E-Discovery in the Cloud Era: What's a Litigant To Do?

by CINDY PHAM*

Introduction

There has been considerable growth in the adoption of cloud computing in the past few years, with this trend forecasted to continue. In 2008, the total cloud service revenue was $46.4 billion, rising to $58.6 billion by 2009.[1] This amount further increased to $68.3 billion in 2010.[2] By 2014, the market is expected to be worth $148.8 billion and it is predicted that people will process more than 50 percent of all computing workloads through cloud computing.[3] Furthermore, it is estimated that, by 2015, cloud usage will grow twelve-fold to represent one-third of Internet traffic.[4] The exponential growth in cloud computing can be attributed to the fact that cloud computing substantially minimizes information technology (IT) costs, does not require management by the user, can be scaled to

* University of Denver Sturm College of Law, J.D. expected, 2013; University of Texas at Austin, B.A. in English, Minor in Business Administration. The author would like to thank Professor David Thomson for his insight and guidance during the development of this Article.

1. *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010*, GARTNER (June 22, 2010), http://www.gartner.com/it/page.jsp?id=1389313; *Gartner Says Worldwide Cloud Services Revenue Will Grow 21.3 Percent in 2009*, GARTNER (Mar. 26, 2009), http://www.gartner.com/it/page.jsp?id=920712.

2. *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010*, *supra* note 1.

3. *Id.*; CISCO, CISCO GLOBAL CLOUD INDEX: FORECAST AND METHODOLOGY, 2010–2015 17 (2011) [hereinafter CISCO WHITE PAPER], *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf.

4. CISCO WHITE PAPER, *supra* note 3, at 6–7 ; *see also The State of Adoption of Cloud Applications*, TATA CONSULTING SERVICES, http://sites.tcs.com/cloudstudy/the-state-of-adoption-of-cloud-applications#.T9gXHStYvlX (last visited July 12, 2012) (predicting American cloud use will increase from 19 percent to 34 percent by 2015).

individual needs, and provides instant mobile access.[5] Most significant, cloud users need only pay for what they use.[6]

However, while there are many benefits to cloud computing, a company using a cloud may find itself mired in complications during the discovery phase of a lawsuit. The cloud expands a company's data sources to seemingly limitless amounts.[7] This presents preservation and production problems because, under Rule 34 of the Federal Rules of Civil Procedure (FRCP), litigants are required to identify, preserve, and collect electronically stored information (ESI) stored in the cloud.[8] If the company does not know how to search for, preserve, and collect the requested information, it may be subject to sanctions.[9] This duty is further complicated because companies often do not know how their cloud operates[10] and because data stored in the

5. Seamus Bellamy, *Is Cloud Computing for You? Five Points to Consider*, PCWORLD (Nov. 29, 2011, 1:00 PM), http://www.pcworld.com/businesscenter/article/245137/is_cloud_computing_for_you_five_points_to_consider.html; *see also* CSC, CSC CLOUD USAGE INDEX 1 (2011), *available at* http://assets1.csc.com/newsroom/downloads/CSC_Cloud_Usage_Index_Report.pdf ("[O]ne-third of respondents cite their need to better connect employees who use a multitude of computing devices as the number one reason they adopt cloud. Seventeen percent cite accelerating the speed of business, while 10 percent say cutting costs is the top reason for cloud adoption.").

6. PETER MELL & TIMOTHY GRACE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011) [hereinafter NIST DEFINITION], *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

7. *See* UNIVERSITY LEADERSHIP COUNCIL, REDEFINING THE ACADEMIC LIBRARY: MANAGING THE MIGRATION TO DIGITAL INFORMATION SERVICES 14 (2011) (internal citations and quotations omitted), *available at* http://www.theconferencecircuit.com/wp-content/uploads/Provosts-Report-on-Academic-Libraries2.pdf ("The prospect of mounting a book digitization project at the scale of Google's never seemed within the capabilities of research libraries until an outside partner with seemingly limitless resources emerged.").

8. FED. R. CIV. P. 34(b)(2)(E) ("Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information: (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request . . .").

9. *Id.* at 37(b)(2)(A), (c)(1). *See also* Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007) (citing Millsap v. McDonnell Douglas Corp., 162 F. Supp. 2d 1262, 1309 (N.D. Okla. 2001) ("The court has inherent power to impose sanctions for the destruction or loss of evidence."); Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 631 (D. Utah 1998)).

10. *See* VARONIS, CLOUD COLLABORATION IN THE ENTERPRISE: RESEARCH REPORT 4–5, 7–8, 11 (2012), *available at* http://www.varonis.com/assets/reports/en/cloud-collaboration-in-the-enterprise-en.pdf (reporting 27 percent of companies utilizing cloud technology did not know how secure their cloud was, 9 percent did not know whether their company provided employees with a corporate account for cloud services, 16 percent did not know whether their employees stored company data with other third-party cloud providers, 20 percent did not know what percent of company data was actually stored in cloud servers, and 70 percent did not know where their cloud providers stored company

cloud is dynamic and rapidly changing, making it harder to locate and preserve.[11]

Litigants may find themselves liable for data loss when they encounter problems gaining access to analyze potentially relevant data stored on a third-party cloud server and difficulties preserving and retrieving data. Litigants may also find themselves in a situation where the court has issued a subpoena to the cloud provider ordering production of the litigant's information, without the litigant's consent, review, or even knowledge. To prevent such problems, companies should be familiar with how their cloud operates and is maintained, work with their cloud provider to develop a litigation plan, and meet and confer with opposing counsel as soon as possible to limit the potential vast scope of cloud-based e-discovery.

Part I of this article provides an overview of how cloud technology works. Part II details e-discovery problems that arise from the use of cloud-based services by clients and lawyers. Part III provides practical guidelines for attorneys and their clients to follow before and during litigation.

I. What is Cloud Computing?

To best serve the needs of clients, attorneys must fully understand how cloud computing differs from other document storage methods and how cloud computing works. Cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing

data); Tam Harbert, *E-Discovery in the Cloud? Not so Easy*, COMPUTERWORLD (April 23, 2012, 6:00 AM), http://www.computerworld.com/s/article/9226375/E_discovery_in_the_Cloud?taxonomyId=19&pageNumber=2 ("[N]early 60% of more than 100 Fortune 2000 enterprises and government agencies said they felt that their cloud-based applications could potentially be subject to e-discovery. In the same survey, however, only 26% of the respondents said they considered themselves somewhat or very prepared for e-discovery requests."); Connie Martin, *For Corporations, Knowing Where Their Data is Stored is the First Step in Keeping the Costs of Electronic Discovery Under Control*, ADVANTAGE COMPANIES (March 5, 2012, 2:57 PM), http://www.advantage-companies.com/blog/conniemartin/2012/03/05/corporations-knowing-where-their-data-stored-first-step-keeping-costs ("We've just recently completed collection on a case where data turned up in locations top management wasn't even aware existed . . . resulting in costs that the GC was unhappy about and unprepared for."). *See also* Press Release, NPD Grp., Consumers Don't Know What "Cloud Computing" Is, Even Though They Use it All the Time (Aug. 9, 2011), https://www.npd.com/press/releases/press_110809.html (Surveying almost 2000 U.S. consumers and reporting 76 percent used some type of cloud-based technology but only 22 percent were familiar with the term "cloud computing.").

11. Thomas Lidbury & Michael Boland, *Technology: e-Discovery in the Cloud*, INSIDE COUNSEL (April 27, 2012), http://www.insidecounsel.com/2012/04/27/technology-e-discovery-in-the-cloud.

resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[12] The National Institute of Science and Technology published this technical definition in 2011, after fifteen drafts and two years of work, and it successfully personifies the nature of cloud computing: fast, easy, and cost-efficient.[13] Simply put, cloud computing is an Internet-based service which provides users access to software, resources, and information stored elsewhere and managed by someone else, anytime and anywhere. In its simplest form, it is a hard drive on the Internet that someone else manages.

With cloud computing, a user's personal computer is not actually doing the heavy lifting. Rather, the user's personal computer acts as a portal to separate computers elsewhere that are shouldering the processing and data storage burden.[14] The user's computer merely has to run the web browsing software required to open the cloud "door" and view the results.[15]

As of 2011, approximately 86 percent of businesses were beginning to or already using cloud technology.[16] Cloud computing has not been limited to companies either. Approximately 65 percent of American law firms use some form of cloud computing, such as for litigation support, data storage, billing, or payroll.[17] The federal

12. NIST DEFINITION, *supra* note 6.

13. Press Release, Evelyn Brown, Nat'l Inst. of Standards & Tech., Final Version of NIST Cloud Computing Definition Published (Oct. 25, 2011), http://www.nist.gov/itl/csd/cloud-102511.cfm.

14. The Sedona Conference, Commentary on Cloud Computing 2 (2011) [hereinafter Sedona Commentary] (working paper), *available at* https://thesedonaconference.org/%5Bfield_event_node_ref-path%5D/meeting-paper/chapter-7-sedona-conference%C2%AE-commentary-cloud-computing.

15. *Id.*

16. CIO LINKEDIN, DO YOU HAVE AN ENTERPRISE-WIDE CLOUD STRATEGY? 1 (2011), *available at* http://www.bluechiptek.com/files/whitepapers/GeneralDataCenter/wp-cio-enterprise-wide-cloud-strategy.pdf; *see also* KPMG, CLARITY IN THE CLOUD 2 (2011), *available at* http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cloud-clarity.pdf ("81% of businesses are either planning their initial forays, are in early or advanced stages of experimentation or have full implementations.").

17. *Law Firm Technology 2011: Head for the Cloud?*, AMERICAN LAWYER, http://www.americanlawyer.com/PubArticleTAL.jsp?id=1202520215210&Law_Firm_Technology_2011_Head_for_the_Cloud (last visited July 12, 2012); *see also* Alan Cohen, *Drawing The Line: How Much Data Access is too Much? Security Concerns Take Center Stage in Our Annual Technology Survey*, AMERICAN LAWYER (Nov. 1, 2011), http://www.americanlawyer.com/PubArticleTAL.jsp?id=1202519591934 ("Continuing cost pressure is among the factors leading firms to explore cloud-based technologies-applications that run on a vendor's infrastructure and that are located far off-site. . . . Nearly two-thirds of firms (63 percent) report using some type of cloud-based solution.").

government has also started taking advantage of the benefits of cloud computing. In 2010, governmental agencies began moving their servers into the cloud.[18] By May 2012, the Federal government began implementing the Digital Government Strategy, a twelve-month action plan to move its major data systems to the cloud.[19]

While the cloud has attracted significant media attention recently, most people have been cloud computing for many years. People have been using web-based email, such as Hotmail, since the mid-1990s,[20] and have been storing and sharing photos online since the early 2000s.[21] When people access an email or a photo-storage website, they are cloud computing. Even though the information is displayed on their computer screens, any user commands will be processed elsewhere by another computer system.[22]

A. Distinguishing the Cloud from Other Data Storage

Before the cloud, there was the data center. And before the data center, there was peer-to-peer sharing. From 2000 to 2008, peer-to-peer data sharing, in which information was exchanged directly

18. Press Release, Steve Hoffman, U.S. Gen. Servs. Admin., GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide (December 1, 2010), http://www.gsa.gov/portal/content/208417; Press Release, U.S. Dep't of Agric., USDA Moves to the Microsoft Cloud (December 8, 2010), http://www.usda.gov/wps/portal/usda/usdahome?contentidonly=true&contentid=2010/12/0638.xml.

19. CHIEF INFO. OFFICERS, DIGITAL GOVERNMENT: BUILDING A 21ST CENTURY PLATFORM TO BETTER SERVE THE AMERICAN PEOPLE 1 (May 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf; Press Release, Chief Info. Officers, Creating a Future-ready, Digital Government Today (June 20, 2012), http://cio.gov/creating-a-future-ready-digital-government-today.

20. Hotmail was established in July 4, 1996, and had a reported 8.5 million users by December 1997. Dick Craddock, *A Short History of Hotmail*, THE WINDOWS BLOG (Jan. 5, 2010), http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/01/06/a-short-history-of-hotmail.aspx; Jeff Pelline, *Hotmail, Microsoft Talk Deals*, CNET (Dec. 5, 1997, 11:00 AM), http://news.cnet.com/2100-1023-206039.html.

21. Jennifer Van Grove, *The Mobile Photo Sharing Boom is Here*, CNN (Dec. 6, 2010, 8:02 AM), http://www.cnn.com/2010/TECH/mobile/12/06/photo.sharing.boom.mashable/index.html ("In the early and mid 2000s there was a measurable boom in online photo sharing services. That boom brought us Flickr, Picasa, Photobucket, ImageShack and dozens more."). *See also, e.g.*, Jefferson Graham, Photobucket Snaps a Portrait of Success, USA Today (May 2, 2007, 9:55 PM), http://www.usatoday.com/tech/products/2007-05-01-photobucket_N.htm (discussing Photobucket's debut in 2003); Dana Mattioli, Shutterfly to Snap Up Kodak Site, Wall Street Journal (last updated April 25, 2012, 2:10 PM), http://online.wsj.com/article/SB10001424052702303592404577364271258571262.html ("Kodak Gallery grew out of Ofoto, which Kodak acquired for less than $100 million in 2001.")

22. Sedona Commentary, *supra* note 14.

between Internet users, was the main source of Internet traffic.[23] In 2008, data center use began to dominate Internet traffic.[24] A data center is composed of information stored at a location with large, dedicated clusters of computers, which are hosted and operated internally by a single organization.[25] Data centers are based on the locality of a specific physical place where the user houses their computer servers.[26] Traditionally a company owns its own data center or leases a data-center ready space upon which to construct their data center.[27] Regardless of whether a company owns or leases, the company fully owns, controls, and manages the hardware in a traditional data center.[28]

Clouds, on the other hand, consist of a third party who charges clients for online access to their third-party-owned data centers, which will host the client's information. With the cloud, a client can simply outsource their information and does not have to manage the data center or even know where it is located.[29] Hence, the name "cloud" and the idea that the data is just floating out there somewhere.[30] To think of it another way, data centers are a product one purchases while clouds are a service one hires.

---

23. CISCO WHITE PAPER, *supra* note 3, at 2.

24. *Id.*

25. THEOPHILUS BENSON, ADITYA AKELLA & DAVID MALTZ, NETWORK TRAFFIC CHARACTERISTICS OF DATA CENTERS IN THE WILD 1 (2010), *available at* http://pages.cs.wisc.edu/~tbenson/papers/imc192.pdf.

26. Randy Bias, *Clouds Are Not Datacenters*, CLOUDSCALING (Oct. 8, 2008), http://www.cloudscaling.com/blog/cloud-computing/clouds-are-not-datacenters/

27. Renting data center-ready space is called colocation; also known as a wholesale data center, outsourced data center, and off-site computer room facilities. Colocation is essentially an empty computer room, ready for a leaser's network equipment, hardware, disk storage, software and connectivity to form a data center. The colocation center merely owns the building and is responsible for maintaining power, cooling, fire suppression and center security. Doug Theis, *Data Centers are Going Green*, LIFELINE DATA CENTERS (June 29, 2012), http://www.lifelinedatacenters.com/category/colocation-compliance/; Doug Theis, *What's the Difference Between Cloud Computing and Collocation?*, LIFELINE DATA CENTERS (Sept. 22, 2011), http://www.lifelinedata centers.com/data-center/whats-the-difference-between-cloud-computing-and-colocation/.

28. Theis, *What's the Difference Between Cloud Computing and Collocation?*, *supra* note 27.

29. Bias, *supra* note 26.

30. A blogger eloquently explained the concept of cloud computing in an attempted haiku:

Out there. Somewhere.

In the clouds. You don't know.

You don't care.

Id.

Currently, traditional data center use continues to grow and dominate Internet traffic, while cloud use is expanding at a highly exponential rate.[31] Though we will likely see a shift towards a cloud-dominated Internet, traditional data centers and clouds are different commodities with different amenities; hence, both models are likely to be used in the future.

