Hastings Business Law Journal

Volume 8
Number 1 *Winter 2012*

Article 6

Winter 1-1-2012

Plus Ultra: Third-Party Preservation in a Cloud Computing Paradigm

Joseph A. Nicholson

PLUS ULTRA: THIRD-PARTY PRESERVATION IN A CLOUD COMPUTING PARADIGM

*Joseph A. Nicholson**

I. INTRODUCTION

> "This is a story about control . . . to get what I want. Control. I have to have a lot."
>
> – Janet Jackson

A natural disaster strikes and, eventually, a devastated homeowner is visited by an insurance adjuster. Though the insurer typically requires the insured to submit a formal request, the claims adjuster assures the homeowner that he will file the request on her behalf. On his way to the next insured, the adjuster enters notes about his meeting onto a remote server through his handheld PDA. Ultimately, the adjuster is consumed with other potential claims and forgets to file their claim. The insurer refuses to pay and the insured files suit, claiming promissory estoppel and detrimental reliance.

During discovery, the plaintiff learns of the electronic notes created by the adjuster and requests a copy. But the insurer does not retain copies of this class of data in its own possession. As part of a growing trend towards cost-cutting and other efficiencies, it has rented large amounts of server space to store and process this type of information, and to provide the very mobility that allowed the adjuster's timely visit. Now faced with a formal production request, the insurer learns the notes are nowhere to be found. As far as can be determined by the remote computing service provider, the file was accidentally mislabeled and is deleted or lost. Or, says the vendor, it might have been located on a server that was recently seized by federal agents in an unrelated matter.[1] No matter what the cause, the insurer

* J.D. Candidate, 2012, University of California, Hastings College of the Law. This work would not have been possible without the patience and insight of Professor Richard Marcus and Chris Mammen, for which the author is most appreciative. Special thanks are also due to Emily A. Cobb of Ropes & Gray LLP, and Vicki Clewes, both of whom gave graciously of their valuable time and considerable knowledge.

1. Or perhaps imagine instead that the complaint includes allegations of fraud and unfair business

cannot produce the requested record because it is simply gone.[2] It has been spoliated.[3]

Who is to blame in this scenario? Who was in control of the lost information? What, if anything, can be inferred from the disappearance of the evidence? Who, if anyone, gets sanctioned for its spoliation? Can the nonparty cloud computing vendor be sanctioned? Or should the plaintiff's case be dismissed because she cannot establish the existence of a promise? Should the defendant or the defendant's counsel be sanctioned instead?

The duty of a party to preserve potentially relevant information attaches at the point at which litigation becomes reasonably foreseeable,[4] meaning the duty for a party can arise years before litigation actually commences.[5] But when that party's information is stored remotely on the servers of a vendor, the typical expectations of preservation take on new and challenging dimensions. How effectively can outside counsel devise, and in-house counsel enforce, a litigation hold for data stored in the cloud? How costly is it to search the cloud for potentially relevant information and purchase new space on which to segregate it? How burdensome is it to monopolize bandwidth and processing capacity to download the data for local storage?

As information and, presumably, responsive documents increasingly move into the actual custody of third parties, the business community and the legal system will face the reality that third-party computer systems not only multiply the number of documents and copies that are created and retained, but also inadvertently destroy, alter, or misplace information. Just as the technical uniqueness of electronically stored data must be recognized in fashioning controlling discovery standards, so too should sanctions be tailored to the electronic context if the values sought to be furthered by

practices against various employees and executives of the insurer. A copy of the adjuster's note referring to his promise has been produced, but a reliable version of the metadata that would prove which employees accessed the notes and when, cannot be found or simply does not exist.

2. A further complication would arise if the only remaining evidence of the adjuster's notes was information about his access to the cloud that existed as proprietary data created by the vendor. The record could be enough to justify an adverse inference against the insurer, but its discovery might be opposed by the vendor as confidential. This could be complicated further still if the proprietary record was not possessed by the vendor but another third-party company providing services directly through the vendor's platform.

3. Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010) [hereinafter *Pension Committee*]; Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001). Though some prefer to use "spoliation" purely for the destruction of evidence, the definition in *Pension Committee* would seem to include scenarios in which evidence is not produced because it cannot be identified through reasonable means and those in which the data has lost its probative value for having been materially altered by automatic electronic processes.

4. Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

5. Micron Tech., Inc. v. Rambus Inc., 255 F.R.D. 135, 148 (D. Del. 2009).

litigation are to be respected.[6] Unless cloud service providers accept a particular contractual obligation to preserve information in dispute, they are likely to escape repercussions from the destruction of the crucial data even when they are the key player in its loss. Both the party contracting with the vendor and their opposition have a stake in preventing this undermining of the basic truth-finding goal that is the foundation of the litigation process.[7]

After amending the discovery rules in 2006, rulemakers are considering further changes and at least one magistrate judge has emphasized the need for any new e-discovery rule to be forward-looking enough to anticipate the cloud computing environment.[8] In the current absence of such a preservation rule, however, this note outlines some of the currently existing means by which businesses and their counsel can approach preservation of ESI in the cloud when needed for litigation. Section II provides an overview of the cloud computing paradigm and the emergence of third parties as the actual and practical custodians of data. The third section outlines some of the basic challenges to discovery in the cloud, where litigants simply have less practical control of data than they might otherwise have if the information was stored locally or in hard copy. This section examines how current litigation tools aimed at compelling production by third parties have little use in encouraging preservation. Finally, section IV discusses how terms of service agreements can ease some of the tension, but typically only at the cost of essential cloud computing benefits, and previews some implications of applying the principle of proportionality in preservation.

