations as well as links to other materials.[xlvii] These materials form a corpus of core materials on this subject, and would be an excellent starting point for research on the topic.

Conclusion

This paper has highlighted some of the benefits and problems associated with cloud computing. The various footnotes provide starting points for additional research into specific topics. However, there are other topics that are germane to cloud computing, but were not addressed herein, such as compliance with Federal Trade Commission ("FTC") rules, compliance with the Health Insurance Portability and Accountability Act ("HIPPA") and other privacy, trade or securities laws. Each cloud user must decide which laws are applicable to them, and appreciate the duties imposed and benefits afforded.

---

[i] Attorney at Law, Law Offices of Ronald Chichester, P.C. B.S. Aerospace Engineering, University of Michigan, 1982; M.S. Aerospace Engineering, University of Michigan, 1984; J.D. University of Houston Law Center, 1991. Ron is admitted to practice in Texas, the U.S. District Courts for the Southern District of Texas and the District of Nebraska, the Court of Appeals for the Federal Circuit, and the U.S. Patent and Trademark Office. Ronald Chichester, P.C. is a Houston-area law firm providing counsel to law firms and companies on a wide variety of technology-related matters, including electronic discovery, intellectual property, computer forensics, electronic commerce, and corporate computer policies and procedures. Visit the firm website at www.texascomputerlaw.com. A copy of this paper is available at his website: http://www.texascomputerlaw.com/presentations/

[ii] The specific definition for cloud computing varies. For instance, Wikipedia uses several sources in its definition of cloud computing. Specifically, they say "Cloud computing is Internet- ("cloud-") based development and use of computer technology ("computing"). In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet." "Cloud Computing," Wikipedia, which is available at: http://en.wikipedia.org/wiki/Cloud_computing (with interla

[iii] *See*, Nicolas Carr, "THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE" (W.W. Norton & Co., 2009).

[iv] Such network capable devices include traditional laptops ands workstations, as well as newer and smaller devices such as netbooks, iPhones, iTouch, Blackberrys, cellular telephones, etc.

[v] "Bandwidth" is the term of art for the network (Internet) connectivity between the provider's server and the user's machine. Oftentimes, the provider charges for both the storage space (to store the data) and the bandwidth needed to access that data. Other providers allow limited amounts of disk space for free, but sell advertising space on the web pages rendered to the user with their data. Still other providers give away limited amounts of disk space and/or bandwidth for free, but charge for additional space/bandwidth.

[vi] "Cloud Computing Risk Assessment" European Network and Information Security Agency (November 20, 2009), a copy of which is available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/

[vii] *Id*. at 4.

[viii] David Navetta, "Legal Implications of Cloud Computing - Part One (the Basics and Framing the Issues)" published on llrx.com on September 12, 2009, available at: http://www.llrx.com/features/cloudcomputing.htm

[ix] Linda Tucci "Addressing Compliance Requirements in Cloud Computing Contracts" on SearchCIO.com on June 11, 2009, available at: http://searchcio.techtarget.com/news/article/0,289142,sid182_gci1359026,00.html

[x] The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

[xi] Health Insurance Portability and Accountability Act of 1996.

[xii] Some sample questions to ask of the cloud provider are:

Standard General Contract Issues

A. For those organizations with no bargaining power, do you have a "default" contract or standard template? If so, can I see it?

B. What are your backup procedures?

C. With respect to "uptime," what are your rates for the different "9's"?

D. In what format is the data stored on your servers?

E. In what format is it possible to export the data from your hosted service?

F. Do you charge for reformatting the data back for export into commonly used software applications (like Word and Excel)?

Security

G. What security measures are implemented by default?

H. What additional security measures are available?

I. Can we use a VPN? SSH? SFTP?

J. What type of encryption do you support?

K. Who will have access to the data?

L. How can you govern who has access to the data?

M. How can we govern who has access to the data?

N. How granular are the various levels of access to the data? (e.g, full rights for some, limited for others, none for the rest?)