B. Technical Aspects of the Cloud

There is a misconception that all cloud computing use is the same. In actuality, there are many different modes of cloud computing, which are varied combinations of 1) how the cloud service is provided and 2) how the cloud service is deployed.[32] For example, a Gmail user's cloud computing infrastructure consists of a fully managed, online webmail application (the service model), which is deployed on a public cloud shared with other Gmail users (the deployment model).[33]

1. The Service Model

Currently, there are three main tiers of cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[34] With all these service models, the

31. CISCO WHITE PAPER, *supra* note 3, at 2, 6–7; s*ee also The State of Adoption of Cloud Applications*, *supra* note 4.

32. *See* NIST DEFINITION, *supra* note 6; Lee Badger et al., Nat'l Inst. of Standards & Tech., *Cloud Computing Synopsis and Recommendations* ES-1 [hereinafter *NIST Draft Synopsis and Recommendations*] (Nat'l Inst. of Standards & Tech., Special Draft Publication No. 800-146), *available at* http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf; Sedona Commentary, *supra* note 14, at 7.

33. *See Gmail*, GOOGLE, http://mail.google.com (last visited July 25, 2012); *Google Privacy Policy*, GOOGLE, https://www.google.com/intl/en/policies/privacy/ (last visited July 25, 2012). *See also* EVERETT DAVIAGE & JEFF BARTLETT, VALIANT SOLUTIONS, IMPLEMENTING GOOGLE APPS 8 (2011), *available at* http://www.valiantsolutions.com/Google_Apps_White_Paper_UMD.pdf ("Google offers some of the best known [public] cloud computing services available with their Google Apps Suite, including Gmail, Google Docs, Google Calendar, and Picasa.").

34. *See* NIST DEFINITION, *supra* note 6, at 2–3. As technology advances and cloud computing use continues to increase, need for other service models also continues to grow. To meet client demands, some cloud providers now offer Computing as a Service, a blend of their other service models. In addition, in April 2011, Cisco submitted a proposal for a new service model: Networking as a Service. Dave Rosenberg, *Cisco Throws Networking into OpenStack Cloud*, CNET (April 10, 2011, 10:44 AM), http://news.cnet.com/8301-13846_3-20052564-62.html; Laura Smith, *The Lines Between Cloud Computing Models Are Blurring*, SEARCHCIO (Feb. 9, 2011), http://searchcio.techtarget.com/news/2240031934/The-lines-between-cloud-computing-models-are-blurring. *See also* Press Release, Hewlett-Packard, HP Expands Converged Cloud Portfolio (June 5, 2012), http://www8.hp.com/lamerica_nsc_carib/en/hp-news/press-release.html?id=1247993.

client accesses the cloud through a web browser and the computer is mostly being used as a monitor, with the cloud running all the applications. However, the models vary due to the level of control clients are able to exert over the cloud and outsourced data.

The Software as a Service (SaaS) model is the most general and simplest service model as users just pay for access to the cloud provider's existing applications in the cloud.[35] With the SaaS service model, the client has little to no control or management over the cloud's infrastructure, such as the cloud provider's network, servers, operating systems, storage, or applications.[36] This means the client cannot control how data is stored and altered within the cloud. The client is merely using a completely preassembled and configured service. An example of this model is web-based email, such as Gmail.[37] The server and e-mail management software are all located in the cloud and managed by Google, the cloud service provider.[38] Other examples of popular SaaS models include Netflix and Amazon's Kindle Cloud Reader.[39] Examples of law firm SaaS use involve web-based time and billing software, and online legal research databases, such as LexisNexis and Westlaw.[40]

With the Platform as a Service (PaaS) model, clients have slightly more control over cloud computing. The PaaS model gives clients the ability to install, configure, and customize their own software applications in the cloud.[41] Clients also have the ability to create new applications in this cloud model using their cloud provider's tools and

35. *See* NIST DEFINITION, *supra* note 6.

36. *Id.*

37. Sedona Commentary, *supra* note 14.

38. CHRISTINE SOARES, FOX ROTHSCHILD LLP, APPLYING E-DISCOVERY BEST PRACTICES TO CLOUD COMPUTING 2 (2012), *available at* http://www.jdsupra.com/post/documentViewer.aspx?fid=6dfdb5f5-cdee-4dbc-b028-4086050d4bca.

39. See *Company Overview*, NETFLIX, https://account.netflix.com/MediaCenter/Overview (last visited July 15, 2012); *Kindle Cloud Reader*, AMAZON, https://read.amazon.com/about (last visited July 15, 2012).

40. *See, e.g.*, *About LexisNexis*, LEXISNEXIS, http://www.lexisnexis.com/en-us/about-us/about-us.page (last visited July 15, 2012); *Know the Difference*, WESTLAWNEXT, http://store.westlaw.com/westlawnext/about/default.aspx (last visited July 15, 2012); CLIO, http://www.goclio.com/ (last visited July 15, 2012).

41. Lee Badger et al., Nat'l Inst. of Standards & Tech., *US Government Cloud Computing Technology Roadmap Volume II Release 1.0: Useful Information for Cloud Adopters* 17, 20 [hereinafter *NIST Cloud Computing Technology Roadmap*] (Nat'l Inst. of Standards & Tech., Special Publication No. 500-293), *available at* http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf.

programming language.[42] Basically, clients have remote access to their own applications, rather than to a Cloud provider's pre-assembled and configured applications. However, under this model, the client still has little to no control or management over the cloud provider's network, servers, operating systems, or storage.[43] Similarly, the client has no control over how data is stored and altered within the cloud. Major PaaS providers include JoyentCloud, Force.com, Google App Engine, and Microsoft Azure.[44] Examples of PaaS users include Voxer, which stores their downloadable smart phone walkie-talkie application on JoyentCloud,[45] and law firms that create smart phone applications that allow potential clients to easily contact the firm.[46]

Of all the service models, the Infrastructure as a Service (IaaS) model offers clients the most control over their data. This type of service is also the most similar to the traditional data center approach to data storage. With the IaaS model, clients rent access to the cloud provider's underlying cloud infrastructure, such as the cloud provider's network, servers, security, hardware, and storage and may integrate its own customized operating system and software onto this

42. *Id. See also Features*, WINDOWS AZURE, http://www.windowsazure.com/en-us/home/features/overview/ (last visited July 16, 2012) (providing tools to create applications that then run on Microsoft's PaaS Azure cloud).

43. *NIST Cloud Computing Technology Roadmap*, *supra* note 41, at 20.

44. *See Customers*, JOYENTCLOUD, http://www.joyentcloud.com/customers/ (last visited July 15, 2012); *Showcase*, GOOGLE DEVELOPERS, https://developers.google.com/showcase/ (last visited July 15, 2012); *Why Force.com?*, FORCE.COM, http://www.force.com/why-force.jsp (last visited July 15, 2012); *Windows Azure Case Studies*, WINDOWS AZURE, http://www.windowsazure.com/en-us/home/case-studies/ (last visited July 15, 2012).

45. *Voxer*, JOYENTCLOUD, http://www.joyentcloud.com/customers/voxer/ (last visited July 15, 2012).

46. Need a lawyer? "There's an app for that." Brian X. Chen, *Apple Registers Trademark for 'There's an App for That'*, WIRED MAGAZINE, http://www.wired.com/gadgetlab/2010/10/app-for-that/ (Oct. 11, 2010, 2:38 PM). *See, e.g.*, *The Auto Injury App*, AARON SACHS & ASSOCS., https://play.google.com/store/apps/details?id=com.tseg.androidaaronsachsautoinjury&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS50c2VnLmFuZHJvaWQuYWFyb25zYWNoc2F1dG9pbmp1cnkiXQ (last visited July 15, 2012) (creating an application with an accident checklist, a daily injury journal, an accident form with the ability to attach camera pictures or video recordings from the scene of the incident, an option to request a police report, and a legal glossary); *Kevin Kurgis Law Firm App*, KEVIN KURGIS LAW FIRM, https://play.google.com/store/apps/details?id=com.tseg.android.kurgis&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS50c2VnLmFuZHJvaWQua3VyZ2lzIl0 (last visited July 15, 2012) (creating an application that has a nearest hospital locator, a lost wage calculator, medical expense tracking log, an accident form with the option to attach pictures taken with the user's camera phone, and the "[c]ontact and location information to a law firm that specializes in personal injury cases.").

base.[47] Under this model, the cloud provider manages and has complete control over the cloud infrastructure, but the client has complete control of the operating system and software.[48] The client may also be able to customize the network services, depending on the cloud provider.[49] Most importantly, while the cloud provider may relocate data from one physical location in the cloud to another to maximize cloud efficiency,[50] the client has control and direct access to the cloud's storage and database servers.[51] In sum, the cloud provider is responsible for housing and running the cloud base, and the client is responsible for maintaining, operating, updating, and configuring the operating system that makes the cloud work.[52] And since cloud providers only bill clients for what they use, the IaaS service model essentially provides companies with an inexpensive version of the traditional data center alongside most of the benefits to cloud computing, such as scalability.

Companies sometimes choose to utilize an IaaS cloud model when they have a project requiring a lot of computer processing power with a quick turnaround. For example, 45 minutes after Hillary Clinton's 1993-2001 schedule became publically available as a non-searchable PDF, the Washington Post employed Amazon's IaaS cloud, the Amazon Elastic Compute Cloud (Amazon EC2) to convert the PDF into a searchable online library.[53] Using the IaaS cloud's 200

47. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 2–2, 7–2. The client also has the option of using the cloud provider's own operating system, but will be responsible for managing it. Wely Lau, *A Developer's Perspective on IaaS vs. PaaS*, CLOUD ZONE (May 11, 2012), http://cloud.dzone.com/articles/developers-perspective-iaas-vs.

48. *NIST Draft Synopsis and Recommendations*, *supra* note 32. However, where the client is using a provider's preloaded operating system, the client does not have control over the lower level of the operating system that sustains the cloud infrastructure and provides virtualization, known as the hypervisor. *Id.*; *NIST Cloud Computing Technology Roadmap*, *supra* note 42, at 21.

49. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 2–2, 7–2.

50. *Id.* at 4–2 ("[M]igration of customer workloads (data storage and processing) from one physical computer to another physical computer . . . is a key strategy that allows a provider to refresh hardware or consolidate workloads without inconveniencing subscribers.").

51. *See Id.* at 7–5; BYRON LUDWIG & SERENA COETZEE, A COMPARISON OF PLATFORM AS A SERVICE (PAAS) CLOUDS WITH A DETAILED REFERENCE TO SECURITY AND GEOPROCESSING SERVICES 3 (2010), *available at* http://www.isprs.org/proceedings/XXXVIII/4-W13/ID_57.pdf.

52. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 7–2.

53. *AWS Case Study: Washington Post*, AMAZON WEB SERVICES, http://aws.amazon.com/solutions/case-studies/washington-post/ (last visited July 15, 2012). *See also*

server instances and with a processing speed of approximately 60 seconds per page, the Washington Post was able to convert the 17,481 pages of non-searchable PDF images to a searchable document within nine hours and provide web portal access to the public 26 hours later.[54] The IaaS cloud allowed them to do, in 26 hours, what would have taken hundreds of hours and only at the cost of $144.62.[55] Another example of IaaS cloud use is Condé Nast Digital Germany, which publishes the German-language editions of *Vogue*, *Glamour*, and *GQ*.[56] The company moved their online magazine websites to GoGrid's IaaS cloud to inexpensively support their heavy volume of online traffic, to store the large quantities of videos and pictures available to the public on their websites, and to provide servers for developer testing.[57]

Although an IaaS cloud model would make discovery during litigation much easier, since the cloud user has greater control over the data in that environment, it is not always the best solution for companies in their normal course of business. The IaaS model requires time to implement, technical knowledge to deploy software applications in the cloud, and IT staff to vigilantly secure, maintain, and update the cloud's operating system. For businesses that may not have these resources or the need to develop their own applications or cloud operating system, a SaaS cloud model would be most efficient. SaaS is easily implemented to provide quick access to a pre-configured application, already suitable for business needs, and the user would not have to manage or worry about the cloud. The SaaS cloud model is also more convenient for companies that only need cloud access for limited purposes, such as virtual access to pre-customized sales forecasting,[58] financial reporting,[59] or case

Clinton's Schedule: Hillary Clinton's Activities as First Lady, 1993-2001, WASHINGTON POST, http://projects.washingtonpost.com/2008/clinton-schedule/ (last visited July 15, 2012).

54. *AWS Case Study: Washington Post*, *supra* note 53.

55. *Id.*

56. VOGUE, http://www.vogue.de/ (last visited July 15, 2012).

57. *Case Study: Top Magazines Lower TCO*, GOGRID (internal citations and quotations omitted), http://www.gogrid.com/cloud-hosting/case-studies/conde-nast-digital-lowers-tco (last visited July 15, 2012) ("With GoGrid, I can add server capacity in about 20 minutes, use it for a few days, and turn it off. So we're not locked into paying for a whole month of service we only need for a day or two."); *see also Vogue Videos*, VOGUE, http://www.vogue.de/videos (last visited July 15, 2012).

58. *See, e.g.*, *Cloud9 Products*, CLOUD9, http://www.cloud9analytics.com/products (last visited July 15, 2012).

59. For example, Groupon uses Host Analytics' SaaS cloud service for their global financial reporting. With its rapidly growing customer base, Groupon chose a SaaS service model because it needed an immediate method of consolidating its international financial

management software.[60] However, the SaaS model may not be suitable when a company already has a preexisting application that fulfills the organization's needs or wants to create or customize their own application—the PaaS model would be better in such situations.[61]

Where a company desires control over an application, a PaaS model would be preferable if the company does not have the tools to build their own application or simply does not wish to manage more than the application. With a PaaS model, a user also does not have to worry about maintaining or protecting the cloud operating system. However, developing an application in a PaaS model with a cloud provider's tools may create proprietary restrictions that prohibit transfer of the application to another cloud provider.[62] If an organization has the resources and does not wish to bind their application to the cloud provider, it should then seek an IaaS model to provide the desired mobility.[63]

Furthermore, cloud computing does not have to be exclusive to any one of the cloud models. In a 2011 study, surveying 3,200 companies, 86 percent stated they used multiple cloud services.[64] A

data quickly, at a low cost, and without relying on in-house IT resources, which Groupon lacked. *Customer Case Study*, HOST ANALYTICS, http://www.hostanalytics.com/sites/default/files/case-studies/Host-Analytics-Case-Study-Groupon.pdf (last visited July 15, 2012). *See also* BEN KEPES, UNDERSTANDING THE CLOUD COMPUTING STACK SAAS, PAAS, IAAS 6 (2011), *available at* http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf (discussing how an SaaS model would be sensible "where demand spikes significantly, for example tax or billing software used once a month").

60. Law firms such as Mcdermott Will & Emery and Kirkland & Ellis LLP, as well as in house counsel for Hyundai, Morgan Stanley, Verizon, ExxonMobile, and Level 3 Communications utilize Nextpoint's case management software. *Who's Using It?*, NEXTPOINT, http://trialmanager.com/who_uses_it.html (last visited Oct. 21, 2012).

61. KEPES, *supra* note 59, at 10.

62. For example, Force.com, a PaaS provider, reserves proprietary interest in applications developed with their tools, preventing a user from transferring the application outside the force.com platform. *See* Master Subscription Agreement Developer Services, Salesforce.com, *available at* http://www.salesforce.com/assets/pdf/misc/salesforce_Developer_MSA.pdf (last visited July 18, 2012) ("UPON ANY TERMINATION OF THIS AGREEMENT, ALL APPLICATIONS AND OTHER MATERIALS DEVELOPED BY YOU USING THE DEVELOPER SERVICES AND HOSTED ON OUR PLATFORM WILL BE PERMANENTLY LOST.").

63. Since IaaS users have control over the cloud's operating system and software, any developer tools they use to create applications are their own.

64. Meghan Kelly, *86 Percent of Companies Use Multiple Cloud Services, Says Study*, VENTUREBEAT (May 10, 2012, 12:44 PM), http://venturebeat.com/2012/05/10/cloud-services-data/ (relying on Cloudability's 2011 customer study). *See also* TECH TRENDS 2012: ELEVATE IT FOR DIGITAL BUSINESS, DELOITTE 29 (2012), *available at* http://www.deloitte.com/view/en_US/us/Services/consulting/technology-consulting/technology-2012/index.htm.

company may choose to do so for an assortment of projects or needs.[65] For example, a company may use a SaaS model to handle company finances, but utilize a PaaS model for specific projects, such as managing company–developed applications.[66] However, regardless of the cloud model, each of the three cloud models have their own benefits, so which one a company chooses to employ depends on the needs and resources of the organization, rather than just data control considerations. In summary, there is no "right" cloud model.