II. PRESERVATION CHALLENGES OF THE CLOUD COMPUTING PARADIGM

In rejecting an independent tort of spoliation against parties to an underlying lawsuit in California, the state's Supreme Court said in 1998 that non-tort remedies for spoliation were apparently effective since "the problem of spoliation does not appear to be widespread."[9] But it appears that, as technological advances in electronically stored information ("ESI")

6. H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 619 (2001). According to renowned author and futurist Bruce Sterling, electronic storage is unique in that it is "inherently unstable." Kari Kraus, *When Data Disappears*, N.Y. TIMES, (Aug. 6, 2011), http://www.nytimes.com/2011/08/07/opinion/sunday/when-data-disappears.html?_r=1.

7. *See* Redish, *supra* note 6, at 600; FED. R. CIV. P. 1 (the resolution of every action should be "just").

8. *E-Discovery: Discussion of the Cost Benefit Analysis of E-Discovery and the Degree to Which the New Rules are Working or Not*, CIVIL LITIGATION CONFERENCE (May 11, 2010) (downloaded using RealPlayer) (Magistrate Facciola dedicating his remarks to the singular point that the cloud computing paradigm represents the future of information technology and e-discovery and that, therefore, any new preservation rule must be designed for and tested against this emergent reality).

9. Cedars-Sinai Med. Ctr. v. Super. Ct., 954 P.2d 511, 518 (1998).

have revolutionized business, they have also exacerbated a once judicially manageable problem into a challenge of entirely new proportions. Just twelve years later, Judge Rosenthal of the Southern District of Texas began his exposition on the topic in *Rimkus Consulting Group, Inc. v. Cammarata* by stating, "[s]poliation of evidence—particularly of electronically stored information—has assumed a level of importance in litigation that raises grave concerns."[10] Indeed. A study presented at the 2010 Civil Litigation Conference and published in the Duke Law Journal found that there were more e-discovery sanctions cases in 2009 than in all years prior to 2005 combined.[11] The same study identified a total of 230 sanctions awarded just for spoliation of ESI in the federal court system before the start of 2010.[12] Though Gibson, Dunn, & Crutcher reports that fewer of the total e-discovery sanctions sought in 2010 were granted than in 2009,[13] the first half of 2011 nevertheless saw a particularly brow-raising sanction awarded for egregious e-discovery abuse[14] and something approaching a "three strikes" rule for bad faith failure to disclose.[15] Another recent survey shows Facebook is a source of evidence in one of every five divorce cases.[16] A report by Deloitte finds that lawyers expect e-discovery will be even more challenging in the near future,[17] suggesting this is not the end, nor even the beginning of the end of our grappling with e-discovery, but perhaps the end of the beginning.

10. *Rimkus Consulting Group, Inc. v. Cammarata* 688 F. Supp. 2d 598, 607 (2010).

11. Dan H. Willoughby et al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 DUKE L.J. 789, 794 (2010).

12. *Id*. at 790.

13. *2010 Year-End Electronic Discovery and Information Law Update*, GIBSON, DUNN & CRUTCHER (Jan. 13, 2011), http://www.gibsondunn.com/Publications/Pages/2010YearEndE-Discovery-InformationLawUpdate.aspx.

14. Green v. Blitz U.S.A., Inc., No. 2:07-CV-372 TJW, 2011 WL 806011, at *10–11 (E.D. Tex. Mar. 1, 2011) (defendant ordered to pay $250,000 civil contempt fine as well as provide copy of sanctions order to every plaintiff in a proceeding against it for the previous two years and to file a copy of the order in every case brought before the court in the next five years.).

15. Lee v. Max Int'l, L.L.C., 638 F.3d 1318, 1321 (10th Cir. 2011) ("[A] party's thrice repeated failure to produce materials that have always been and remain within its control is strong evidence of willfulness and bad faith, and in any event is easily fault enough, we hold, to warrant dismissal or default judgment.").

16. *Facebook Fueling Divorce, Research Claims*, TELEGRAPH, (Dec. 21, 2009, 1:02 PM) http://www.telegraph.co.uk/technology/facebook/6857918/Facebook-fuelling-divorce-research-claims.html; *Big Surge in Social Networking Says Survey of Nation's Top Divorce Lawyers: Facebook is Primary Source for Compromising Information*, AM. ACAD. OF MATRIMONIAL LAWYERS, (Feb. 10, 2010) http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social-networking-evidence-says-survey-.

17. *E-Discovery: Mitigating Risk Through Better Communication*, DELOITTE (2010), http://www.deloitte.com/assets/DcomUnitedStates/Local%20Assets/Documents/FAS_ForensicCenter_us_fas-us_dfc/us_dfc/us_dfc_e_discovery_survey_final_061710.pdf.

A. THE CLOUD COMPUTING PARADIGM

Waxing philosophical in the famous case of *Zubulake I*, District Judge Shira Sheindlin noted, "The world was a far different place in 1849, when Henry David Thoreau opined (in an admittedly broader context) that '[t]he process of discovery is very simple."[18] Unfortunately for litigants, their counsel, and the courts, the world is a very different place today than it was in 1999 or in 2003—and it is likely to be significantly more different five or ten years into the future. For one thing, the backup tapes that are seemingly ubiquitous in the e-discovery disputes of just five or ten years ago, though still in use, have been superseded by CD-ROM, DVD, Blue-Ray, hot-swappable flash drives and, increasingly, online backup.[19] While not new, the emergence of cloud computing in particular represents a paradigm shift[20] that has already revolutionized social networking and is forecast to have a profound ongoing impact on IT organizations,[21] law firms and corporate law departments,[22] health care providers,[23] and the corporate world in general.[24] The increasing functionality of the Internet is decreasing the role of the personal computer, which is reversing the trend towards a decentralized computing environment.[25] In the words of CNET News Editor in Chief Dan Farber, 2008 marked only the beginning of "the age of planetary computing" in which "billions of people will be wirelessly interconnected" by a "massive scale, brutally efficient cloud-based infrastructure."[26]

18. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003).