O. Who within your organization will have access to the data?

P. How do you ensure that those within your organization will not compromise the security and integrity of the data?

Q. To implement any (and all) security protocols, what software applications do we need for our users?

Data Ownership

R. Do you claim any ownership rights to the data that we store on your servers? If so, what rights would you claim?

Data Retention/Electronic Discovery

S. Can you implement non-standard "tailored" document retention policies?

T. Can the tailored document retention policies implement selective litigation holds?

U. Can litigation hold-related transactions be logged?

V. What happens if I need to preserve data? Do we need to enlist you to make certain data "read only"?

W. What metadata do you keep about the data?

X. How do you preserve/produce system metadata for the documents stored on the system?

Y. What kind of user/document logging do you track? (e.g., who accessed what, and what did they do with it.)

Z. Are there any additional logging options?

AA. How is the data collection to be done if I need to produce data during litigation?

BB. Who can/will produce the data? (I.e., will we be able to produce the data ourselves? Our third-party expert? Or must we rely on you?)

CC. How much do you charge for identifying/searching/processing/producing the data?

DD. Given that "preservation" of documents and their metadata kick in almost immediately after litigation commences, how soon can you implement a litigation hold notice?

EE. After getting a subpoena, how long does it take for you to produce data?

Privacy

FF. Which jurisdictions are your data centers in, and how is privacy protected in those jurisdictions?

GG. How do you respond to governmental requests for information about your data?

HH. Would you warn us if the government issues a subpoena?

II. How can you ensure that cross-border legal (privacy) limitations on storage of data are met?

[xiii] See Derrick Harris, "iCloud Breach Highlights Some Hard Truths About the Consumer Cloud," Washington Post, available at: http://www.washingtonpost.com/business/technology/icloud-breach-highlights-some-hard-truths-about-the-consumer-cloud/2012/08/06/5e466424-df6f-11e1-8d48-2b1243f34c85_story.html

[xiv] See, Barb Darrow, "DropBox: Yes, We Were Hacked" available at: http://gigaom.com/cloud/dropbox-yes-we-were-hacked/?utm_medium=content&utm_campaign=syndication&utm_source=washingtonpost&utm_content=icloud-breach-highlights-some-hard-truths-about-the-consumer-cloud_550012

[xv] See, specifically, Sections 521.002 (Definitions), 521.052 (Business Duty to Protect Information), and 521.053 (Notification Required Following Breach of Security of Compromised Data); a copy of the text of the statute is available at: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm

[xvi] See specifically, Texas Business & Commerce Code §501.001 (Certain Uses of Social Security Numbers Prohibited), §501.001 (Remedies), §501.052 (Privacy Policy Necessary to Require Disclosure of Social Security Numbers) the latter of which stipulates that the person providing the social security number be afforded a policy by the requestor indicating where the data will be stored, and how it will be protected, and §501.053 (Remedies). A copy of the statute is available at: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.501.htm

[xvii] See: http://www.uspto.gov/web/offices/pac/mpep/documents/0100_140.htm

[xviii] *See* 15 C.F.R. 742.15.

[xix] Eric Zelman, "Cloud Goes Boom, T-Mo Sidekick Users Lose All Data", InformationWeek, October 10, 2009 available at: http://www.informationweek.com/blog/main/archives/2009/10/cloud_goes_boom.html. *See also*, Rich Miller, "The Sidekick Failure and Cloud Culpability," Data Center Knowledge, October 12, 2009, available at: http://www.datacenterknowledge.com/archives/2009/10/12/the-sidekick-failure-and-cloud-culpability/. *But see*, Sam Johnson, "If it's dangerous it's NOT cloud computing" available at: http://samj.net/2009/10/if-its-dangerous-its-not-cloud.html (it's not the cloud that's bad, it was the components without sufficient redundancy that was the real culprit).

[xx] For an example of a cloud provider that went out of business during ongoing contracts, look at the story of Grok Cloud (http://www.grokthis.net/).