2. The Deployment Model

Once clients decide on a service model that best fits their needs, they must choose a deployment model, which determines the cloud environment and how the chosen service model is provided to the user.[67] The deployment model basically describes where the data is located and who has access to it.[68] Currently, there are four types of deployment models: 1) the private cloud; 2) the community cloud; 3) the public cloud; and 4) the hybrid cloud.

Within the private cloud deployment model, the chosen cloud service is operated exclusively for one organization, and managed by

("Along the way, leading organizations moved from cautious exploration to the reality of multiple individual cloud offerings handling critical pieces of their business operations-and sourced from multiple public and private providers.") (calling this "hyper-hybrid" cloud use); Press Release, RightScale, *RightScale Sees Multi-Cloud Use on the Rise* (Mar. 27, 2012), *available at* http://www.rightscale.com/news_events/press_releases/2012/rightscale-sees-multi-cloud-use-on-the-rise.php (finding "87 percent of compute power managed through the RightScale platform comes from companies that utilize multiple clouds.")

65. *See* Joe McKendrick, *Time to Focus on 'Services,' Not 'Cloud': Deloitte*, FORBES, (Feb. 15, 2012, 12:05 PM), http://www.forbes.com/sites/joemckendrick/2012/02/15/time-to-focus-on-services-not-cloud-deloitte/ ("Instead of relying on one type of cloud model or another, companies are adopting a range of services, originating from outside the firewall, from third-party providers, and from their own IT departments. They seek the security, control, and differentiation their own IT provides. They want the flexibility and incremental cost model outside cloud services offer. They want it all.").

66. The cosmetic company Avon uses Salesforce.com's SaaS Sales Cloud for their finance needs and also uses Salesforce.com's PaaS cloud, Force.com, to develop and manage its leadership management application. *Avon*, SALESFORCE.COM, http://www.salesforce.com/customers/stories/avon.jsp (last visited July 19, 2012). See also *Caesars Entertainment Hits the Efficiency Jackpot with Force.com*, SALESFORCE.COM, http://www.salesforce.com/showcase/stories/caesars.jsp (last visited July 19, 2012) (detailing Caesars Entertainment's use of Force.com's PaaS platform to build applications such as custom application for room reservations, and use of Salesforce.com's SaaS Chatter cloud for social networking among their employees).

67. *NIST Cloud Computing Technology Roadmap*, *supra* note 41, at 17.

68. Sedona Commentary, *supra* note 14, at 9.

the organization or a third party.[69] If the cloud is self-managed, there is no third-party cloud provider. This cloud fully belongs to the organization, which must build, run, and maintain the entire cloud infrastructure behind the organization's own firewalls.[70] In a third-party-hosted private cloud,[71] there is a cloud provider that implements the cloud service on a nonshared infrastructure, behind the cloud provider's organization-dedicated firewalls.[72] The organization does not have to build or maintain the infrastructure, and has the ability to manage the firewall and has full control of who has access to it.[73] This deployment model offers the most security, privacy, and client control, but also is the most expensive to implement and more appropriate for a larger company with the resources and need.[74] In addition, a cloud provider may not offer private cloud deployment for certain service models.[75]

Under the public cloud deployment model, the cloud service is open to the general public and the cloud service provider has full ownership and control.[76] In a public cloud, client data may reside on

69. *See* NIST DEFINITION, *supra* note 6, at 3.

70. GOGRID, SKYDIVING THROUGH THE CLOUDS 8–9 (2011), *available at* http://www.lunariconsulting.com/uploads/GoGrid_Skydiving_through_the_Clouds.pdf.

71. Also referred to as an outsourced private cloud. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 4–2.

72. *Id.* at 9; *Private Cloud Hosting*, ONLINE TECH, http://www.onlinetech.com/cloud-computing-hosting/packages/private-cloud (last visited July 19, 2012) (providing private cloud deployment models with dedicated firewalls).

73. NICOLE BLACK, CLOUD COMPUTING FOR LAWYERS 159 (2012); Jason Yaeger, *Private Cloud Security: How Your Data Security Changes in the Cloud*, ONLINE TECH, http://www.onlinetech.com/resources/wiki/cloud-computing/private-cloud-security-how-your-data-security-changes-in-the-cloud (last visited July 19, 2012); *see also, e.g.*, *Build Your Own Private Cloud with IBM SmartCloud Foundation*, IBM, http://www.ibm.com/cloud-computing/us/en/private-cloud.html (last visited July 19, 2012).

74. For example, to set up and use a hosted private cloud, one cloud provider's setup prices range from $1,273 to $4,479 and monthly fee charges range from $2,612 to $8,534. For its public cloud, this same company does not charge a set up fee and monthly changes range from $99 to $529. PAY PER CLOUD, http://www.paypercloud.com/cloud-hosting.aspx (last visited July 19, 2012).

75. *See* BLACK, *supra* note 73 ("The vast majority of cloud-computing products offered to law firms are public clouds…"); *Google Privacy Policy*, *supra* note 33 (offering only a public deployment method for its Google cloud services in which customer data is intermingled with other users); *Store.Westlaw.com Online Privacy Statement*, WESTLAW, http://store.westlaw.com/about/privacy/default.aspx#1 (last visited July 20, 2012) (offering only a public cloud model to store Westlaw user data and maintaining control of who has access to the data); *see also* PAY PER CLOUD, *supra* note 74 (offering only IaaS cloud service models).

76. *See NIST Draft Synopsis and Recommendations*, *supra* note 32, at 4–14.

servers with other cloud users' data.[77] Consequently, this model offers the least security, privacy, and client control-especially over user data. Public clouds include Gmail, Yahoo Mail, Apple's iCloud, Dropbox, and the Amazon Elastic Cloud.[78] This deployment model is the most well known and used since it requires lower resources and cost.[79] For example, if a law firm is utilizing a public SaaS cloud application to keep track of billing, the law firm circumvents having to purchase, house, or maintain the cloud hardware or software.[80]

With a community cloud model, the cloud provider offers services to multiple organizations that jointly manage and operate the cloud infrastructure.[81] Like the private cloud, this deployment model may be managed by the organizations or by a third party, and may be hosted by a third party or by one of the community organizations.[82] The community cloud is a middle ground that offers more security and control over user data than the private cloud deployment model.[83]

The hybrid cloud deployment model is a combination of any of the other deployment models.[84] The combined models continue to be unique entities, but are bound together by standardized or proprietary technology that allows the provider to "burst" into other cloud deployment models as needed.[85] The hybrid cloud model

77. *Id.*

78. STEVE BACA, GLOBAL KNOWLEDGE, CLOUD COMPUTING: WHAT IT IS AND WHAT IT CAN DO FOR YOU 4 (2010), *available at* http://www.whitestratus.com/file/theme/docs/what-is-cloud-computing.pdf; Mike Lata, *Google Drive, Dropbox, iCloud: Data Privacy in the Public Cloud*, TRAINSIGNAL (May 8, 2012), http://www.trainsignal.com/blog/public-cloud-storage-privacy.

79. *See* DELL, PRIVATE CLOUDS FOR SMBS: BUILDING THE BUSINESS CASE 2 (2010), *available at* http://marketing.dell.com/Global/FileLib/SMB-WP/wp_private_clouds.pdf ("[A public cloud deployment model] saves businesses money and manpower hours by utilizing the host provider's equipment and management and alleviating onerous management tasks from overburdened IT departments.").

80. BLACK, *supra* note 73.

81. NIST DEFINITION, *supra* note 6, at 3; Tharam Dillon et al., *Cloud Computing: Issues and Challenges*, *in* 2010 24TH IEEE INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS 27 (2010), *available at* http://www.computer.org/csdl/proceedings/aina/2010/4018/00/4018a027-abs.html.

82. NIST DEFINITION, *supra* note 6, at 3.

83. *See, e.g.*, *Community Clouds*, NIMBULA, http://nimbula.com/solutions/service-providers/community/ (last visited July 20, 2012) (providing a community cloud deployment model for its IaaS cloud service, with collaborative permission requirements that enable the organizations to restrict data access amongst themselves).

84. NIST DEFINITION, *supra* note 6, at 3.

85. *Id.*; *see also* Tian Guo et al., *Seagull: Intelligent Cloud Bursting for Enterprise Applications*, *in* 2012 USENIX ANNUAL TECHNICAL CONFERENCE SHORT PAPERS 1 (2012), *available at* https://www.usenix.org/conference/usenixfederatedconferencesweek/seagull-intelligent-cloud-bursting-enterprise-applications ("[Cloud bursting] allows the

allows organizations to optimize their resources while offering more control over their service through a private cloud.[86] However, this optimization may also be more costly and means the organization's data may become distributed amongst a number of public, private, or community clouds.[87] For example, under a hybrid deployment model, a cloud provider may "burst" a client's applications or data from a private cloud deployment model to a public cloud model, creating and leaving a trail of metadata and embedded data in each cloud.

Similarly to the service models, there is no "right" deployment model. Each of the four deployment models has its own positives and negatives.

3. The Cloud Provider

Regardless of what cloud computing structure a client chooses, the cloud provider's goals are to be cost-effective and to run the cloud efficiently.[88] In order to do so, the cloud provider may employ management strategies, such as powering off unused components during periods of reduced consumer demands.[89] However, for the most efficiency, most cloud providers will often migrate client workloads, including data storage and processing, from one physical computer to another.[90] They are also not limited to keeping data and processing to one physical computer at a time; the cloud provider may divide the responsibilities of running applications and data storage into small pieces to be distributed among the cloud's servers.[91]

Furthermore, to ensure data availability and durability, cloud providers may configure the cloud to automatically replicate and back up client data, without customer knowledge, interference, or

enterprise to expand its capacity as needed while making efficient use of its existing resources.")

86. Dillon et al., *supra* note 81, at 28. *See also* RackConnect, Rackspace, http://www.rackspace.com/hosting_solutions/hybrid_hosting/rackconnect/ (last visited July 20, 2012) (providing a hybrid cloud deployment model in which the client has control of data stored in the private cloud).

87. Dillon et al., *supra* note 81, at 30; BLACK, *supra* note 73.

88. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 4-1.

89. *Id.*

90. *Id.* at 4-2; *see also Virtualization Technologies*, IBM, http://www.research.ibm.com/haifa/projects/systech/reservoir/research.shtml (last visited July 20, 2012) (discussing how IBM's cloud technology migrates customer "workloads across data center subnets and across data centers").

91. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199 (2010); *see also NIST Draft Synopsis and Recommendations*, *supra* note 32, at ES-2 ("Cloud computing favors applications that can be broken up into small independent parts.").

requests.[92] This data may also be replicated in several servers across large geographic distances.[93] And similar to that of personal computers, a cloud provider's data center also has automatic deletion policies in which unallocated space is overwritten and data is routinely deleted.[94] Apple, for instance, only keeps certain iPhone location data for a week before deleting it from its servers.[95] At the other end of the spectrum, some companies have a policy of keeping older or deleted versions of files for extended periods of time.[96]

4. The Cloud

In conclusion, diverse combinations of service models and deployment models formulate a cloud computing infrastructure. Depending on the combinations, cloud users have different levels of client control over company data. On one end, a cloud user may have full knowledge of where the user's data is at all times and have full access to preserve and retrieve it. On the other end, a cloud user may not know where the user's data is stored or even how to access it. Additionally, a cloud provider may separate, delete, or constantly relocate and replicate client data across its servers.[97] These

92. Daniel J. Abadi, *Data Management in the Cloud: Limitations and Opportunities*, *in* BULLETIN OF THE IEEE COMPUTER SOCIETY TECHNICAL COMMITTEE ON DATA ENGINEERING 3 (2009), *available at* ftp://131.107.65.22/pub/debull/A09mar/abadi.pdf. *See also* Amy Lee, *Google Explains Gmail Fail that 'Erased' Users' Emails, Disabled Accounts*, HUFFINGTON POST (Mar. 1, 2011), http://www.huffingtonpost.com/2011/03/01/google-gmail-problems-explained_n_829638.html (discussing how about 40,000 Gmail users lost all their email, which Gmail was able to recover due to their policy of backing up user data on tape).

93. Abadi, *supra* note 92 ("Amazon's S3 cloud storage service replicates data across 'regions' and 'availability zones' so that data and applications can persist even in the face of failures of an entire location.")

94. David D. Cross & Emily Kuwahara, *E-Discovery and Cloud Computing: Control of ESI in the Cloud*, 1 EDDE JOURNAL, Spring 2010, at 7, *available at* http://www.crowell.com/documents/e-discovery-and-cloud-computing-control-of-esi-in-the-cloud.pdf.

95. *iCloud Terms and Conditions*, APPLE, http://www.apple.com/legal/icloud/en/terms.html (last visited July 20, 2012).

96. *See, e.g.*, How Do I Recover Old Versions of Files, Dropbox, https://www.dropbox.com/help/11/en (last visited July 20, 2012) ("[Dropbox] keeps snapshots of every change in your Dropbox folder over the last 30 days (or more with the Pack-Rat feature).").

97. A requesting party may ask that data be produced in "native" format, which keeps its metadata intact. However, the cloud provider's actions may alter the data to the extent that there is no readily accessible native format. Brendan M. Schulman & Samantha V. Ettari, *Cloud Computing Meets E-Discovery*, N.Y.L.J., October 2011, at 2, *available at* http://www.kramerlevin.com/files/Publication/9c41c210-c7a0-4fe6-92d1-eadd0b839645/Presentation/PublicationAttachment/64bbeb34-67f1-4264-a7df-9b7e02b2c34c/Schulman %20NYLJ.pdf.

circumstances create problems for a litigant attempting to locate, preserve, and collect requested ESI.

II. Discovery Problems in the Cloud

With the intricate workings of a cloud and a third party's control and access to the client's data storage, it is no wonder cloud computing has created problems for some litigants during discovery.

A. Responding Party's Duties under the Federal Rules of Civil Procedure

Under the Federal Rules of Civil Procedure, "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[98] Furthermore, Rule 34 (a) defines discoverable information as documents or ESI "in the responding party's possession, custody or control."[99] The federal courts have also consistently held data in the possession of a third party to be within the party's possession, custody and control, so long as the party "has the right, authority, or practical ability to obtain the documents from a non-party to the action."[100] Thus, the responding party has the burden to identify, preserve and collect ESI stored in the cloud.[101]

In addition, though the Rules themselves are silent as to a party's preservation duties, under the comments to Rule 37(e), "A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case."[102] If there is no affirmative duty to preserve, the comment states the

98. FED. R. CIV. P. 26(b)(1).

99. FED. R. CIV. P. 34(a).

100. Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523 (D. Md. 2010) (internal citations omitted); SOARES, *supra* note 38. *See also, e.g.*, Nycomed U.S. Inc. v. Glenmark Generics Ltd., No. 08-CV-5023 CBA RLM, 2010 WL 3173785, at *7 (E.D.N.Y. Aug. 11, 2010) ("Glenmark's exclusive and complete access to documents residing on a third-party's server is sufficient to establish Glenmark's 'control' over those documents and thus to impose on Glenmark an obligation to conduct an appropriate ESI search of those files."); Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007) (reasoning that because a duty arose under ERISA to maintain records, the employer was in possession of the documents and may not "delegate [its] duties to a third-party under ERISA.").

101. SOARES, *supra* note 38.

102. FED. R. CIV. P. 37(f) Advisory Comm.'s Notes to 2006 Amend. (Rule 37(f) was renumbered as Rule 37(e) as part of the 2007 Amendments to the Federal Rules of Civil Procedure. Citations to the Rule 37(f) comments will henceforth refer to Rule 37(e)).

specific obligation to preserve evidence relevant to the litigation attaches at the time a party reasonably anticipates litigation.[103] Likewise, most federal courts have adopted the Rule 37(e) comments to hold a party's preservation duty attaches when the party reasonably anticipates litigation.[104]

B. Compliance Issues with the Cloud

The main problems with cloud discovery are the lack of client control and the fact that clients and cloud providers have not seriously considered potential e-discovery needs.[105] Depending on the cloud infrastructure,[106] clients often do not have control over a cloud's operating system or data storage; they merely have access to their data. Only in an IaaS model will a client have control over the cloud's operating system and data.