19. George Ou, *Are Tape Backup Systems Obsolete?*, ZDNET (July 10, 2006), http://www.zdnet.com/blog/ou/are-tape-backup-systems-obsolete/267; Maxim Yurin, *The History of Backup*, SOFTLOGICA http://www.backuphistory.com/ (last visited Sept. 22, 2011); *see also E-Discovery: Discussion of the Cost Benefit Analysis of E-Discovery and the Degree to Which the New Rules are Working or Not*, *supra* note 8.

20. *Enterprise Cloud Services: Deriving Business Value From Cloud Computing*, WHITE PAPER (2008) *available at* http://cloudservices.microfocus.com/main/Namespaces/MFECS/doc/MFECS-WP-deriving-business-value.pdf; Venkat Rangan, *E-Discovery and the Cloud: The Duty to Preserve Electronically Stored Information (ESI)*, E-DISCOVERY 2.0 (May 28, 2010), http://www.clearwellsystems.com/e-discovery-blog/2010/05/28/e-discovery-and-the-cloud-the-duty-to-preserve-electronically-stored-information-esi/.

21. Michael Biddick, *Why You Need a SaaS Strategy*, INFO. WEEK (Jan. 16, 2010), http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=222301002.

22. David Narkiewicz, *Legal Tech Forecast: Cloudy, With Only a Chance of Purchasing New Software*, 32 PA. LAW 56, 56 (2010).

23. Chris Chatman, *How Cloud Computing is Changing the Face of Health Care Information Technology*, 12 NO. 3 J. HEALTH CARE COMPLIANCE 37, 37-38 (2010).

24. William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software As a Service Agreement*, 66 BUS. LAW 237, 242 (2010).

25. William J. Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L. J. 1195, 1199–1200 (2010).

26. Bill Farber, *Cloud Computing Hangover*, CNET NEWS (June 26, 2008 10:35 AM), http://news.cnet.com/8301-13953_3-9978153-80.html.

The quintessential feature of cloud computing is that, rather than storing data on an individual computer or in onsite backups, high-speed Internet access is used to outsource this service, often to third-party providers.[27] In cloud computing, the user's individual computer accesses the cloud through the Internet in a manner reminiscent of the way a "dumb terminal" is used to access a mainframe.[28] In a growing number of companies, employees are no longer the custodians[29] of the records they produce—from their desks, laptops or handheld devices they access and manipulate documents and records that are stored remotely on third-party servers.

This cloud computing paradigm has emerged against a backdrop in which the federal courts have become increasingly attentive to the novel issues e-discovery creates in litigation. But despite the prodigious efforts already made by courts, individual judges, scholars and rulemaking bodies, third-party spoliation has been a relatively undeveloped area of e-discovery that seems to only now be receiving the serious attention it deserves.[30] Though the consequences of this oversight to date may be limited, it is particularly alarming given not just the proliferation of ESI, but the increasing rate at which potentially relevant and discoverable ESI will be in the hands of third-party service providers. As currently understood, parties to litigation are deemed to be in "control" of information to which they have access or the legal right to obtain, even if it is actually in the

27. Clouds can be either internal or external, and each type can further be classified as private, essentially an intra-net, or community-based, with access limited to specific groups or individuals. For this article, "cloud computing" will typically refer to public clouds in which third parties provide cloud computing services to businesses and the general public. *See* Peter Mell & Tim Grance, *Effectively and Securely Using the Cloud Computing Paradigm*, slide 11 (Mar. 13, 2009), http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud computing.pdf.

28. Robison, *supra* note 25, at 1199–1200.

29. The precise definition of "custodian" in this context is "somewhat tricky." *Agenda for April 2011 Meeting*, CIVIL RULES ADVISORY COMM., 12 (2011) *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Civil/CV2011-04.pdf. And what responsibilities are involved is troubling and convoluted in its own right. In the context of cloud computing, "custodian" can refer to the employee who creates and routinely access a file or the third-party storing it. To the extent that cloud service providers attempt to completely disavow any responsibility for preservation in their terms of service, service providers are probably best described as having possession of the ESI, while the employee or the party is charged with the preservation obligations of a custodian. This framework, however, still leaves open the question of control, which is from a practical perspective, probably the most significant.

30. *See, e.g.*, Greyhound Lines, Inc. v. Wade, 485 F.3d 1032, 1035 (8th Cir. 2007) (no sanction for third-party spoliation where intentional destruction is the requisite level of culpability). At least one commentator has observed an emerging consensus that the 2006 Amendments inadequately addressed the problems associated with e-discovery and that a rule addressing preservation and spoliation would be "a valuable addition to the Federal Rules." *See* Thomas Y. Allman, *Achieving a More Rational Treatment of Preservation Obligations: The Need to Amend The Federal Rules (Again)*, *in* ELECTRONIC DISCOVERY GUIDE 2010, at 140 (PLI Litig. & Admin. Practice, Course Handbook Ser. No. 23262, 2010). Discussion of such a rule was placed on the April 2011 agenda of the Civil Rules Advisory Committee. *Agenda for April 2011 Meeting*, *supra* note 29, at 205.

possession and custody of a third party.[31] The traditional custodian is often the employee or agent of the party who creates and accesses ESI locally, and therefore stores and preserves a record. Barron's legal dictionary suggests the word specifically implies not ownership, but a "keeping, guarding, care, watch, inspection, preservation or security of a thing."[32] Though the law does not recognize a vendor's duty to preserve data in its custody apart from the terms of service under which its services are offered, the nature of cloud computing appears to put the vendor in a position superior to the traditional custodian in terms of preservation and control.