[xxi] Henry Newman, "Why Cloud Storage Use Could Be Limited in Enterprises" Enterprise Storage Forum, October 9, 2009, available at: http://www.enterprisestorageforum.com/technology/features/article.php/3843151

[xxii] Ronald Chichester, "The Collection Process: Collecting Evidence or Collecting Sanctions" at 1, AccessData White Paper (2009), available at: http://www.accessdata.com/downloads/media/Collecting_Evidence_or_Collecting_Sanctions.pdf

[xxiii] *Id*. "The duty to preserve evidence 'arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" *Acorn v. City of Nassau*, 2009 WL 605859 at 2 (E.D.N.Y. March 9, 2009) citing *Zubulake v. USB Warburg LLC* ("*Zubulake IV*"), 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (which itself quoted *Fujitsu Ltd. v. Federal Express Corp*., 247 F.3d 423, 426 (2d Cir. 2001). "Once the duty to preserve arises, a litigant is expected, at the very least, to 'suspend its routine document and retention/ destruction policy and to put in place a litigation hold.'" *Id*., citing *Zubulake IV*, 220 F.R.D. At 218; and see also *Doe v. Norwalk Cmty. Coll*., 2007 U.S. Dist LEXIS 51084, at *14 (D. Conn. July 16, 2007) (A party needs to take affirmative acts to prevent its systems from routinely destroying information).

[xxiv] Federal Rules of Civil Procedure ("FRCP") Rule 37 (Failure to Make Disclosures or to Cooperate in

Discovery; Sanctions), a copy of which is available at: http://www.law.cornell.edu/rules/frcp/Rule37.htm

[xxv] Chichester, supra, note 16 at 1, citing *Kipperman v. Onex Corp*., 2009 WL 1473708 (N.D. Ga. May 27, 2009) ($1,022,700.00 in monetary sanctions levied against the defendant for a "textbook case of discovery abuse.")

[xxvi] FRCP Rule 37(b)(2)(iii): "striking pleadings in whole or in part." *See, e.g., Channel Components, Inc. v. Am. II Electronics, Inc*., 915 So. 2D 1278 (Fla. Dist. Ct. App. 2005) (striking of the pleadings considered, but not imposed by the Court).

[xxvii] FRCP Rule 37(b)(2)(vi): "rendering a default judgment against the disobedient party." *See, e.g., Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y. Oct. 15, 2008) (Magistrate Judge recommended default judgment in favor of the plaintiff, plus attorney fees); *Atlantic Recording Corp. v. Howell*, 2008 WL 4080008 (D. Ariz. August 29, 2008) (default judgment warranted after "brazen destruction of evidence").

[xxviii] FRCP Rule 37(b)(2)(v): "dismissing the action or proceeding in whole or in part." *See, e.g., Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. February 13, 2009) (all of plaintiff's claims were dismissed, and an adverse instruction was awarded to the defendant's cross-claims after the plaintiff intentionally discarded her laptop in spite of a duty to preserve it.).

[xxix] *See, e.g., Smith v. Slifer Smith & Framption/Vail Assocs. Real Estate, LLC*, 20009 WL 482603 (D. Colo. February 25, 2009) (despite lack of evidence of a "smoking gun," the Court awarded an adverse inference against the defendant because some documents were destroyed well after the litigation hold notice was put in place.)

[xxx] *See, e.g., Easton Sports, Inc. v. Warrior LaCrosse, Inc*., 2006 WL 2811261 (E.D. Mich. Sept. 28, 2006) (adverse inference sanction awarded when defendant intentionally deactivated their cloud-based Yahoo! email account).

[xxxi] *See, e.g., Gippetti v. UPS, Inc.,* 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) (Court declined to impose sanctions because the conduct in question came under one of the safe harbor provisions).

[xxxii] Imaging, in computer forensic parlance, is the practice of making an exact duplicate (bit-for-bit) of a hard disk or a portion thereof, thereby preserving the electronic evidence. Imaging is an excellent way to prevent spoliation of the evidence, and to avoid subsequent sanctions by the court.

[xxxiii] John J. Barbara, "Cloud Computing: Another Digital Forensic Challenge" DFI News, October 27, 2009, available at:
http://www.dfinews.com/articles.php?pid=716
See also, Christine Taylor, "The Cloud and eDiscovery", NetworkComputing.com, July 30, 2009, available at: http://www.networkcomputing.com/e-discovery/the-cloud-and-ediscovery.php
For an cloud-industry spin on the topic, *see* Dan Morrill, "Cloud Computing Making Forensics Easier" Cloud Ave., September 22, 2008, available at:
http://www.cloudave.com/link/Cloud-computing-making-forensics-easier (Cloud computing makes forensics *easier* because you can backup key evidence files onto the cloud for preservation).