However, under Rule 34, the courts will likely find the responding party has control over information stored in the cloud, regardless of the cloud provider's physical control over the information and the client's lack thereof.[107] As a result, parties often

103. *Id.*

104. *See* John B. v. Goetz, 531 F.3d 448, 459 (6th Cir. 2008) ("As a general matter, it is beyond question that a party to civil litigation has a duty to preserve relevant information, including ESI, when that party has notice that the evidence is relevant to litigation or ... should have known that the evidence may be relevant to future litigation."); Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010) ("It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation."); Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 612 (S.D. Tex. 2010) (citation and internal quotation marks omitted) ("Generally, the duty to preserve arises when a party has notice that the evidence is relevant to litigation or . . . should have known that the evidence may be relevant to future litigation."); Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007) ("To ensure that the expansive discovery permitted by Rule 26(b)(1) does not become a futile exercise, putative litigants have a duty to preserve documents that may be relevant to pending or imminent litigation."); In re Napster, Inc. Copyright Litig., 462 F. Supp. 2d 1060, 1067 (N.D. Cal. 2006) ("As soon as a potential claim is identified, a litigant is under a duty to preserve evidence which it knows or reasonably should know is relevant to the action.").

105. Lidbury & Boland, *supra* note 11.

106. The cloud service and deployment method form the cloud infrastructure. *See supra* I.B.4.

107. *See* Flagg v. Detroit, 252 F.R.D. 346, 347 (E.D. Mich. 2008) (confirming the obligation to preserve and produce ESI cannot be avoided merely "through the simple expedient of storing it with a third party"); Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *1 (C.D. Cal. Sept. 21, 2007) ("Federal courts have consistently held that documents are deemed to be within a party's possession, custody or control for purposes of Rule 34 if the party has actual possession, custody or control, or has the legal right to obtain the documents on demand."); Cyntegra, Inc. v. Idexx Labs., Inc., No. CV06-4170PSG(CTX), 2007 WL 5193736, at *5 (C.D. Cal. Sept. 21, 2007), *aff'd*,

have difficultly complying with discovery requests and risk sanctions under Rule 37 for failure to provide ESI.[108]

1. Locating Information in the Cloud

In the cloud, where information has not been in the physical custody of the litigant, the litigant may not have access to the cloud's data storage, know how to search for responsive information, or even know exactly where the data is located.

With traditional e-discovery, a litigant might have a computer forensic expert directly access the hard drive of a personal computer or network server to identify and preserve responsive ESI.[109] With cloud discovery, the cloud provider's hardware and servers are stored off-site, possibly in another country, and depending on the type of cloud computing structure, the litigant may not have access to the cloud's data storage to perform a comprehensive search for data. For example, if the litigant has outsourced company email to a cloud provider with a SaaS cloud model, such as web-based email, the litigant may be limited to a standard search toolbar to locate and retrieve email.[110] There may also be an issue if personal email is mixed with business content on a web-mail account.[111] Similarly, litigants using a PaaS model also do not have complete access to the cloud's data storage to conduct discovery.

However, if the litigant is able to work with their cloud provider to obtain access to the cloud's data storage, the litigant may then encounter problems actually locating information. In non-cloud e-discovery, a company's information is stored on a user's computer or on a structured database and can generally be linked to the custodian who created the data. Potentially relevant data is found by determining who the reasonable custodians or key players are and reviewing information on their hard drives and/or the data they created, accessed, or modified on the company's internal server.[112] A company's own structured database also allows litigants unrestricted

322 F. App'x 569 (9th Cir. 2009) ("[C]ourts have extended the affirmative duty to preserve evidence to instances when that evidence is not directly within the party's custody or control so long as the party has access to, or indirect control over, such evidence.").

108. FED. R. CIV. P. 37(e).

109. Jeffrey Ziplow, et al., *E-Discovery Issues Might Grow Inside the Cloud*, 1055 PLI/Pat 257, 262 (2011).

110. *See* Lidbury & Boland, *supra* note 11.

111. *Id.*

112. Sedona Commentary, *supra* note 14, at 23.

access to explore whatever else might be relevant.[113] Since searching for potential relevant information is custodian based, rather than subject matter based, locating information in a cloud, where it may not be connected to a specific custodian, poses a problem.[114] This is further complicated because data is spread across the cloud's servers and constantly moved,[115] meaning a single file or document may be stored in multiple and variable storage locations.[116] Consequently, the cloud provider does not necessarily know where the litigant's data is actually located, and is merely able to retrieve it.[117]

2. Preserving ESI in the Cloud

Unless the company is using an IaaS cloud service model, a litigant will not be able to access the cloud's operating server to suspend the auto-delete functions associated with their files.[118] Additionally, since the Federal Rules do not require that a third-party cloud provider preserve evidence without a duty to do so, once the information is located, preserving potentially relevant ESI may be difficult, if not impossible.[119] However, this duty may have been created under the cloud provider's service contract with the party. Alternatively, a duty may be imposed if the cloud provider is served with a subpoena, attaching Rule 26 preservation and production duties to the third party.[120] Absent this duty, a litigation hold to the

113. *Id.*

114. *Id.*

115. Since cloud users only pay for what they use, the cloud providers move applications and data around to different servers depending on the user's processing needs. *See* VMWARE, VMWARE CLOUD APPLICATION PLATFORM 9 (2011), *available at* http://www.vmware.com/files/pdf/VMware-Cloud-Application-Platform-Brochure.pdf. ("On virtualized infrastructure, an application may be running on a server with four CPUs at 9 a.m., but when employees log on during their lunch hour at noon, the application will be automatically moved to a server with 16 CPUs."); *see also supra* Part I.B.3 (discussing how cloud providers divide application processing and data into fragments, stored across their data centers).

116. *See supra* Part I.B.3.

117. Steven A. Meyerowitz et al., *Practice Safe SaaS: Don't Lose Your Head (or Data) in the Clouds*, PRIVACY & DATA SECURITY L. (2009), *available at* http://news.acc.com/accwm/downloads/UHY_Enewsletter_43010.pdf.

118. *See supra* Part I.B.1 (discussing how clients only have complete control of the cloud operating system and software with a IaaS cloud model).

119. *See* FED. R. CIV. P. 26, 37, 45; Greg Dickenson, *Third Party Discovery*, EDDE JOURNAL, Spring 2012, at 12-14, *available at* http://www2.americanbar.org/sections/scitech/ST203001/PublicDocuments/EDDE%20JOURNAL%20-%20volume%203%20issue%202.pdf.

120. FED. R. CIV. P. 45. There may be complications for the litigant if the litigant and cloud provider have not discussed how the cloud provider is to respond to subpoenas.

cloud provider may be unenforceable, and the litigant would be responsible for any spoliation of evidence.[121]

Under the Rules, the responding party's preservation duties extend to preserving potentially relevant embedded files and metadata.[122] Since the preservation duty attaches when the litigant reasonably anticipated litigation, the litigant will not know whether the requesting party will want these types of data until the Rule 26(f) conference, well after the time the preservation duty is created.[123] Embedded data refers to draft language, editorial comments, and other client-deleted matter a computer program automatically retains in electronic files hidden from the user.[124] This means that deleted and previous versions of documents continue to exist.[125] Metadata refers to information detailing the "history, tracking, or management of an electronic file" that a computer program likewise automatically

Under Rule 45, third parties may issue subpoenas for potentially relevant ESI directly to the litigant's cloud provider, without providing notice to the litigant. The cloud provider therefore does not have to disclose this subpoena to the litigant or even choose to involve the litigant when responding to the subpoena, leaving the litigant exposed to risk of privilege waiver. Ashish S. Prasad, *Cloud Computing and Social Media: Electronic Discovery Considerations and Best Practices*, METROPOLITAN CORPORATE COUNSEL, February 2012, at 26, *available at* http://www.metrocorpcounsel.com /pdf/2012/February/26.pdf.

121. Spoliation is the sanctionable loss or destruction of information that may be potentially relevant in a pending or reasonably foreseeable litigation. Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 516 (D. Md. 2010); Treppel v. Biovail Corp., 249 F.R.D. 111, 120 (S.D.N.Y. 2008); Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007). *See also Google Terms of Service*, GOOGLE, *available at* http://www.google.com/intl/en/policies/terms/ (last modified Mar. 1, 2012) (stipulating Google will not be liable for any lost data); *AWS Customer Agreement*, AMAZON WEB SERVICES, *available at* http://aws.amazon.com/agreement/ (last updated Mar. 15, 2012) (stipulating Amazon will not be liable for damages associated with data loss).

122. FED. R. CIV. P. 26 Advisory Comm.'s Notes to 2006 Amend., 34(a)(1)(A), 37(f) Advisory Comm.'s Notes to 2006 Amend. *See also* STEVEN S. GENSLER, 1 FEDERAL RULES OF CIVIL PROCEDURE, RULES AND COMMENTARY RULE 34 (2012) ("It seems clear that metadata falls within the scope of Rule 34 in that it constitutes electronically stored information.").

123. FED. R. CIV. P. 26(f).

124. FED. R. CIV. P. 26(f) Advisory Comm.'s Notes to 2006 Amend.

125. Embedded data exists because: "A cardinal rule for product design of computers, disks, and tapes is to protect user data from accidental deletion. Computer operating systems erase disk files into recycle or trash folders to prevent accidental deletion of user data, and have file recovery commands. File deletion erases only file block pointers, links that let a file system reassemble a file." Gordon F. Hughes, Daniel M. Cummins & Tom Coughlin, *Disposal of Disk and Tape Data by Secure Sanitization*, IEEE SECURITY & PRIVACY, Jul./Aug. 2009, at 29, *available at* http://www.bandwidthco.com/whitepapers/datarecovery/scrubbing-sanitation/Disposal% 20of%20Disk%20and%20Tape%20Data%20by %20Secure%20Sanitization.pdf.

retains and hides from the user.[126] While a computer automatically retains embedded data and metadata, it does not necessarily do so forever. These types of data can be permanently deleted if the computer writes over disk space the data resides on, either automatically by the computer or manually according to a company's retention schedule.[127] If potentially relevant embedded data or metadata is stored on a company's own servers and computers, the company is able to pause the computer's automatic write-over program. However, a company may not do so in the cloud unless it has control over the cloud's operating system.[128] Without such control, the company must work with its cloud provider to halt any automatic write-over.

Preserving embedded data and metadata in a cloud may be complicated if the litigant is not exclusively using a private cloud deployment model. With a public, community, or hybrid deployment model, the litigant's information will be separated, stored, and intermingled with that of other organizations, which may pose problems for the litigant and other cloud users. First, once the information is located, the cloud provider may be unable to segregate the litigant's data from other clients' data.[129] Second, the litigant may be unable to preserve this intermingled data "without significant disruptions to the cloud provider's operations and/or to [its] other clients."[130] Third, the amount of intermingled data may be vast since data marked to be written over may not have actually been

126. FED. R. CIV. P. 26(f) Advisory Comm.'s Notes to 2006 Amend.

127. MATTHEW S. CORNICK, USING COMPUTERS IN THE LAW OFFICE 152 (6th ed. 2012); Roberto D. Pietro & Nino V. Verde, *Digital Forensics Techniques and Tools*, *in* HANDBOOK OF ELECTRONIC SECURITY AND DIGITAL FORENSICS 348 (Hamid Jahankhani et al., eds., 2010).

128. Companies only have control over the cloud's operating system if they are utilizing an IaaS cloud service model. *See supra* Part II.B.1.

129. *See Addressing the Preservation & Production of Database Information in Civil Litigation*, THE SEDONA CONFERENCE DATABASE PRINCIPLES, Apr. 2011, at 7, *available at* www.thesedonaconference.org/publications ("[S]ome of the important issues to keep in mind are: … The extent to which the requested data may be co-mingled with data of other non-parties, and the difficulty of extracting only the requested data."); Alberto G. Araiza, *Electronic Discovery in the Cloud*, 2011 DUKE L. & TECH. REV. 8, ¶ 27 (2011) (internal quotation marks omitted) ("Common metadata may be maintained in repositories shared between clients, which makes it a major problem to isolate [that] data and maintain the security.").

130. Ziplow, *supra* note 109.

permanently destroyed[131] and because some cloud providers have longer retention policies than others.[132]

One of the benefits of cloud computing is its elasticity and ability to shift resources for cost-efficiency. In the cloud, "data may always be in transit, never anywhere, always somewhere."[133] Because segregating the litigant's data may be impossible, the cloud provider would have to preserve the physical data storage, which would require preserving other clients' information and restricting the other cloud users from access to their own information.[134] The cloud provider would also have to preserve multiple data storages since the litigant's information is often stored in pieces across the cloud's servers. This would frustrate the efficiency of the cloud by preventing the cloud provider from shifting resources and information. Also, since cloud service is often on a pay-per-use basis, nonparty cloud clients may face increased costs. Considering this, a cloud provider may be reluctant—if not unwilling—to comply with a litigation hold.

In addition, as cloud providers automatically and continually replicate and back up data stored in the cloud, the litigant will face the difficulty of trying to preserve all these duplicates. Because most cloud users do not have control over the cloud's operating system,[135]

131. CORNICK, *supra* note 127 ("When you delete a file, all you have done is made the disk space occupied by that file available to be written over. Depending on the computer's storage capacity, the size of the deleted file, and the amount of new data being put on the hard drive, it can be a long time before a 'deleted' file is actually written over.").

132. Microsoft Azure, a PaaS cloud provider, has a minimum retention policy for current clients in which data may be kept for at *least* ten days. Furthermore, Microsoft Azure's Services Use Rights states that if service is terminated, it *may* delete data permanently from its servers. *Monitoring and Diagnostic Guidance for Windows Azure—Hosted Applications*, MICROSOFT SYSTEM CENTER (June 11, 2010), *available at* http://download.microsoft.com/download/4/C/B/4CB0167F-B6D9-4B46-8DF1-69CCCA66FDDE/SystemCenterOperationsManagerMonitoringforAzureHostedAppsatMicrosoft.pdf; *Online Services Use Rights*, MICROSOFT ONLINE SERVICES USE RIGHTS, at 15 (Oct., 2012), *available at* http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31. *See also Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/your-info# deleting (last visited July 21, 2012) (disclaiming that Facebook keeps information from a deleted Facebook account for up to 90 days); *How Can I Recover Deleted Email Messages?*, GOOGLE, http://support.google.com/a/bin/answer.py?hl=en&answer=112445 (last visited July 21, 2012) (stating Gmail permanently deletes "deleted" emails after 30 days).

133. Meyerowitz et al., *supra* note 117 (quoting Steven W. Teppler, Senior Counsel, KamberEdelson, LLC, Presentation at the April 2009 Storage Networking World Show (Apr. 6-9, 2009)).

134. Araiza, *supra* note 129, at 32.

135. *See supra* Part I.B.1 (discussing different levels of operating control given to users under each of the cloud service models).

the litigant may be unable to get the cloud provider to cease replicating and backing up data.

Litigants may also have difficulty complying with their preservation duties if they change cloud service providers. Because of intermingled embedded data and metadata, a litigant who moves information to another cloud provider, may still have discoverable data on the previous provider's cloud servers. Upon termination of the cloud service, cloud providers try to ensure their next clients do not observe data residue from their former client.[136] However, "[s]trong data erase policies (e.g., multiple overwriting of disk blocks) are time consuming and may not be compatible with high performance when tenants are changing."[137] Therefore, providers do not always purge all of a former client's data from their cloud data centers, and may even waive any duty of doing so from their service agreement.[138]

Additionally, discoverable information may be destroyed if the cloud provider chooses to terminate the service agreement, if the provider goes bankrupt or ceases to exist, or even accidentally. After a grace period, if a litigant fails to pay, the cloud providers may terminate "for cause" and delete the litigant's data. For example, Amazon's 2012 version of its cloud service agreement states that, "Upon any termination of this Agreement: (i) all your rights under this Agreement immediately terminate."[139] This means a user may lose property rights to data stored on Amazon's cloud, permitting Amazon to delete any and all of the user's data. The agreement only

136. *NIST Draft Synopsis and Recommendations*, *supra* note 32, at 7–8.