One of the very reasons that the Internet was early depicted as a cloud is that, while it creates the potential to access a wide variety of interconnected resources, it also obscures what is available.[33] Far from the literal "series of tubes"[34] the Internet has been imagined to be, the very concept of network infrastructure is something of an abstraction based on complex interactions between servers, applications, data and heterogeneous platforms.[35] For example, mature cloud computing services employ a feature called multi-tenancy, which means that one application instance may be serving hundreds of companies simultaneously.[36] Rather than the service provider customizing an application, each user customizes their access via metadata.[37] While the fact that ESI is often recorded in multiple locations and in more than one medium may make it relatively rare that a particular piece of discoverable information is only available as ESI from a third party, locating and distinguishing and authenticating duplicate or slightly different versions typically occurs with considerable difficulty and expense.[38]

---

31. *See* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523–24 (D. Md. 2010).

32. BARRON'S LAW DICTIONARY 133 (6th ed. 2010). The Latin root *custodia* could refer to both a physical container in which something was placed for safekeeping or to the care itself shown towards the object.

33. Mell & Grance, *supra* note 27, at slide 7.

34. The phrase was famously coined by Sen. Ted Stevens on June 28, 2006, in a speech opposing net neutrality. Ted Stevens, Speech Regarding Net Neutrality (July 28, 2006), *available at* http://www.youtube.com/watch?v=f99PcP0aFNE. The phrase was mocked by Jon Stewart on *The Daily Show* roughly two weeks later. *The Daily Show With John Stewart* (Comedy Central Television broadcast July 12, 2006), *available at* http://www.thedailyshow.com/watch/wed-july-12-2006/headlines---internet. For a measured defense of Stevens, *see* Ed Felten, *Taking Stevens Seriously*, *Freedom to Tinker* (July 17, 2006, 7:21 AM), http://www.freedom-to-tinker.com/blog/felten/taking-stevens-seriously.

35. Mell & Grance, *supra* note 27, at slide 7.

36. *Id.* at slide 39.

37. *Id.*

38. Brandon M. Kimura & Eric K. Yamamoto, *Electronic Discovery: A Call For a New Rules Regime For the Hawaii Courts*, 32 U. HAW. L. REV. 153, 161 (2009); *but see Cryptographic Hash Algorithm Competition*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 15, 2005), csrc.nist.gov/groups/ST/hash/sha-3/index.html. The reduction of digital documents and images to a series of hash values that can be summed to produce a unique identifying value is a likely way that seemingly similar

The term "cloud computing" is a visual metaphor that conveys the versatility of the Internet.[39] The Internet is in fact the quintessential cloud computing service, consisting of a group of computer servers linked together and functioning as a single "cloud" of resources.[40] And, essentially, the cloud computing paradigm is nothing more than the realization of the Internet's full potential. Today, cloud computing services leverage international networks of computing resources, including applications, processing, storage, technical support, and technical infrastructure, with the result that data stored "in the cloud" can be located anywhere in the world and even shifted amongst servers depending on immediate demands.[41] In a 2011 survey of over 500 IT professionals, CTOs and developers, forty percent to fifty percent indicated current use of cloud-based solutions for product test and development, operation of data centers, increasing office productivity and email.[42] It will not be uncommon for a business or government agency to operate a call center staffed by employees who were selected through Internet staffing agencies like Salesforce.com, who access customer records stored on distant servers via Internet and who manipulate those records or create new ones that will also be stored remotely. The traditional notion that these operators are the ultimate custodians of these records seems inaccurate and unhelpful.

B. RISE OF THE THIRD-PARTY CUSTODIAN

If cloud computing is the way of the future, then that future will be a world in which much discovery involves "documents" in the custody of nonparties. While uniform definitions are elusive,[43] cloud computing typically refers to data and software applications that are stored in cyberspace on remote servers, rather than on the servers or PCs of the firms that use them.[44] Subsets of cloud computing include "software as a service" ("SaaS"), "infrastructure as a service" ("IaaS"), "platform as a service" ("PaaS"), and the perhaps more familiar social networking services of Web 2.0.[45] The essence of all forms of cloud computing is that the service provider allows its users to do their processing and storage of

pieces of ESI will be quickly distinguished or identified in the near future. Such algorithmic approaches, however, will probably not obviate the need for a document-by-document evaluation of similar electronic documents and evaluation of the differences in terms of relevance.

39. Mell & Grance, *supra* note 27, at slide 7.

40. Robinson, *supra* note 25, at 1199.

41. Barry Reingold & Ryan Mrazik, *Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part I)*, 14 NO. 5 CYBERSPACE LAW. 1, 1 (2009).

42. *Cloud Survey Results*, GOGRID, 6 (2011), http://go.gogrid.com/2011_survey_results.

43. Denny, *supra* note 24, at 237; Narkiewicz, *supra* note 22, at 56; *Cloud Survey Results*, *supra* note 42, at 3.

44. Narkiewicz, *supra* note 22, at 56.

45. Reingold & Mrazik, *supra* note 41, at 1.

information on its servers—reliance on the Internet to satisfy the computing needs of end users is the hallmark of the cloud computing paradigm.[46]

At the same time, these resources are massively scalable, meaning they can be custom fit to provide virtually any computing service needed.[47] Users can buy as much or as little computing, storage, processing and development power as they need without actually owning any of the hardware, software or technology expertise.[48] SaaS is already used for a variety of computing tasks, such as running spreadsheets, hosting websites, producing and keeping payroll records, compiling and storing data, and word processing.[49] PaaS and IaaS allow users to write software applications on a hosted web platform and rent network capacity, respectively.[50]

While this outsourcing of computing and storage presents obvious security challenges, its numerous advantages outweigh the risks for a growing number of businesses. Cloud computing has lower capital costs than on-site storage and computing, is quick and cheap to setup, and allows for employee mobility by making applications available at remote offices, on the road, via a smartphone, or from a home PC.[51] And though cloud computing is currently far from universal, it is difficult to imagine that the future workplace will not include a variety of cloud computing features. Already, about three-fourths of companies using SaaS consider these applications "extremely important" and about one-third describe them as "mission critical."[52] The scalability and pay-as-you-go features of cloud computing make it "cash-flow-friendly," an important factor in economic conditions where up-front funding is more difficult to obtain.[53]

To further compound the implications for e-discovery, government agencies are also implementing cloud computing technology to comply with mandates to cut costs and increase transparency—and they are advocating similar adoptions by private sector organizations.[54] In particular, the Department of Health and Human Services has already begun actively promoting and supporting a nationwide upgrade of health IT infrastructure by distributing grants for the creation of electronic health

46. Richard Stallman, *Who Does That Server Really Serve?*, Boston Review (Mar. 18, 2010), http://bostonreview.net/BR35.2/stallman.php; *Enterprise Cloud Services: Deriving Business Value From Cloud Computing*, *supra* note 20.