[xxxiv] Barbara, *supra*, note 27. For more information about virtual machines (which act as virtual servers), see:
http://en.wikipedia.org/wiki/Virtual_machine

[xxxv] Phillip Malone, "Social Networking Evidence: Sources, Authentication and Admissibility" H2O Playlist Bets, November 23, 2009, available at:
http://h2obeta.law.harvard.edu/315300

[xxxvi] FRCP Rule 26(f), the so-called "Meet & Confer" conference in which, under the amended Federal Rules, opposing counsel identify where data is stored, and any potential problems with the searching and production of that data. Several states have their own equivalents.

[xxxvii] For an excellent article that describes the basic network forensic process, see Nikkel, Bruce J. "Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence," Digital Investigation: The International Journal of Digital Forensics and Incident Response, Vol. 1, No. 4 (oid:10.1016/j.diin.2004.10.001) (August 1, 2005). A copy of the article is available at:
http://www.digitalforensics.ch/nikkel04.pdf

[xxxviii] Orin Kerr, "District Judge Concludes E-mail Not Protected by Fourth Amendment (But See Correction)" The Volokh Conspiracy, October 28, 2009, available at:
http://volokh.com/2009/10/28/district-judge-concludes-e-mail-not-protected-by-fourth-amendment/

[xxxix] http://www.facebook.com For an example of things to be concerned about if you or your employees use FaceBook, *see*, Jamie N. Nafziger and Kelcey Patrick-Ferree, "Don't just close your eyes and leap: top five issues in the Facebook terms of use" ACC Lexology, October 9, 2009, available at: http://www.lexology.com/, and James D. Heeney and Sharaf Sultan "Social networking: what employers need to know" ACC Lexology, October 14, 2009, also available at: http://www.lexology.com/

[xl] http://twitter.com

[xli] http://www.mayspace.com

[xlii] *See, e.g.*, "The pitfalls of Social Networking Websites," McLaughlin Investigative Group, available at: http://www.mclaughlinpi.com/blog/?p=25

[xliii] *See, e.g.,* Mandy Locke, "Police increasingly use Myspace-like sites as investigation tool" PoliceOne.com, July 16, 2007, available at: http://www.policeone.com/investigations/articles/1290064-Police-increasingly-use-Myspace-like-sites-as-investigation-tool/

[xliv] *See, e.g.,* "Social Networking Sites and Litigation," Adjunct Law Prof Blog, September 11, 2009, available at: http://lawprofessors.typepad.com/adjunctprofs/2009/09/social-networking-sites-and-litigation.html

[xlv] *See, e.g.,* "Why you need to know whether your jurors blog" on the blog *Deliberations*, November 12, 2008 available at: http://jurylaw.typepad.com/deliberations/voir_dire_questions/

[xlvi] The Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 (March 2009), available at: http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf. That opinion also cited: citing "Deception in Undercover Investigations: Conduct Based v. Status Based Ethical Analysis," 32 Seattle Univ. L. Rev.123 (2008), and "Ethical Responsibilities of Lawyers for Deception by Undercover Investigators and Discrimination Testers: An Analysis of the Provisions Prohibiting Misrepresentation under Model Rules of Professional Conduct," 8 Georgetown Journal of Legal Ethics 791 (Summer 1995).

[xlvii] The links and other materials are available at: http://www.law.berkeley.edu/institutes/bclt/socialnetworking/schedule.htm See specifically the audio recordings of "Problems Unique to Social Networking and the Law", "Does Overt Access to Social Networking Data Constitute Spying or Searching?", "Are You Really My Friend? The Law and Ethics of Covert or Deceptive Data-Gathering", "MyFace in Court: Admissibility and the Probative Value of Social Networking Evidence", "Regulating Crime in the Cloud: Policing Unlawful Behavior on Social Networks", and "Can Lawyers "Tweet" About Their Work? Confidentiality & Legal Professionalism in the Age of Social Media".