137. *Id.*

138. By explicitly stating the cloud provider will retain customer data or by omitting language requiring the cloud provider to delete or purge client data after service is terminated, the cloud provider may do what they wish with a former client's data. *See Cloud Terms of Service*, RACKSPACE, http://www.rackspace.com/cloud/legal/ (last revised May 7, 2012) ("[W]e may destroy all but the most recent backup. These backups may not be available to you or, if available, may not be useful to you outside of the Rackspace Cloud systems."); *Dell Cloud Solutions Agreement*, DELL (emphasis added), http://content.dell.com/us/en/home/d/solutions/cloud-solutions-agreement.aspx (last revised June 21, 2012) ("We *may* delete your data stored in the Cloud (a) sixty (60) days following any termination by us pursuant to Section 5 of this Agreement, or (b) if you (or your reseller, if you purchased the Solution from a reseller) fail to renew an applicable Solution Description within sixty (60) days of expiration."); *Terms of Service*, JOYENT, http://www.joyent.com/about/policies/terms-of-service/ (last visited July 22, 2012) ("As soon as you cancel the service, your right to use it stops right away. You may not have access to data that you stored on the service after you terminate the service.").

139. *AWS Customer Agreement*, *supra* note 121.

promises not to erase any of the litigant's content if the termination is not "for cause" or if the service is merely suspended.[140]

In a former version of this agreement, Amazon stated that it would "have no obligation to continue to store [a user's] data during any period of suspension or termination or to permit [the user] to retrieve the same."[141] Commenters have construed this to mean Amazon will not make any commitment to preserve the client's data or allow any retrieval if services are terminated for cause.[142] Similarly, these provisions may apply if the cloud provider determines the litigant is violating its terms in other ways. So even if the litigant cures the cause of the termination, the litigant may be held liable for any data lost during the period the cloud provider terminated the agreement.[143] This liability may not only include risk of sanction for loss of potentially relevant information during the discovery phase of litigation, but also claims for breach of contract, negligence, property damage, and any claims arising out of any federal or state statute.[144]

---

140. *Id.*

141. Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 206 (2011) (quoting AWS Customer Agreement, Amazon Web Services (Oct., 2010)).

142. *Id.* (comparing versions of Amazon's cloud service agreement: "In neither the October 2010 nor August 2011 versions of the Agreement does Amazon give assurance that it will take precautions to *protect* such data or to ensure that post-termination protection will be equal or in any way comparable to pre-termination protection. . . . If Amazon elects to terminate the service, it makes no commitments to keeping stored data whatsoever or to allow any retrieval of data").

143. *See id.* ("Customers might lose data while they attempt to cure the causes that led to the termination."); *see also, e.g.*, *Terms of Service*, JOYENT, *available at* http://www.joyent.com/about/policies/terms-of-service/ (last visited July 22, 2012) ("YOU EXPRESSLY UNDERSTAND AND AGREE THAT JOYENT SHALL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF JOYENT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES RESULTING FROM: (i) THE USE OR THE INABILITY TO USE JOYENT SERVICES . . . .").

144. *See* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 521 (D. Md. 2010) (internal quotation marks omitted) ("[T]he duty [to preserve potentially relevant ESI] may arise from statutes, regulations, ethical rules, court orders, or the common law. . . ., a contract, or another special circumstance."); Cyntegra, Inc. v. Idexx Labs., Inc., No. CV06-4170PSG (CTX), 2007 WL 5193736, at *3 (C.D. Cal. Sept. 21, 2007), ("Defendant asserts that Plaintiff's failure to preserve business documents constituted spoliation and make sanctions appropriate. Although the documents were stored on NetNation's outsourced servers, they were deleted due to Plaintiff's failure to make payments after March 7, 2006. (Opp'n to Renewed Motion at 1:22-23). Plaintiff, in defense, claims: (1) the lost information was irrelevant to this action; (2) the information Defendant says it needs for its defense was produced, was available in discovery, or does not exist; and (3) it lacked sufficient control over the documents. Plaintiff also seeks sanctions against Defendant for

If the cloud provider goes bankrupt or ceases to exist, litigants may be unable to access and retrieve their information. If a company files for Chapter 7 Bankruptcy, the company's operations-in this case, cloud service- ceases instantly upon the filing.[145] The company is not required to notify its clients, so at best "users of a cloud system can expect to have at most sixty days, on down to just a few days, to take steps to protect themselves."[146] If a company files for Chapter 11 Reorganization Bankruptcy, it may be able to continue to operate as a business to allow clients to retrieve their property,[147] so at least temporarily, cloud users will not have to worry about being locked out of the cloud or having their service or necessary licenses

acting in bad faith by refiling this motion. The law and facts provided do not support Plaintiff's defenses, and instead demonstrate spoliation of evidence."); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No.99-185 TUC ACM, 2000 WL 726789, at *2 (D. Ariz. Apr. 18, 2000) (characterizing loss of computer data as physical damage); Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737-38 (Minn. Ct. App. 1991) (holding computer information is tangible property); J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979) ("Where a special relationship exists between the parties, a plaintiff may recover for loss of expected economic advantage through the negligent performance of a contract although the parties were not in contractual privity."); *see also, e.g.*, 12 U.S.C. § 1829b (2012) (mandating insured depository institutions retain certain records "for such period as the Secretary may prescribe for the type in question"); CAL. CIV. CODE § 1798.81.5(b) (2006) ("A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").

145. DAVID S. CAPLAN, BANKRUPTCY IN THE CLOUD: EFFECTS OF BANKRUPTCY BY A CLOUD SERVICES PROVIDER 4 (2010), *available at* http://ftp.documation.com/references/ABA10a/PDfs/3_3.pdf. *See also* 11 U.S.C. § 721 (2012) (mandating the business cease operations unless the court has authorized a "trustee to operate the business of the debtor for a limited period, if such operation is in the best interest of the estate and consistent with the orderly liquidation of the estate.").

146. CAPLAN, *supra* note 145, at 5; *see also Liquidation Under the Bankruptcy Code*, UNITED STATES COURTS, http://www.uscourts.gov/FederalCourts/Bankruptcy/BankruptcyBasics/Chapter7.aspx (last visited July 22, 2012) (providing no notice requirement for the petitioning business and that the bankruptcy clerk will only give notice to creditors listed by the debtor, *after* the business files for Chapter 7 bankruptcy); *AlphaRed Declares Chapter 7 Bankruptcy*, STEADFAST (Dec. 23, 2008), http://steadfast.net/blog/index.php/general/alphared-declares-chapter-7-bankruptcy (giving clients only a one day notice of bankruptcy, "I just wanted to state that as AlphaRed has now declared Chapter 7 bankruptcy and is ending service tomorrow it is certainly time for any existing AlphaRed clients to get moved out. We again are willing to help, by offering free backup space to any affected users and we do have servers immediately available.").

147. 11 U.S.C. § 362(a)(3) (2012) ("Except as provided in subsection (b) of this section, a petition . . . operates as a stay, applicable to all entities, of . . . (3) any act to obtain possession of property of the estate or of property from the estate or to exercise control over property of the estate . . . .").

terminated unexpectedly.[148] Under Chapter 11, the debtor must give clients notice of the bankruptcy to retrieve their data.[149] In a situation where a cloud provider's business has been dissolved, depending on requirements set out by its state of incorporation, the cloud provider may not be required to provide notice and opportunity for clients to retrieve their data before dissolution makes such retrieval impossible.[150]

However, whenever clients are given notice and time to retrieve their data, this process could take months. For example, in 2009, the cloud provider, Coghead, gave notice to clients that it was ending its cloud services and provided customers two months to retrieve their applications and data.[151] Nevertheless, it took one client approximately four and a half months—over double the time allotted—to move his data from Coghead's server to another cloud provider.[152]

A litigant may also be liable for failing to preserve potentially relevant information that a cloud provider accidentally lost. In 2009, T-Mobile's server crashed, causing over a million users to permanently lose data.[153] Courts will likely find situations of

148. *See* CAPLAN, *supra* note 145 ("[F]or a time at least, landlords cannot lock an IaaS host out of its facility, utility or network providers cannot terminate service, and software licensors cannot terminate necessary licenses.").

149. *See* In re Savage Indus., Inc., 43 F.3d 714, 720 (1st Cir. 1994) ("[T]he debtor in possession or trustee must ensure 'parties in interest' adequate notice and opportunity to be heard *before* their interests may be adversely affected.") (citing Bankruptcy Code, 11 U.S.C. § 1109(b) (internal quotation marks omitted) ("[P]arties in interest have right to be heard in chapter 11 case.")).

150. A company's state of dissolution is determined by its state of incorporation. First Nat. City Bank v. Banco Para El Comercio Exterior de Cuba, 462 U.S. 611, 621 (1983) ("As a general matter, the law of the state of incorporation normally determines issues relating to the *internal* affairs of a corporation."). *See, e.g.*, CAL. CORP. CODE § 1903 (West 2012) ("The board shall cause written notice of the commencement of the proceeding for voluntary winding up to be given by mail . . . to all known creditors and claimants whose addresses appear on the records of the corporation."); MINN. STAT. § 302A.727 (2012) ("When a notice of intent to dissolve has been filed with the secretary of state, the corporation *may* give notice of the filing to each creditor of and claimant against the corporation known or unknown, present or future, and contingent or noncontingent." (emphasis added)).

151. Paul Krill, *Coghead Customers Have Two Months to Save Their Data*, INFOWORLD (Feb. 25, 2009), http://www.infoworld.com/t/platforms/coghead-customers-have-two-months-save-their-data-815.

152. Robert L. Scheier, *What to Do if Your Cloud Provider Disappears*, INFOWORLD (April 20, 2009), http://www.infoworld.com/d/cloud-computing/what-do-if-your-cloud-provider-disappears-508.

153. Nick Wingfield, *T-Mobile Offers $100 Gift Card to Some Sidekick Customers*, WALL ST. J. (Oct. 12, 2009, 9:38 PM), http://blogs.wsj.com/digits/2009/10/12/t-mobile-offers-100-gift-card-to-some-sidekick-customers/ ("Regarding those of you who have lost

accidental loss no different from a cloud provider's purposeful and routine deletion, and find that the litigant has control of the data.

In addition, preservation problems may exist when a cloud provider is unexpectedly shut down. On January 19, 2012, the United States Department of Justice shut down Megaupload.com, a giant Internet file-sharing site, and arrested seven employees, charging them with generating more than $175 million in profits through racketeering, conspiracy to commit copyright infringement, and conspiring to commit money laundering, as well as two substantial counts of copyright infringement.[154] This left 150 million users cut off from their information and facing deletion of their data.[155] After reviewing Megaupload's servers, the U.S. government stated the hosting companies had a right to begin deleting data, since Megaupload's assets were frozen and the provider was no longer able to pay for the storage.[156] While the hosts have not yet deleted any data, as of October 26, 2012, increasing costs of storage and the on-going case against Megaupload have left clients in limbo as to whether they will ever regain access to their information.[157]

---

personal content, T-Mobile and Microsoft/Danger continue to do all we can to recover and return any lost information. Recent efforts indicate the prospects of recovering some lost content may now be possible." (quoting *T-Mobile Status Update on Sidekick Data Disruption*, T-MOBILE (Oct. 9, 2009)). *See also* Nick Wingfield, *Microsoft, T-Mobile Stumble with Sidekick Glitch*, WALL ST. J. (Oct. 11, 2009), http://online.wsj.com/article/SB10001424052748703790404574467431941990194.html (reporting personal data not stored locally on a Sidekick customer's device had almost certainly been lost).

154. Indictment, United States v. Kim Dotcom, No. 1:12CR3, 2012 WL 263498 (E.D.Va. Jan. 5, 2012); *Megaupload.com Charged With Piracy Violations, Shut Down by Feds*, HUFFINGTON POST (Jan. 20, 2012, 2:44 PM), http://www.huffingtonpost.com/2012/01/19/megauploadcom-piracy-charges_n_1216764.html.

155. Byron Acohido, *Government Takedown of Megaupload Leads to New Fears*, USA TODAY (Jan. 20, 2012, 11:03 PM), http://www.usatoday.com/tech/news/story/2012-01-20/megaupload-arrests-FBI/52697186/1.

156. Hayley Tsukayama, *Megaupload Data Could Be Deleted Starting Thursday*, WASH POST (Jan. 30, 2012), http://www.washingtonpost.com/business/technology/megaupload-data-could-be-deleted-starting-thursday/2012/01/30/gIQAeggGcQ_story.html.

157. Jeremy Kirk, *Judge Weighs Fate of Orphaned Megaupload Data*, PCWorld (Oct. 7, 2012, 11:02 AM), http://www.pcworld.com/article/2011289/judge-weighs-fate-of-orphaned-megaupload-data.html. *See* Matthew Barakat, *Megaupload User Data in Limbo*, USA TODAY (April 13, 2012, 10:36 PM), http://www.usatoday.com/tech/news/story/2012-04-13/megaupload-data/54267820/1 ("Currently the data—25 million gigabytes' worth—sits on 1,100 powered-down servers stored in a climate-controlled warehouse in Harrisonburg, Va. The company that leased the servers to Megaupload, ... Carpathia[,] is paying thousands of dollars a day just to store the machines. They are also losing revenue that would be available if it erased the data and repurposed the servers for other uses."); Nick Perry, *Carpathia Hosting Can't Afford to Keep Megaupload Data: Company Will Delete Data if No One Pays the Bill*, HUFFINGTON POST (Mar. 22, 2012, 2:01 PM), http://www.huffingtonpost.com/2012/03/22/megaupload-company-will-delete-data_n_

There is currently no case law that relates to loss of data due to a third-party cloud provider's bankruptcy, dissolution, or indictment. Arguably, a court may find the litigant had no control over the lost data, since the litigant no longer "has the right, authority, or practical ability to obtain the documents from a non-party to the action."[158] However, such a holding provides no assurances. Without a backup copy of the data, the litigant may be subject to a spoliation sanction.[159]

3. Retrieval

Once a litigant has managed to locate and preserve potentially relevant ESI, the litigant may have problems collecting this data. First, although major Cloud providers may have safeguards in place to assure accuracy, the litigant could inadvertently retrieve ESI belonging to other clients, creating liabilities such as inadvertent waiver of privilege or breach of privacy.[160] Privilege may be waived if confidential information is disclosed to an unprivileged third party.[161] Because a litigant's data is intermingled and may be inseparable from other third-party cloud users' data in a public cloud, a cloud provider's production of intermingled data may constitute waiver of a third party's privilege.

Inadvertent production of a third party's data may also constitute breach of privacy if the third party's confidential information is made available to the nonaffiliated litigant. For example, covered entities, such as health care providers, bound by the federal Health Insurance Portability and Accountability Act (HIPAA) may only store protected health information in a cloud with the contractual stipulation that the cloud provider is also bound by the same privacy

1373285. html; Tom Schoenberg, *Megaupload Judge Defers Decision on Seizing Users' Data*, BLOOMBERG (June 29, 2012, 5:57 PM), http://www.bloomberg.com/news/2012-06-29/megaupload-judge-defers-decision-on-seizing-users-data.html (reporting that a U.S. judge has deferred making a decision on whether millions of gigabytes of data belonging to Megaupload users should be preserved so users could regain access to it).

158. Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523 (D. Md. 2010) (internal citations omitted).

159. Courts will likely consider information also available from other reasonably accessible sources to be acceptable if the requesting party is not prejudiced by it. FED. R. CIV. P. 26(b)(2) Advisory Comm.'s Notes to 2006 Amend.

160. Araiza, *supra* note 129, at 26; NEW YORK STATE BAR ASSOCIATION, REPORT OF THE PRIVACY TASK FORCE 40-41 (2009), *available at* http://www.nysba.org/AM/Template.cfm?Section=Privacy_Report.