47. Reingold & Mrazik, *supra* note 41, at 1.

48. *Id.*

49. *Id.* at 2; Stallman, *supra* note 46.

50. Reingold & Mrazik, *supra* note 41, at 1–2.

51. Biddick, *supra* note 21; Chatman, supra note 23, at 37–38.

52. Biddick, *supra* note 21.

53. *Enterprise Cloud Services: Deriving Business Value From Cloud Computing*, *supra* note 20.

54. Chatman, *supra* note 23, at 37–38.

records ("EHR") systems.[55] Another emerging technology trend at least tangentially related to cloud computing also suggests probative information will be increasingly concentrated in the possession of companies or other organizations that will not necessarily be the parties to the dispute in which the information is relevant. So called "smart grid" technology in some states, like California, concentrates the end consumers' energy usage data in the utility company itself.[56] Because smart meters gather information about an individual home or locale's energy consumption virtually in real time, the ability to process and interpret the data gives unprecedented access into one of the traditionally most private spaces in life.[57] In other states, utilities are teaming with telecom companies who provide broadband transmission capacity and other edge services that require them to either purchase or directly gather data from electricity consumers.[58] In either event, it is already foreseeable that such information will be relevant in a variety of civil and criminal cases.[59]

For many individuals, however, social networking sites like Facebook, Twitter, and YouTube are probably the most recognizable facet of the cloud computing paradigm.[60] Any lingering doubts about the viability of such ventures as legitimate, for-profit enterprises should be put to rest by Goldman Sachs's attempt to raise $1.5 billion in financing for Facebook, making it arguably "the hottest property on the planet," and a similar $1.1 billion venture fund implemented by JPMorgan & Co.[61] In 2011, Twitter and Salesforce.com alone are expected to rent a combined 400,000 square feet of San Francisco office space, helping the vacancy rate in the City by

55. Chatman, *supra* note 23, at 38.

56. *How the SmartMeterTM System Works and What It Can Do for You*, PG&E.COM, http://www.pge.com/myhome/customerservice/smartmeter/facts/ (last visited Mar. 2, 2011).

57. Jennifer Lynch & Lee Tien, Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining To The Smart Grid 1, 4-9 (2010) *available at* https://www.eff.org/files/CDTEFFJointComment030910.pdf.

58. *See* Cynthia J. Larose, *Energy and Clean Technology Alert: Smart Grid Privacy Issues To Be Examined by the Federal Communications Commission – Comment Period through October 2, 2009*, MINTZ LEVIN (Sep. 25, 2009), http://www.mintz.com/publications/1954/Energy_and_Clean_Technology_Alert_Smart_Grid_Privacy_Issues_To_Be_Examined_by_the_Federal_Communications_Commission__Comment_Period_through_October_2_2009; Jesse Ward, *The Smart Grid Primer: Building the Smart Grid Broadband Network*, NATIONAL TELECOMMUNICATION COOPERATIVE ASSOCIATION (Aug. 23, 2010), http://www.ntca.org/new-edge/epapers/the-smart-grid-primer-building-the-smart-grid-broadband-network.

59. Lynch & Tien, *supra* note 57, at 4–9.

60. For example, in July 2010 Facebook exceeded 500 million active users, well in excess of the total population of the entire United States. *See Company Timeline*, FACEBOOK, http://www.facebook.com/press/info.php?timeline (last visited Mar. 2, 2011).

61. Dominic Rushe, *Goldman Sachs Suffers Facebook Fiasco*, GUARDIAN (Jan. 17, 2011, 9:41 p.m.), http://www.guardian.co.uk/business/2011/jan/17/goldman-sachs-facebook-private-placement; Dan Levy & Ari Levy, *Twitter Boosts San Francisco Offices as Banks Give Up Space*, BLOOMBERG (Mar. 02, 2011, 4:58 p.m.), http://www.businessweek.com/news/2011-03-02/twitter-boosts-san-francisco-offices-as-banks-give-up-space.html.

the Bay drop faster than any other in the country.[62]

Unlike much of the ESI of just a few years ago, information created by users of social networks is often not stored permanently on a user's computer, but rather on the social network's own servers.[63] As of 2009, Facebook utilized 30,000 servers in several different data centers, handling the equivalent of 1,000 times the volume of mail delivered daily by the U.S. Postal Service, according to its Vice President of Technology.[64] Twitter similarly maintains a 15,000-square-foot data center to accommodate the upwards of 90 million "tweets" sent daily via its networks.[65] Though some data, such as the 80 billion pictures more or less permanently stored by Facebook[66] may be available through other reasonably accessible means, other content, particularly data generated on the networking site rather than simply uploaded to it, is probably no more than ephemeral data on the user's own computer.