161. Carla R. Walworth et al., PRIVILEGE LAW, ITS GLOBAL APPLICATION, AND THE IMPACT OF NEW TECHNOLOGY 3-5 (2012), *available at* http://www.americanbar.org/content/dam/aba/publications/young_lawyer/attorneyclientprivlege.authcheckdam.pdf (discussing the three jurisdictional approaches to inadvertent waiver).

and security requirements under HIPAA as the covered entity itself.[162] Therefore, inadvertent disclosure of protected health information by the cloud provider would create liabilities under HIPAA. Similarly, under the Gramm-Leach-Bliley Act, financial institutions are restricted from storing consumers' private financial information on a cloud without the cloud provider first agreeing to be bound under the same disclosure and security provisions of the Act.[163] Along with statutorily mandated duties, a cloud provider may also have an implied or contractual duty not to disclose confidential information.[164] Because of these risks, a cloud provider may be reluctant to produce data that may expose it to third-party claims.

Secondly, if the litigant is successful in locating potentially relevant ESI, depending on the cloud deployment model, the litigant may be unable to collect this data. If the cloud's data center is located in a jurisdiction outside of the US, there may be restrictions on the transfer or disclosure of data.[165] In 1995, the European Council and Parliament enacted the Data Protection Directive, which only permits personal data located in the European Economic Area (EEA)[166] to be transferred outside the EEA if the receiving country

162. Under HIPAA, a covered entity may not use or disclose protected health information unless as permitted or required by 45 C.F.R. § 164.502(a), and must ensure such protected health information is only accessible to those authorized under 45 C.F.R. § 164.508. 45 C.F.R. §§ 164.502, 164.504(e), 164.508 (2012). *See also* Robert Gellman, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 9 (2009), *available at* http://www.worldprivacyforum.org /pdf/WPF_Cloud_Privacy_Report.pdf ("Before a covered entity may transfer protected health information to a service provider, the entity and the provider must enter into a *business associate agreement*. While a business associate is not directly subject to the HIPAA rule currently, the agreement between the business associate and the covered entity would essentially require the business associate to comply with the same standards that apply to the covered entity.")

163. 15 U.S.C. § 6802 (2012). *See also*, *e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (2012); Cable Communications Policy Act, 47 U.S.C. § 551 (2012).

164. *See* Complaint at 4-6, In the Matter of Facebook, Inc., F.T.C. File No. 0923184 (2011), *available at* http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf (claiming Facebook illegally deceived consumers by allowing third-party applications and advertisers access to private user data).

165. Sedona Commentary, *supra* note 14, at 20.

166. The EEA is composed of the 27 countries of the European Union in addition to the non-European countries of Iceland, Liechtenstein, and Norway. The European Union is composed of the following 27 countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. While Switzerland is not part of the EEA Agreement, it is also bound to the Directive under a bilateral agreement with the European Union. *European Union*, EUROPEAN COMMISSION, http://ec.europa. eu/justice/data-protection/bodies/authorities/eu/index_en.htm (last visited July 24, 2012);

can ensure an adequate level of protection.[167] However, the European Union has not accepted the United States as a country that meets the standard of protection,[168] and it only allows data export into the United States from parties who comply with the United States' Department of Commerce's Safe Harbor Privacy Principles.[169] Moreover, other countries have enacted similar restrictions that prohibit the export of data.[170] Therefore, a litigant may be prevented from retrieving potentially relevant data located on a physical server in a country bound by the Directive or a similar mandate.

C. Sanctions

Rule 37 governs sanctions for failing to comply with discovery requests. The comments to Rule 37(e) state that once litigation is pending or is reasonably anticipated, a party is put on notice to

EEA Agreement, EFTA, http://www.efta.int/eea/eea-agreement.aspx (last visited July 22, 2012).

167. Directive 95/46/E, ch. IV, art.5 1995 O.J. (L. 281) (EU), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT. While the Directive is currently undergoing reform to consider the impact of new technology, it remains to be seen whether the European Union will remove this data transfer limitation. *Reform of the Data Protection Legal Framework*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/review/index_en.htm (last visited July 22, 2012).

168. The United States falls short of this standard because the United States privacy laws only protect the data of U.S. citizens. *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, at 5 n.16, (Oct. 24, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_en.pdf.

169. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited Oct. 26, 2012) (stating the European Union only recognizes the United States' Department of Commerce's Safe Harbor Privacy Principles and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection).

170. *See* Ley Federal de Protección de Datos Personales en Posesión de los Particulares [Federal Law for the Protection of Personal Data], ch. 4, § III, Diario Oficial de la Federación [DO], 21 de Diciembre de 2011 (Mex.), *available at* http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011 (requiring informed consent for transfer of data out of Mexico unless the recipient meets certain conditions, such as following Mexican law with respect to data rights); BNA International, *Long-Awaited Changes to Russian Personal Data Law: Two Sides to a Coin*, WORLD COMMUNICATIONS REGULATION REPORT, vol. 6, no. 9, Sept. 2011, at 2, *available at* http://www.salans.com/en-GB/Locations/~/media/Assets/Salans/Publications/2011/20110927-Long-Awaited%20Changes%20to%20Russian%20Personal%20Data%20Law.ashx (discussing Russia's 2011 Personal Data Law amendments, which restrict cross-border of data outside of Russia to countries that are parties to the European Union or other countries approved by Russian officials that can guarantee adequate protection of personal data).

preserve information.[171] After a responding party is given notice, the destruction of information available from reasonably accessible sources is no longer to be considered routine and in good faith, and instead is considered to be spoliation.[172] To avoid spoliation, litigants place a litigation hold on any possibly relevant information that is stored on their personal hard drives or on a cloud server. However, because the cloud provider may not have a duty to comply with the litigation hold, litigants using cloud services risk spoliation because of the third party's physical control over their data.[173]

A cloud provider may choose to ignore the litigation hold because it may be unable to separate the litigant's data from other users' data and would have to just preserve this intermingled data, which may be more burdensome for a cloud provider. In addition, the owner(s) of the other data may not wish for their data to be restricted and may want to access, modify, or delete their data. The cloud provider may be disinclined to disrupt their other clients' cloud use for a litigant. The cloud provider may also be unwilling to halt its routine and automatic deletion of data and may not wish to store the potentially relevant ESI in a static server, hindering its ability to utilize the server and maximize its resources. If the cloud provider does not comply with the litigation hold, potentially relevant ESI may be deleted. Even if the ESI is not deleted, potentially relevant metadata and embedded data may become altered or modified in the cloud.[174] This change from its original form at the time of notice may be considered spoliation.[175] Because a court will likely consider the litigant to be in control of the cloud-stored data, the court may impose sanctions for the cloud provider's spoliation.

Moreover, even if a litigant is successful in recruiting their cloud provider's cooperation, litigants may still be hindered in complying with their duties because cloud providers usually lack the discovery

171. FED. R. CIV. P. 37(e) Advisory Comm.'s Notes to 2006 Amend.

172. "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." FED. R. CIV. P. 37(e).

173. *See supra* Part II.B.2.

174. *See* Schulman & Ettari, *supra* note 97 ("Each of these metadata fields, and perhaps others, is at risk of being altered by cloud systems that constantly move data to the most efficient storage location, use automated file naming conventions, and store files without reference to custodian.").

175. Spoliation may also mean the significant and meaningful alteration of data. Brewer v. Dowling, 862 S.W.2d 156, 158 n.2 (Tex. App. Fort Worth 1993) (quoting Black's Law Dictionary 1257 (5th ed. 1979)).

tools or even a defined search feature to help users locate, preserve, collect, and process ESI for e-discovery purposes.[176] If ESI was maintained in-house, a litigant can either utilize his or her own e-discovery software or methods, or employ a third-party SaaS cloud discovery application.[177] However, when ESI is stored in a third-party cloud, the cloud provider may inherently lack discovery tools or be unable to support other third-party discovery applications that can provide these missing discovery tools.[178] Since a litigant may be technologically unable to preserve, harvest, or even review potentially relevant ESI, the litigant may be helpless to prevent spoliation.

Currently, whether a court may impose sanctions for spoliation of cloud-stored data is unpredictable. Courts are not required to impose sanctions for spoliation under Rule 37 but may do so as they deem just.[179] In many circuits, courts hold that any sanction is available so long as the responding party is culpable in any way, such as simple negligence.[180] Other circuits require a showing of bad faith

176. BARRY MURPHY, EDJ GROUP, "THE CLOUD AND EDISCOVERY" SERIES: GEARING UP FOR THE CLOUD AND SOCIAL MEDIA 11 (2012), *available at* http://www.americanbar.org/content/dam/aba/events/labor_law/2012/04/aba_national_symposium_on_technology_in_labor_employment_law/mw2012tech__murphy.authcheckdam.pdf ("Many Cloud providers have not developed the tools to preserve or collect vital metadata."); Lidbury & Boland, *supra* note 11.

177. *See* CATALYST, http://www.catalystsecure.com/ (last visited July 22, 2012) (offering e-discovery support); NEXTPOINT, http://www.nextpoint.com/ (last visited July 22, 2012) (offering e-discovery management software).

178. For example, some webmail providers, such as Gmail, do not provide more than the standard search tool bar. Although users may have the option of downloading emails onto a computer for more comprehensive searches, these files may not be all-inclusive of what may be discoverable in a webmail account, and may not preserve an email's native format. *See How Do I Download Messages to Another Computer Once I've Enabled POP?*, GOOGLE GMAIL, http://support.google.com/mail/bin/answer.py?hl=en&answer=13289 (last visited July 23, 2012) (providing instructions on how to download emails). *But cf.* SPRINGCM, http://www.springcm.com/salesforce (last visited July 23, 2012) (providing a cloud e-discovery application specifically compatible with salesforce.com, a SaaS cloud, and force.com, a PaaS cloud).

179. FED. R. CIV. P. 37(b).

180. INST. FOR THE ADVANCEMENT OF THE AM. LEGAL SYS., NAVIGATING THE HAZARDS OF E-DISCOVERY: A MANUAL FOR JUDGES IN STATE COURTS ACROSS THE NATION 19 (2d ed. 2012) [hereinafter NAVIGATING THE HAZARDS OF E-DISCOVERY]. *See also* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) ("The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence."); Silvestri v. Gen. Motors Corp., 271 F.3d 583, 593 (4th Cir. 2001) ("But even when conduct is less culpable, dismissal may be necessary if the prejudice to the defendant is extraordinary, denying it the ability to adequately defend its case."); Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 438 (S.D.N.Y. 2010) ("'[The] sanction [of an adverse inference] should be available even for the negligent destruction of documents if that is necessary to further the remedial purpose of the inference. It makes

before harsh sanctions—such as dismissal or spoliation instructions—may be imposed.[181] Furthermore, some courts find culpability for sanctions only require "responsibility and control" instead of "evil intent."[182] If the court follows the negligence approach, the court may find the cloud provider's negligent spoliation of ESI resulted in prejudice so great as to deserve sanctions. If the court follows the bad faith approach, a litigant may be able to avoid sanctions if the litigant attempted to obtain the cloud provider's cooperation during discovery and made good faith efforts to locate, preserve, and collect the ESI. If the court follows the responsibility and control approach, since the litigant is found to be control of the data, the court may sanction the litigant for merely being unable to prevent the cloud provider's spoliation. These contradictory jurisdictional approaches impact whether a court will impose sanctions and, if so, the severity of the sanctions it might impose.

D. Proportionality

Proportionality refers to the balancing of a requesting party's need for relevant information against the responding party's burden and cost associated with producing the ESI. This proportionality consideration is included in Rule 26, which states that a responding party is not required to produce ESI from sources it identifies as

---

little difference to the party victimized by the destruction of evidence whether that act was done willfully or negligently.'") (quoting Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 75 (S.D.N.Y. 1991)).

181. NAVIGATING THE HAZARDS OF E-DISCOVERY, *supra* note 180; *see also* Turner v. Pub. Serv. Co., 563 F.3d 1136, 1149 (10th Cir. 2009) (citation and internal quotation marks omitted) ("Mere negligence in losing or destroying records is not enough because it does not support an inference of consciousness of a weak case. Without a showing of bad faith, a district court may only impose lesser sanctions."); Bashir v. Amtrak, 119 F.3d 929, 931 (11th Cir. 1997) ("[A]n adverse inference is drawn from a party's failure to preserve evidence only when the absence of that evidence is predicated on bad faith."); Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 614 (S.D. Tex. 2010) (requiring evidence of bad faith before imposing severe sanctions, such as default judgment or adverse inference instructions); Russell v. Univ. of Tex. of Permian Basin, 234 Fed. Appx. 195, 208 (5th Cir. 2007) ("Mere negligence is not enough' to warrant an instruction on spoliation."); *but cf.* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 536 (D. Md. 2010) (holding negligence and gross negligence are not sufficient to impose severe sanctions, but that the conduct does not have to rise to the level of bad faith).

182. Carole S. Gailor, *In-depth Examination of the Law Regarding Spoliation in State and Federal Courts*, JOURNAL OF THE AM. ACAD. OF MATRIMONIAL LAWYERS, June 2010, at 79, *available at* http://www.aaml.org/sites/default/files/MAT102_2.pdf (citing Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193 (D. Utah 2009)). *See also* Bowman v. Am. Med. Sys., Inc., No. 96-7871, 1998 WL 721079, at *3-5 (E.D. Pa. Oct. 9, 1998) (imposing the severe sanction of dismissal because a third party disposed of material evidence Plaintiff was responsible for).

unreasonably accessible due to cost or burden.[183] A litigant may try to seek a reprieve from production under this rule if the litigant encounters any problems collecting data in the cloud. However, a court may nonetheless order discovery of data not reasonably accessible because it is stored in a third-party cloud if there is good cause.[184]

There are two main proportionality analyses a court could use to determine whether ESI is unreasonably accessible and whether there is good cause to order production notwithstanding.[185] The two-tiered approach under the Advisory Committee's note to Rule 26 is the most commonly used proportionality analysis.[186] Under this approach, the responding party first must show that the requested information is not reasonably accessible because of undue burden or cost. The location of the data is not what determines inaccessibility, but whether retrieving them would be an undue burden or cost too much.[187] Whether there is good cause to order production regardless of the burden is determined by considering the seven factors specified in the Advisory Committee's note.[188] A litigant would have an easier

183. FED. R. CIV. P. 26(b)(2)(B).

184. *Id.*

185. Courts may rely on the proportionality standard laid out under the Comments to Rule 26 or the Zubulake court's proportionality analysis. *See* FED. R. CIV. P. 26 Advisory Comm.'s Notes to 2006 Amend.; Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 (S.D.N.Y. 2003).

186. *See* Tucker v. Am. Int'l Grp., Inc., No. 3:09-CV-1499 CSH, 2012 WL 902930, at *4 (D. Conn. Mar. 15, 2012) (applying the Advisory Committee's proportionality standard); Star Direct Telecom, Inc. v. Global Crossing Bandwidth, Inc., 272 F.R.D. 350, 359 (W.D.N.Y. 2011) (applying the Advisory Committee's proportionality standard); Peskoff v. Faber, 251 F.R.D. 59, 60 (D.D.C. 2008) (applying the Advisory Committee's proportionality standard); Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 147–48 (D.D.C. 2007) (applying the Advisory Committee's proportionality standard); Best Buy Stores, L.P. v. Developers Diversified Realty Corp., 247 F.R.D. 567, 571 (D. Minn. 2007) (applying the Advisory Committee's proportionality standard); PSEG Power N.Y., Inc. v. Alberici Constructors, Inc., No. 1:05-CV-657(DNHRFT), 2007 WL 2687670, at *10–11 (N.D.N.Y. Sept. 7, 2007) (applying the Advisory Committee's proportionality standard).

187. *See* Petcou v. C.H. Robinson Worldwide, Inc., CIVA1:06CV2157HTWGGB, 2008 WL 542684, at *1 (N.D. Ga. Feb. 25, 2008) (determining requested information was not reasonably accessible after the responding party demonstrated cost of retrieving about two years' worth of e-mails for one employee would be approximately $79,300).

188. Courts will consider: (1) specificity of the discovery request; (2) quantity of information available from other and more easily accessed sources; (3) failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) importance of the issues at stake in the litigation; and (7) the parties' resources. This test weighs each factor equally and

time demonstrating that retrieval from the cloud would be too burdensome under this approach because the litigant would only have to explain the difficulties with retrieval. In addition, the good cause analysis places equal weight on all factors so the litigant will have a fair chance of arguing nonmonetary reasons against production.[189] However, a court may still find good cause for production of readily accessible, but intermingled and inseparable, data stored in a shared cloud server that may harm other clients.

Courts may also define inaccessibility under Judge Scheindlin's standard set out in *Zubulake v. UBS Warburg LLC*, which initially focuses on the location of the data before deciding whether producing the information would be unreasonably burdensome or costly.[190] Under this approach, accessibility will then depend on the media on which it is stored and whether the requested data is located on: (1) active, online data; (2) near-line data; (3) offline storage/archives; (4) backup tapes; or (5) erased, fragmented, or damaged data.[191] If the data falls into any of the first three categories, the data will be deemed accessible and the request will be granted, regardless of any need for such information or the burden or cost to the producing party.[192] A litigant will not be able to argue that data is inaccessible under this approach if the requested information involves active, online or near-line data stored in a cloud server that is physically located in a jurisdiction that prohibits transfer of information out of the country to the United States. In addition, if a litigant is able to demonstrate inaccessibility, under *Zubulake*'s good cause analysis, a court will focus on the cost burden on a responding party instead of

does not consider cost shifting. FED. R. CIV. P. 26(b)(2) Advisory Comm.'s Notes to 2006 Amend.

189. *Id.*

190. *Zubulake*, 217 F.R.D. at 320; s*ee also* Johnson v. Neiman, 4:09CV00689 AGF, 2010 WL 4065368 (E.D. Mo. Oct. 18, 2010) (relying on *Zubulake* to determine accessibility); Helmert v. Butterball, LLC, No. 4:08CV00342 JLH, 2010 WL 2179180, at *8 (E.D. Ark. May 27, 2010) ("Reasonable accessibility is best understood in terms of whether the ESI 'is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production).'") (citing *Zubulake*, 217 F.R.D. at 318); Major Tours, Inc. v. Colorel, No. 05-3091(JBS/JS), 2009 U.S. Dist. LEXIS 97554, at *10 (D.N.J. Oct. 20, 2009) (relying on *Zubulake* to determine accessibility).

191. *Zubulake*, 217 F.R.D. at 318–20.

192. *Id.* at 319-20; *see also* Major Tours, Inc. v. Colorel, 2009 U.S. Dist. LEXIS 97554, at *10 (citing *Zubulake*, 217 F.R.D. at 319-20) ("[T]he Court notes that the requested data is maintained on defendants' backup tapes. This storage media is typically classified as inaccessible.").

other burdensome considerations.[193] Therefore, the difficulties producing fragmented, intermingled, and inseparable data from a public cloud may not be convincing enough to overcome the good cause burden under this approach. Complications with jurisdictional data transfer restrictions or a cloud provider's loss of data also may be insufficient.

These different approaches to proportionality may have implications for cloud discovery. Depending on the approach, it may be more difficult to demonstrate an unreasonable burden and dispute good cause with production of ESI stored on a cloud. If location and costs are the sole considerations as to whether there is an unreasonable burden, litigants may face problems with readily accessible data they cannot retrieve due to jurisdictional rules.[194] This is further complicated because most people are unfamiliar with cloud technology and may believe the ease of accessing information stored in a cloud means production will be as simple. However, under either approach, litigants may have difficulties producing readily accessible common metadata stored in shared servers that may harm other clients.[195] Likewise, there may be issues with embedded data not reasonably accessible in which the intermingling of data with other clients' data prevent production.[196] The litigant may find their cloud provider unwilling to produce the requested ESI as mandated by a court. This third-party resistance may not be excusable either, since courts generally find a party has control over data stored with a third party.[197] Courts may be further unsympathetic and find the

193. The court will apply either the good cause factors stated under Rule 26 (b)(2)(C) of the Advisory Committee's Note to Rule 26. *See* Johnson v. Neiman, 4:09CV00689 AGF, 2010 WL 4065368, at *1-2 (E.D. Mo. Oct. 18, 2010) (applying the Advisory Committee's Note to Rule 26 to find no good cause to order production as the estimated cost to produce the request would have been $76.03 per hour); Major Tours, Inc. v. Colorel, No. 05-3091JBSJS, 2009 WL 3446761, at *4-5 (D.N.J. Oct. 20, 2009) (deciding the court will not order defendants to conduct an ESI search because the expense outweighs its likely usefulness).

194. *See supra* Part II.B.3 (discussing international data transfer restrictions).

195. *See supra* Part II.B.3 (discussing issues of intermingled data in public cloud models).

196. *Id.*

197. *See* Nycomed U.S. Inc. v. Glenmark Generics Ltd., No. 08-CV-5023 CBA RLM, 2010 WL 3173785, at *7 (E.D.N.Y. Aug. 11, 2010) (holding responding party had control over documents stored with a third party); Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494, 515 (D. Md. 2009) ("Rule 34 'control' would not require a party to have legal ownership or actual physical possession of any documents at issue."); Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007) (holding responding party had control over data as they could not delegate their statutorily mandated preservation duties to a third party); *see also* N.J. Mfrs. Ins. Co. v. Hearth & Home Techs., Inc., No. 3:06-CV-2234,

responding party's decision to move their data into the cloud, and out of their physical control, to be at their own peril.[198]

Therefore, high costs of production will likely be a litigant's only way to avoid retrieval issues and meet the unreasonable burden standard under either proportionality approach. In *Procter & Gamble Co. v. Haugen*, the court found that while the responding party had ready access to data located on a third party server, production was an undue burden since the responding party would have either had to purchase a costly mainframe or pay the third party $30 million in order to obtain that data, which had been altered due to routine updates to the database.[199] However, while this case may offer hope to a litigant, *Procter* may be distinguishable since this case was decided in 2005-before the 2006 amendments to the Federal Rules. In addition, the *Procter* court found the data was in the control of the third-party server, even though the responding party had access to the information.[200] This is not the rule today.[201]

Depending on the cloud service and deployment models a company utilizes, production costs may vary. However, the more data there is in a litigant's cloud, the more it could cost to determine relevancy and privilege, "One terabyte of data can cost less than $100 to store but more than $1 million in litigation costs to collect, processes, review, and produce."[202] In a legal world where there are undefined burden and good cause standards, litigants may find it burdensome in itself to dispute production.

Furthermore, because the Rule 26 (b)(2)(B) proportionality provision only applies to *production* of data and not to preservation

---

2008 WL 2571227, at *7 (M.D. Pa. June 25, 2008) (forgoing a discussion regarding control, but nonetheless holding, "A plaintiff, particularly one who was represented by counsel prior to the spoliation, is not relieved of this responsibility merely because the plaintiff did not itself act in bad faith and a third party to whom Plaintiff entrusted the evidence was the one who discarded or lost it.").

198. Allison C. Stanton & Andrew J. Victor, *What We See in the Clouds: A Practical Overview of Litigating Against and on Behalf of Organizations Using Cloud Computing*, 59 U.S. ATTORNEYS' BULLETIN, no.3, May 2011, at 40 (citing Radian Asset Assurance, Inc. v. Coll. of the Christian Bros. of N.M., No. CIV 09-0885 JB/DJS, 2010 WL 4928866, at *1-2. (D.N.M. 2010) (holding the transfer of data from on-line network storage to near-line storage is a normal business function), *available at* http://www.umiacs.umd.edu/~oard/teaching/708x/spring12/readings/stanton2.pdf ("Courts may view cloud computing as a normal business function where the data cannot be made inaccessible when the organization should have known of potential E-Discovery needs when incorporating cloud computing into their systems.").

199. Procter & Gamble Co. v. Haugen, 427 F.3d 727, 739 (10th Cir. 2005).

200. *Id.* at 739–41.

201. *See supra* note 100 and accompanying text.

202. Stanton & Victor, *supra* note 198.

of data, litigants have to make costly efforts to meet their preservation duties.[203] Though a litigant decides production of ESI is not unreasonably accessible, the litigant is not relieved of "its common-law or statutory duties to preserve evidence."[204] In other words, there are no proportionality considerations for any unreasonable burdens or cost of preservation.

Although the price of electronic storage has decreased substantially with the cloud,[205] it may be expensive for litigants to search a cloud for potentially relevant information and to then purchase new litigant-controlled space to segregate it.[206] To do so, they will also have to monopolize the cloud provider's bandwidth and processing capacity.[207] In addition, while the per unit expense of storing ESI continues to fall, "much more information is also being created and saved, meaning that the overall cost of storage for many companies and organizations has not changed considerably."[208] In a recent interview with The Institute for the Advancement of the American Legal System, one Fortune 500 company reported spending approximately $1.4 million on outside vendor hosting costs in 2011 to preserve ESI for pending litigations.[209]

E. Cost Shifting

After a court determines the responding party must produce requested ESI stored on a cloud server, it may then consider cost shifting. While the "presumption is that the responding party must bear the expense of complying with discovery requests,"[210] a court has the discretion to shift all or part of the costs of production to

203. FED. R. CIV. P. 26(b)(2)(B).

204. FED. R. CIV. P. 26 Advisory Comm.'s Notes to 2006 Amend.

205. In 1999, the cost of physical data storage was $100 per gigabyte. It now costs less than $1 for a gigabyte and under $100 to store a terabyte of data. Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 143 (2008); Stanton & Victor, *supra* note 198. *See, e.g.*, *How Much Does Dropbox Cost?*, DROPBOX, https://www.dropbox.com/help/73/en (last visited July 24, 2012) (offering up to 18 gigabytes of cloud storage space for free); *Pricing Details*, WINDOWS AZURE, http://www.windowsazure.com/en-us/pricing/details/ (last visited July 24, 2012) (offering 1 gigabyte of cloud storage for a flat rate of $9.99 per month, which is approximately $0.32 a day).

206. Joseph A. Nicholson, *Plus Ultra: Third-Party Preservation in a Cloud Computing Paradigm*, 8 HASTINGS BUS. L.J. 191, 192 (2012).

207. To ensure data is protected from spoliation, the litigant will have to isolate their data for preservation and processing on their current cloud provider's servicers or move the data to a private IaaS cloud for handling. *Id.*; *supra* Part I.B.

208. NAVIGATING THE HAZARDS OF E-DISCOVERY, *supra* note 180, at 7.

209. *Id.*

210. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).

the requesting party.[211] However, most courts hold cost shifting is only appropriate when the requested data is inaccessible due to burden or cost.[212] Thus, depending on the proportionality approach used, a litigant may not even have a cost-shifting recourse for expensive production of data stored in a cloud.[213]

In addition, litigants may face an uphill battle for cost shifting because "courts thus far have been reluctant to shift the cost of that burden to the requesting party, sometimes explaining that the producing party is uniquely positioned to control the scope of those costs.[214] Courts may consider a litigant's use of cloud technology, which means the litigant will have the resources and ability to utilize new discovery technology to lower production expenses.[215] Regardless, new technology or methods to reduce discovery costs may not be able to significantly lower costs due to the overwhelming

211. Peskoff v. Faber, 251 F.R.D. 59, 61 (D.D.C. 2008) (citing *Oppenheimer*, 437 U.S. at 358).

212. Many courts rely on the Comments to Rule 26, which states, "The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible." FED. R. CIV. P. 26(b)(2) Advisory Comm.'s Notes to 2006 Amend. *See Peskoff*, 251 F.R.D. at 61 (holding cost shifting is only appropriate when inaccessible data is sought); OpenTV v. Liberate Techs., 219 F.R.D. 474, 476 (N.D. Cal. 2003) (citing Zubulake v. UBS Warburg LLC, et al., 216 F.R.D. 280, 284 (S.D.N.Y. 2003) ("Shifting the cost of production from the producing party to the requesting party should be considered only when inaccessible data is sought."). In contrast, some courts only analyze whether the cost of production represents such an undue burden or expense to justify cost shifting or courts that only consider fairness and efficiency when determining whether to shift costs. *See* Haka v. Lincoln Cnty., 246 F.R.D. 577, 579 (W.D. Wis. 2007) (concluding fairness and efficiency, rather than any formal balancing test, required the parties split e-Discovery search costs evenly, with the producing party paying the full cost of the privilege/relevance review).

213. Under the *Zubulake* proportionality standards, since inaccessibility is determined by data source, cost shifting is only considered when the requested ESI is located on backup tapes or erased, fragmented, or damaged data. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 319–20 (S.D.N.Y. 2003).

214. Mia Mazza et. al., *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 RICH. J.L. & TECH. 11, 125 (2007).

215. *See* NAVIGATING THE HAZARDS OF E-DISCOVERY, *supra* note 180, at 12 (internal citations omitted) ("New technology continues to be developed to assist in reviewing and analyzing electronically stored information. New programs are being developed to assist in reducing the amount of data early in the process so that overall costs of review and production can also be reduced. Technological advancements are also lessening the burden and cost of restoring backup tapes."); Stanton & Victor, *supra* note 198 ("[W]ith advances in technology, smarter automated tools will be able to help alleviate this problem by increasing efficiency when reviewing large volumes of information in the cloud. The potential help these tools provide becomes available if one has access to these resources. The investment in and access to litigation technology in handling the data in discovery may, however, very well lag behind the rise in storing data in the cloud.").

amount of ESI generated in a cloud.[216] Furthermore, currently, the main focus of cost shifting continues to be production costs.[217] This poses a problem as exercising control over and preserving cloud-stored data may result in significant costs, which a court will not consider shifting to the requesting party.[218] Negligence by a third-party cloud provider also creates an expensive burden for the responding party when collecting, processing, and producing ESI.[219]

III. Practical Solutions to Cloud Discovery

Because of the intricacies of cloud computing and problems with third-party control of ESI, companies should be familiar with their cloud provider's services before contracting with them, should specify litigation and discovery procedures in their cloud service agreement, and meet and confer with opposing counsel early on to reduce expensive preservation burdens.

A. Know Your Cloud

Being familiar with cloud technology and how the cloud works allows a company and their attorneys to understand the implications of their cloud use during litigation. Knowing the differences between cloud providers and the numerous possibilities of the different cloud computing model combinations may assist counsel in learning about their client's cloud. Further, a company will then be able to contract for such implications in their service agreement.

If an attorney is representing a company already contracted with a cloud provider, the attorney should work closely with the company's IT staff to understand what kind of cloud infrastructure the company uses (i.e., SaaS versus IaaS or public versus private), what is stored in the cloud, what the terms of the service agreement are, and what data retrieval options and tools are available.[220] The attorney should then contact the cloud provider to learn whether the cloud provider adheres to the U.S. Safe Harbor Principles,[221] where

216. NAVIGATING THE HAZARDS OF E-DISCOVERY, *supra* note 180, at 12.

217. *See supra* text accompanying notes 208–09.

218. *See supra* text accompanying notes 208–09; Nicholson, *supra* note 206, at 214.

219. *See* Nicholson, *supra* note 206, at 216.

220. Stanton & Victor, *supra* note 198, at 42.

221. The EU has recognized companies adhering to the Safe Harbor Program as meeting the Directive's adequate level of protection standard to allow cross-border transfer of information out of Member States. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, *supra* note 169; Press Release, EUROPA, EU-U.S. joint statement on data protection by European Commission Vice-

the data is physically located and what the cloud provider's archival and retention capabilities are, such as whether the company even has access to its data.[222] The attorney should know whether the provider can integrate the company's retention policies to manually overwrite metadata and embedded data, whether the provider can pause its automatic deletion policies, and, if the company is not using a private cloud, whether the company's metadata and embedded data can be separated and compartmentalized from other clients.[223] The attorney should also be aware of whether the cloud provider offers discovery tools or is able to implement third-party discovery applications for use during litigation. Most importantly, the attorney should know whether the cloud provider would be cooperative during litigation when it has no contractual duty to do so.