Information generated on social networks has already been used in family law for divorce and child welfare cases, in employment law cases, and in the damages phases of other civil litigation.[67] For example, photos deleted from a Facebook account became the focus of a heated discovery dispute in a 2010 Virginia case for wrongful death and resulted in an adverse inference sanction for spoliation.[68] In late 2009, a teenager in New York was released after twelve days in prison, and robbery charges against him were dropped, once his family produced a time-stamped Facebook status update that convinced police of his innocence—but not before the date and time of the update were confirmed by Facebook pursuant to a Brooklyn Assistant District Attorney's subpoena.[69] Though the implications of the cloud computing paradigm for criminal law are beyond the scope of this work, the example of the so-called "Facebook alibi" illustrates a central point—that crucial evidence will increasingly be in the

62. Levy & Levy, *supra* note 61.

63. Andrew C. Payne, Note, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 848 (2010).

64. Payne, *supra* note 63, at 848.

65. *Id*. Lena Rao, *Twitter Seeing 90 Million Tweets Per Day, 25 Percent Contain Links*, TECH CRUNCH (Sept.14, 2010), http://techcrunch.com/2010/09/14/twitter-seeing-90-million-tweets-per-day/.

66. Payne, *supra* note 63, at 848.

67. *Id*. at 841–42.

68. Peter Vieth, *Facebook 'Sideshow' No Distraction, Lawyer Says*, VIRGINIA LAWYERS WEEKLY, Dec. 16, 2010. The defense in the case had sought to use pictures of the plaintiff "drinking a beer and having a his arm around a girl" to contest his claim for post-traumatic stress disorder after the death of his wife. After the plaintiff deleted the photos from his Facebook account despite receiving a discovery request for them, his lawyer was sanctioned in the amount of $6,000 and the jury was twice instructed it could draw adverse inference from the destruction of this evidence. Nevertheless, the jury awarded plaintiff nearly $10.6 million, one of the highest awards ever in Virginia death cases, which prompted plaintiff's lawyer to remark that the deleted pictures "didn't make a hill of beans."

69. *Facebook Alibi Frees Brooklyn Man Rodney Bradford From Jail*, CBS NEWS (Nov. 19, 2009), http://www.cbsnews.com/8301-504083_162-5675551-504083.html.

possession of third parties.[70]

From emails and text messages, to online shopping and banking, the technology revolution has created the e-client.[71] Since at least the 1990s, electronic evidence has been vital in determining the outcome of cases involving allegations of sexual harassment, disputes over trade secrets, copyright infringement, and insider trading.[72] It's only a matter of time before litigation, and especially e-discovery, directly confronts the reality of cloud computing. As ESI increasingly shifts into the hands of third parties, such as social media networks, there is little doubt that it, and the metadata[73] authenticating it, will continue to be relevant and potentially discoverable in a variety of litigation contexts. As third-party custodians of that information, cloud computing providers will likely play roles ranging from inadvertent spoliator to last-chance source of "smoking gun" evidence. Whether seeking information or complying with discovery expectations, all parties have a stake in minimizing and preventing loss or material alteration of data stored in the cloud.

III. THE PROBLEMS OF PRESERVATION

From business transactions to financial arrangements to social interactions, more than ninety percent of all information created and stored today is in the form of ESI.[74] Already eighty percent of all business records are never converted to paper.[75] "As businesses increasingly rely on electronic record keeping, the number of potential discoverable documents has skyrocketed and so also has the potential for discovery abuse."[76] "As documents are increasingly maintained electronically, it has become easier to delete or tamper with evidence (both intentionally and inadvertently) and more difficult for litigants to craft policies that ensure all relevant

70. *See* PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 185–86 (ABA 2nd ed. 2008) (Evidentiary value may exist only in a deviant or later version of a file stored in another location, and parties seeking to use ESI as evidence will have to address questions of the trustworthiness of the source). Not only is data created and stored through social networks discoverable evidence, attempts to delete it prompted a charge of evidence-tampering against a Rutgers University student whose alleged use of Twitter to promote an online video of a classmate led to the classmate's suicide. *See* Associated Press, *Deleting Called Tampering With Evidence*, TIMES UNION (Apr. 24, 2011, 12:01 a.m.), http://www.timesunion.com/news/article/Deleting-called-tampering-with-evidence-1350074.php.

71. Kimura & Yamamoto, *supra* note 38, at 161.

72. Redish, *supra* note 6, at 563.

73. The Sedona Conference defines metadata as "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted." *The Sedona Principles: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* THE SEDONA CONFERENCE, 94 (Sept. 2005), http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf.

74. Kimura & Yamamoto, *supra* note 38, at 154–55.

75. *Id*. at 162.

76. *In re* Seroquel Prod. Liab. Litig., 244 F.R.D. 650, 653–54 (M.D. Fla.).

documents are preserved."[77] But if courts are still coming to terms with just the proliferation of ESI, what will happen when all that information migrates into the hands of third parties?

E-discovery issues in the cloud computing paradigm will increasingly become centered on the complex relationship between the responding party, its inside and outside counsel, and one or more third-party custodians and vendors. A common issue, whether litigated or not, will be the implementation of litigation holds and effective preservation and production of data stored "in the cloud."[78] Another will be the burden on counsel to fill the space between the client and the cloud service provider, and the extent of counsel's liability when spoliation occurs—in other words, the extent of the burden that will be placed on responding parties and their counsel to ensure ESI is produced from the cloud or, at least, that sanctions against them are not appropriate. Though perfect preservation is not even the goal,[79] how much data and potential evidence will simply be allowed to slip away because third parties do not have an enforceable pre-discovery obligation to preserve?

A. THIRD-PARTY DUTIES ARE DISPROPORTIONATE TO THEIR ACTUAL CONTROL

As a part of routine discovery, a party may serve on any other party a request to produce certain items, including ESI, that are in the responding party's "possession, custody, or control."[80] In the context of cloud computing, "control" is usually the most relevant test for the end user, since the service provider most likely has possession and custody.[81] "Control" as used in Federal Rule of Civil Procedure 34 refers to the "right, authority, or practical ability to obtain" from a nonparty to the action.[82] A number of cases have gone to significant lengths to make parties to the litigation responsible for ESI lost while in the possession of a third party if

77. Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 214 (S.D.N.Y. 2003).