If an attorney is representing a company planning to move to a cloud, the attorney should advise his or her client to consider contracting with a cloud provider that has a discovery-ready or

President Viviane Reding and U.S. Secretary of Commerce John Bryson (Mar. 19, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192&format=HTML&aged=0&language=EN&guiLanguage=en (last visited July 24, 2012) ("The EU and the United States remain dedicated to the operation of the Safe Harbor Framework–as well as to our continued cooperation with the Commission to address issues as they arise–as a means to allow companies to transfer data from the EU to the United States, and as a tool to promote transatlantic trade and economic growth."). *See also Rackspace Cloud Privacy Statement*, RACKSPACE, http://www.rackspace.com/cloud/legal/privacystatement/ (last visited July 24, 2012) (stating Rackspace is Safe Harbor certified).

222. SOARES, *supra* note 38, at 2–3.

223. For example, Google's new IaaS cloud service, Google Compute Engine (GCE) allows users to compartmentalize their data from other users. *Google Compute Engine*, GOOGLE DEVELOPERS, https://developers.google.com/compute/docs/faq#whatareprojects (last visited July 24, 2012) ("A project is a container for all Google Compute Engine resources. Each project is a totally compartmentalized world; projects do not share resources, can have different owners and users, are billed separately, and are not any more accessible to each other than your home computer is accessible to your neighbor's computer."). *See also CloudLock Protected Folders*, CLOUDLOCK, http://www.cloudlock.com/applications/cloudlock-vault/ (last visited July 24, 2012) (providing a data management application compatible with Google Apps with a "secure area in [a user's] Google Docs environment where documents are stored and cannot be deleted or modified"); *IBM SmartCloud Enterprise*, IBM, http://www-935.ibm.com/services/us/en/cloud-enterprise/object-storage.html (last visited July 24, 2012) (stating the IaaS provider keeps data intact instead of breaking user files down into chunks); Press Release, Nasuni, Nasuni Announces New Snapshot Retention Functionality in Nasuni Filer; Enables Fail-Safe File Deletion in the Cloud (Mar. 21, 2011), *available at* http://www.nasuni.com/news/press_releases/11-nasuni_announces_new_snapshot_retention (giving cloud users control over the cloud's deletion and retention policies).

enabled system in place.[224] If it is not practical for the client to do so,[225] the attorney should negotiate the cloud service agreement to the most discovery-ready extent possible.[226]

B. Stipulate a Litigation Plan

1. The Service Agreement

When contracting with a cloud provider, know that the company has the upper hand in negotiations. However, clouds are a service industry and there are numerous cloud providers willing to alter their service agreements for a potential client's needs.[227]

The company should first discover whether the provider follows any data integrity standards that can track data from entry through its movements through the cloud server.[228] If it does not, the contract

224. *See, e.g.*, *Google Apps for Business*, GOOGLE, http://www.google.com/intl/en/enterprise/apps/business/products.html (last visited Sept. 4, 2012) (providing e-discovery-ready systems).

225. *See supra* Part I.B.1 (discussing how some companies lack the resources or need to contract for a IaaS or PaaS cloud model, and are best serviced by using a ready-to-employ SaaS cloud service model, which may not be negotiable). *See also, e.g.*, *Create an Account*, DROPBOX, https://www.dropbox.com/register (last visited Sept. 4, 2012) (requiring that a user agree to their terms before allowing them to create an account).

226. Some SaaS cloud service providers that generally use a standard nonnegotiable service agreement may be willing to negotiate a contract. *See Create an Account*, GOOGLE, https://accounts.google.com/NewAccount (last visited Sept. 4, 2012); *Google Apps for Business*, *supra* note 224 (allowing potential users to contact the Sales Department and customize their services). *See also* Amir Efrati, *Google Wins U.S. Contract*, WALL ST. J. (May 1, 2012), http://online.wsj.com/article/SB10001424052702304868004577378411430202238.html (discussing Google's new contract with the U.S. Department of Interior).

227. *See* W. Kuan Hon, Christopher Millard & Ian Walden, Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now (May 9, 2012) (unpublished Legal Studies Research Paper, Queen Mary University of London, School of Law), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199 (interviewing global cloud providers, cloud users, and law firms to discover the extent to which cloud providers will negotiate service agreements and finding that "market participants [are] developing a range of cloud services with different contractual terms, priced at different levels, and embracing standards and certifications that aid legal certainty and compliance").

228. W. Scott Blackmer, *Data Integrity and Evidence in the Cloud*, INFO. LAW GRP. (Jan. 29, 2010), http://www.infolawgroup.com/2010/01/articles/cloud-computing-1/data-integrity-and-evidence-in-the-cloud/ (discussing various cloud data integrity standards, "The SNIA Cloud Data Management Interface (CDMI) specification and other SNIA cloud storage standards, the Data Integrity Field (DIF) standard (which, among other things, verifies input-output addresses to avoid misplacing data entered in the cloud), WS-Reliability (an OASIS standard for reliable message delivery in web services) and WS-Transaction (OASIS protocols for coordinating distributed applications), as well as XML-based solutions that add some transaction management functionality to web applications").

should include language adopting a detailed method of data tracking, such as how metadata will be created, stored, relocated, and deleted. If a litigant is concerned with encountering any jurisdictional transfer prohibitions, and the cloud provider does not adhere to the U.S. Safe Harbor Program's transfer protection standards, the litigant may choose to stipulate that the data only be stored and processed in countries that do not have data transfer restrictions.

Next, the contract should incorporate language detailing the cloud provider's preservation duties for the purpose of e-discovery. There should be a provision triggering the cloud provider's preservation duty upon receiving a litigation hold notice from the client. This provision should address how the cloud provider should comply with the litigation hold. In situations where the cloud service is shared with others, the contract should provide for a method of separating and preserving the client's metadata and embedded data from other clients. The cloud provider should also agree to freeze its automatic deletion policies and, likewise, its automatic replication and backup practices upon notice. The contract should further stipulate a timeframe within which the cloud provider has to complete all litigation hold procedures.[229]

The service agreement should then stipulate the cloud provider's production duties for the purpose of e-discovery. This provision should stipulate a timeframe within which the cloud provider has to provide production.[230] If the company fears that it will encounter jurisdictional problems trying to retrieve their data, the contract should require that the company's ESI only be stored within the United States, or the company should seek a cloud provider that is safe harbor certified.[231]

The Agreement should also stipulate procedures for when the cloud provider receives a third-party Rule 34 subpoena, search warrant, or other lawful request for user information.[232] The provision should require that the cloud provider give the client prompt notice and details of the subpoena. The agreement should then detail how the client may access the data in the cloud; how the

229. SOARES, *supra* note 38, at 3.

230. *Id.*

231. *See Rackspace Cloud Privacy Statement*, *supra* note 221 and accompanying text.

232. Robert McHale, *Cloud Security and Privacy: A Legal Compliance and Risk-Management Guide, Part 1*, INFORMIT (May 3, 2010), http://www.rmchale.com/publications/CloudSecurityandPrivacy_ALegalComplianceandRiskManagementGuide.pdf(discussing privacy risks that may arise if a cloud provider receives a lawful request for information).

cloud provider plans to respond; who will bear the costs associated with processing data for a response; and whether the cloud provider will seek a protective order to limit or prevent disclosure of the company's data.[233]

To mitigate risks of data loss if another company acquires the business, the service agreement should state that the contractual provisions would continue to remain in force with the new company. The contract should also stipulate that the company will provide notice if it plans to file for bankruptcy or dissolve. The agreement should specify a timeframe as to when notice is required. To mitigate risks of accidental or unforeseeable data loss, the company should consider requiring the provider to regularly back up its data at the company's own site.[234]

2. Example Service Agreement Language[235]

Below is an example of language that may be included in a company's Service Agreement with a cloud provider. This language is not intended to substitute for a complete cloud service agreement,[236] but to provide a simple overview of some potential negotiating points:

> 1. Customer Data.
>
> 1.1. The Customer Data belongs to Customer, and Cloud Provider makes no claim to any right of ownership in it.
>
> 1.2. Cloud Provider must keep the Customer Data confidential in accordance with Section 2 of this Agreement.
>
> 1.3. Cloud Provider must compartmentalize and keep separate Customer Data from other customers utilizing Cloud Provider's services.

233. Tanya L. Forsheit, *E-Discovery Involving Cloud*, 1010 PLI/Pat 157, 170-71 (2010); McHale, *supra* note 232.

234. *See* Robert L. Scheier, What to Do if Your Cloud Provider Disappears, InfoWorld (April 20, 2009), http://www.infoworld.com/d/cloud-computing/what-do-if-your-cloud-provider-disappears-508 ("Intuit's QuickBase Desktop service, for example, lets customers back up their data from QuickBase onto a local Microsoft Access database as often as they like.").

235. This author relied on an assortment of agreements in the drafting of this section. *See Sample RightNow Technologies Master Cloud Services Agreement with Customer*, RIGHTNOW,http://www.rightnow.com/RightNow_Cloud_Services__Agreement_Sample.pdf (last visited July 24, 2012); *AWS Customer Agreement*, *supra* note 121.

236. This is especially so since a cloud provider will generally provide the service agreement. At best, the user may be able to negotiate the terms of the form contract. In addition, since every cloud user has different needs, the user should contract according to their own company-specific requirements. For practical purposes, this example agreement language only includes language related to issues discussed in this article and is not all inclusive of what should be stipulated in a user's service agreement with a cloud provider.

1.4. Cloud Provider must take reasonable technical and organizational measures to keep personal data secure and to protect it against accidental loss or unlawful destruction, alteration, disclosure or access; and, must deal with the information only in accordance with Customer's instructions, provided they are reasonable and lawful.

1.5. Cloud Provider must comply with Customer's company retention policy, as it relates to Customer's Data and purge - not just merely mark files for deletion - data Customer has identified for destruction. This includes, and is not limited to, backed up, fragmented, metadata, and embedded data.

2. Security and Data Privacy

2.1. The Customer Data may include privileged information, confidential information, or valuable trade secrets that are the sole property of Customer. Cloud Provider must take reasonable care to prevent against accidentally or unlawful loss, access, or disclosure of Customer Data.

2.2. Customer may specify the regions in which Customer Data will be stored and accessible by End Users. Cloud Provider will not move Customer Data from the selected regions without notifying Customer, unless required to comply with the law or requests of governmental entities.

2.3. Upon receiving a Subpoena for Customer's Data, Cloud Provider will promptly notify Customer and provide details of the Subpoena.

2.3.1. Cloud Provider will disclose to Customer how Cloud Provider intends to respond to the Subpoena.

2.3.2. Upon Customer request, the Cloud Provider will seek a protective order to limit or prevent disclosure of Customer's Data.

2.3.3. Cloud Provider will bear all costs associated with processing data for response. However, Customer shall bear all costs of a protective order.

3. Third-party Claims

3.1. Upon receiving a Litigation Hold Notice of a third-party claim, Cloud Provider has an obligation to immediately secure and preserve the identified Customer Data. Customer will have access to the server(s) preserving this Customer Data to process and collect Data as needed.

4. Termination and Suspension.

4.1. Customer may terminate this Agreement for any reason by (i) providing Cloud Provider notice and (ii) closing Customer accounts for all Services, for which Cloud Provider will provide an account closing mechanism. Cloud Provider may terminate this Agreement for any reason by providing Customer 30 days advance notice.

4.2. Either party may terminate rights granted under a particular Agreement if the other breaches any material term of

> the Agreement and the breach is not cured within 30 days of written notice. Customer's breach of the Conditions and Use section of this Agreement shall be considered a material breach.
>
> 4.3. Instead of terminating rights granted to a Customer under this Agreement, Cloud Provider may suspend the provision of Services to Customer for a period of up to 45 days. At any time during that period, Cloud Provider may terminate the rights granted to Customer.
>
> 4.4. Sections 1.1, 1.2, 1.3, 2.1, and 2.2 continue after this Agreement ends.
>
> 4.5. If Cloud Provider terminates this Agreement voluntarily or for cause, upon termination of Customer's Subscription Service, Cloud Provider must promptly provide Customer with all Customer Data in comma separated value (CSV) format. However, Cloud Provider must retain Customer Data in backup media for an additional period of up to 12 months, or longer if required by law. After such retention, Cloud Provider must fully purge – not merely mark for deletion – all remaining Customer Data.
>
> 4.5 If Customer terminates this Agreement, upon termination of Customer's Subscription Service, Cloud Provider must promptly provide Customer with all Customer Data in comma separated value (CSV) format. Cloud provider must promptly purge—not merely mark for deletion—all remaining Customer Data. This includes, and is not limited to, backed up, fragmented, metadata, and embedded data.

C. Meet and Confer

Though drafting a service agreement with specific discovery provisions will significantly reduce the burden on a litigant, the litigant may still have a sizeable preservation and production burden. To save costs and headaches, the litigant should meet and confer with opposing counsel as soon as possible to discuss discovery-specifically regarding discovery of ESI stored in a cloud. If possible, both parties' IT personnel should be present to explain how the parties' clouds work and any difficulties there may be with discovery.[237] With this knowledge, parties may be more inclined to believe opposing counsel is not hiding a "smoking gun" in certain forms, such as metadata or

237. Opposing counsel may be more willing to trust a company's IT staff than the company's lawyer. This is especially so if opposing counsel's own IT staff is present to confirm the accuracy of the information. However, if parties do not wish to involve IT staff, the litigants should instead know the technology and potential e-discovery problems and be prepared to explain and discuss the information themselves.

embedded data, and agree to limit their requests to more easily preserved and produced ESI.

If the litigant wants to facilitate a productive 26(f) conference but fears opposing counsel will be uncooperative, the litigant should send opposing counsel a letter with a list of cloud e-discovery issues, among others, to discuss at the conference.[238] This letter should invite opposing counsel to be knowledgeable and prepared regarding these issues in order to facilitate and streamline discovery. In addition, this notice letter should be sent as soon as the litigation schedule is set, to give both parties time to prepare and so there is a record of the litigant's efforts to cooperate. If opposing counsel does not agree to this cooperation, the party appears unreasonable-conduct a court may find sanctionable.[239] Therefore, a notice letter will likely ensure opposing counsel will be prepared to discuss cloud e-discovery issues.

D. Educating the Court

It is the worst-case cloud e-discovery scenario: the litigant's company did not plan accordingly for e-discovery before signing their cloud provider's service agreement, the cloud provider refuses to cooperate with the litigant, and opposing counsel refuses to restrict the scope of discovery. In this nightmare situation, the litigant's best option is to demonstrate to the court that the litigant is attempting to reasonably comply with discovery. The litigant may do so by holding a tutorial before the court and opposing counsel, explaining how their cloud works and the difficulties the litigant may face trying to comply with discovery obligations.[240] This tutorial should be conducted early in litigation to help address potential disputes that may arise later.[241] While there is still the risk that the judge will be unsympathetic, by educating the court, the litigant increases the chance of the judge being more understanding if spoliation does occur.

---

238. The author would like to thank the Honorable Craig Shaffer for recommending this solution. Interview with Magistrate Judge Craig Shaffer, U.S. Dist. Court for the Dist. of Colo., in Denver, Colo. (July 9, 2012).

239. A court may sanction a party under Rule 16(f) if the party or its attorney "does not participate in good faith" in the pretrial conference. FED. R. CIV. P. 16(f)(B). A court may also sanction a party under Rule 37(f) for failing to "participate in good faith in developing and submitting a proposed discovery plan as required by Rule 26(f)." FED. R. CIV. P. 37(f).

240. Jonathan Redgrave, Panel Discussion at the Inst. for the Advancement of the Am. Legal System eDiscovery Boot Camp: an Educational Summit for State Court Judges (June 23, 2012).

241. *Id.*

IV. Conclusion

Although e-discovery disputes do not arise in the majority of litigation, with the growing use and reliance on cloud technology, this may not always be the case. The issue is especially complicated because of a third party's physical control of the cloud and intricate advancements in cloud technology. Clients and their counsel should not limit themselves to only an IaaS-based private cloud system due to fear of discovery, as this is neither practical nor necessary. Instead, clients and their counsel should (1) be aware of the difficulties litigating in the cloud era and plan accordingly with specific service agreements; (2) ensure their cloud provider has tools equipped to handle discovery or can accommodate another third party's discovery management application; and (3) be prepared to demonstrate reasonable discovery compliance in worst-case scenarios.

***