78. Narkiewicz, *supra* note 22, at 56; *see also* Orbit One Communs., Inc. v. Numerex Corp., 271 F.R.D. 429, 436 (S.D.N.Y. 2010) (identifying the boundaries of the duty to preserve involve not just *when* the duty attaches and *what* evidence must be preserved, but "*how* must a party go about fulfilling its ultimate obligation, and *who* is responsible for seeing that it is fulfilled?") (emphasis in original).

79. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, *supra* note 73, at no. 5.

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

81. Venkat Rangan, *E-Discovery and the Cloud: Possession, Custody and Control*, E-DISCOVERY 2.0 (Sept. 3, 2010), http://www.clearwellsystems.com/e-discovery-blog/2010/09/03/e-discovery-and-the-cloud-possession-custody-and-control/.

82. *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007) ("*NTL*"); *see also* Moreno v. Autozone, Inc., No. C-05-4432 CRB, 2008 WL 906510, at *1 (N.D. Cal. Apr. 1, 2008) ("Control is generally defined as the legal right to obtain the documents on demand and at times has been construed more broadly to include the practical ability to obtain the documents sought upon demand.").

the information was at least nominally under the party's "control."[83] To some extent, this practice has expanded the jurisdictional scope of the district court beyond its statutory 100 miles—courts have routinely extended the affirmative duty to preserve evidence far beyond its jurisdictional reach even where the 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.[84] Does this still make sense in the cloud computing paradigm given the mutability of ESI and the limited ability of parties to actually control the preservation of data?[85] Should it matter whether a third party has been entrusted with potential evidence only after it's been identified as such or whether it is the normal and customary "custodian" of such information? Circuits are split as to whether the practical ability to obtain materials is sufficient to constitute "control" in the meaning of Rule 34.[86]

Of course, the fact that the information was stored on a third party server alone is not sufficient to challenge "control." For example, where a service provider destroys information because the party stops paying for its services and cancels its contract, any spoliation of evidence can appropriately be blamed on the party.[87] But practically speaking, what a party can "access" is not necessarily the same as what the party can "control"[88]—cloud computing and the Internet make access a much broader category than control. Who, for example, has control over the notes of an insurance adjuster entered on a handheld device from a car onto a remotely hosted word processing application? What may be merely accessed through a contractual or agency relationship but not controlled is vulnerable between the attachment of a duty to preserve and a formal request for discovery.[89]

83. *See, e.g.*, *In re* Flag Telecom Holdings, Ltd. Sec. Litig., 236 F.R.D. 177, 180 (S.D.N.Y. 2006) ("The test for the production of documents is control, not location . . . . Documents may be within the control of the party even if they are located abroad."); *see also,* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523–24 (D. Md. 2010).

84. *See Victor Stanley*, 269 F.R.D. at 523–24.

85. Consider Facebook, for example. By creating an account, one gains "access" to a variety of information about other users with very little, if any, control over the content.

86. *In re NTL, Inc. Sec. Litig*., 244 F.R.D. at 195; Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1426–27 (7th Cir. 1993).

87. *See, e.g*., Cyntegra, Inc. v. Idexx Lab., Inc., No. CV 06-4170 PSG, 2007 WL 5193736, at *5 (C.D. Cal Sept. 21, 2007).

88. Thomas A. Cooper, *Jurisdictional, Procedural, and Economic Considerations for Non-Party Electronic Discovery*, 59 EMORY L.J. 1339, 1353 (2010).

89. It may be, however, that the current broad reading of control can be narrowed on the back end by limiting what is "reasonably accessible," and therefore subject to production during discovery, to that which the responding party could have reasonably indentified and preserved given both the foreseeability of the issues in litigation and the relevant practical challenges. In fact, similar considerations are generally used to exempt metadata from the ordinary scope of the preservation duty. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, *supra* note 73, at nos. 5 and 9.

While a third party may play a relatively large role in the actual preservation and maintenance of information on a daily basis in the course of its normal business practices, such a custodian who negligently or willfully destroys evidence in its possession faces little consequence, if any, apart from those it has contracted to sustain or which might be inflicted on its reputation in the market. Although parties to a lawsuit must accept the reality that discovery is by definition invasive and potentially very expensive, nonparties have a different set of expectations.[90] Third parties should not be required to subsidize litigation in which they do not have a stake, and they do not have a general duty to preserve evidence for use by others.[91] A nonparty's responsibility to preserve information is generally limited to the mutual obligations of a contract or other agreement,[92] or an independent obligation under a statute or regulation, such as applies to auditors under the Sarbanes-Oxley Act of 2002,[93] stock exchanges, and securities dealers under the Securities and Exchange Act,[94] and various implementing regulations under the Fair Labor Standards Act.[95] But violation of these statutory duties, even by a party, will not necessarily result in an award of sanctions in favor of a requesting party.[96] This reality is cold comfort to those situated like the plaintiff, for example, in the introductory hypothetical.

"[W]hen does the duty arise to preserve evidence or items that potentially could become evidence? To whom does this duty extend? And, what items must be preserved? Answers to these three questions are of critical importance for attorneys who counsel their clients."[97] These questions are all the more important when the client has entrusted possession and custody of potential evidence to a third party, because under current federal rules and statutory regimes, the penalty for third party spoliation of evidence will always fall, if anywhere, on one of the parties.[98]

90. Cusumano v. Microsoft, *162 F.3d 708, 717 (1st Cir. 1998)*.

91. *Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas*, THE SEDONA CONFERENCE, 3 (Apr. 2008), *available at* http://www.thesedonaconference.org/dltForm?did=Rule_45_Subpoenas; Fletcher v. Dorchester Mut. Ins. Co., 773 N.E.2d 420, 424–25 (Mass. 2000).

92. *See generally* Benjamin J. Vernia, *Negligent Spoliation of Evidence, Interfering With Prospective Civil Action, as Actionable*, 101 A.L.R 5TH 61, § 9 (Agreement).

93. *See* 18 U.S.C. § 1520(a)(1)–(2) (2006).

94. *See* 15 U.S.C. § 78q(a) (2006).

95. *See* 29 U.S.C. § 211(c) (2006); 29 C.F.R. § 516.5-6 (2006).

96. *See, e.g.*, Sarmiento v. Montclair State Univ., 513 F. Supp. 2d 72, 94 (D.N.J. 2007) (adverse inference not available against defendant employer where its failure to preserve records was a violation of a federal statutory obligation because the litigation was not reasonably foreseeable at the time of the spoliation).

97. MARGARET M. KOESEL & TRACEY L. TURNBULL, SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION 1 (ABA 2d ed. 2006).

98. *See* KOESEL & TURNBULL, *supra* note 97, at 18–21 ("A duty to preserve may extend beyond the parties themselves and extend to evidence entrusted to their agents, experts, insurers, attorneys, and the like. In such instances, a party may be held liable for spoliation committed by a third party to whom it entrusted the destroyed evidence.").

B. PRESERVATION TOOLS ARE INEFFECTIVE AGAINST THIRD PARTIES

The general lack of a duty to preserve is the basic flaw in using existing preservation tools to encourage a third party to take steps towards segregating and preserving potential evidence. As discussed below a party can pay for additional storage or other services, but it cannot expect the third-party vendor to assume any preservation responsibilities, apart from those to which it has contractually obligated itself, without additional compensation. One can put the vendor of one's opposing party on notice with a preservation letter, if their identity is known, but this does little, if anything, to shift the underlying responsibilities for preservation. Parties today cannot stop paying for cloud services and force their vendors to continue preserving their data pursuant to an independent legal duty to do so.

At the early stage of an initial litigation hold, potentially before litigation has even commenced, the burden of "freezing" the relevant data in the cloud could be overwhelming for the potential litigant, the third party, or both. The reliability of any computer system and the information gleaned from it can be a difficult issue when the servers are located just in the next room. But even when computer systems function perfectly, ESI remains fluid and dynamic and thus can be altered or destroyed by the ordinary operation of a computer, often without the operator's knowledge or direction.[99] Practices like multi-tenancy draw into question the feasibility of easily segregating and searching through the ESI of a particular user, with implications for determining which data is "reasonably accessible."[100] In the cloud, the data fragmentation and dispersal that enhances security also creates a data retention challenge and a potential exposure to foreign laws.[101]

At the same time, cloud computing will probably exponentially increase the amount of potentially discoverable "documents," as data about data becomes increasingly probative. The ability or willingness of a cloud computing service provider to produce information stored on its servers, may be limited by the Stored Communications Act ("SCA").[102] Because no cause of action lies against any provider for producing information, facilities, or assistance in accordance with the terms of a court order,

99. 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, 4 (2007). *See also* Kraus, *supra* note 6 ("disks corrode, bits "rot" and hardware becomes obsolete").

100. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, *supra* note 73, at no. 8.

101. Mell & Grance, *supra* note 27, at slides 22, 24.

102. Stored Communications Act, 18 U.S.C. § 2701 (2006).

warrant, subpoena, or statutory authorization,[103] cloud services providers typically require a court to mandate production of their customers' ESI without consent.[104]

But email and its protections under the current form of the SCA may prove to be an exception rather than the rule in the cloud computing paradigm, and perhaps rightly so.[105] Many cloud computing services arguably fail to qualify for the privacy protections of the SCA because they do not meet one or both of the statutory requirements of "electronic storage," which must be either of a temporary and intermediate nature, incidental to electronic transmission, or stored by the provider for the purpose of backup protection.[106] For example, some word processing applications merely allow for the sharing of data, rather than its communication—the data itself never leaves the providers cloud and thus the "send or receive" functionality required by the SCA is lacking.[107] Similarly, the authority to access users' data for a wide variety of purposes other than mere storage or processing, such as for generating targeted advertisements, takes many cloud computing service providers outside the current SCA definition of a "remote computing service."[108] Thus, it may not be as easy in the future to simply assume that service providers are shielded by statute from producing any user content in their possession or custody. Though the SCA provides an important privacy safeguard for computing network users, particularly those on social networking sites and Web 2.0, it seems the primary civil litigation impact of cloud computing will be in the number of nonpersonal records entering the cloud that are less likely to involve privacy issues.[109] In other words, just because ESI is stored in the cloud doesn't mean it is necessarily "private" or should be subject to heightened procedural safeguards. As a result, third parties with relevant ESI in their cloud should be increasingly expected to produce from their servers.[110]

103. Stored Communications Act, 18 U.S.C. § 2703(e) (2006).

104. *See, e.g.*, Rangan, *supra* note 81.

105. *See* Marcia Hofmann, *Social Media Seeking User Data Share This*, CALIFORNIA LAWYER (Mar. 2011).

106. Robison, *supra* note 25, at 1209.

107. *Id.* at n. 97.

108. *Id.* at 1212–14.

109. For example, in 2011 the U.S. Supreme Court determined that the privacy exemption to the Freedom of Information Act does not apply to the information of corporations. *See* F.C.C. v. AT&T Inc., 131 S. Ct. 1177, 1181 (2011). In the rare case that a third party subpoena seeks information that would constitute a trade secret, existing considerations regarding the use of protective orders would likely be sufficient.

110. *See* Thomas Y. Allman, *Conducting Discovery After the Amendments: The Second Wave*, 10 SEDONA CONF. J. 215, 216 (2009) ("[R]elevant information in operating systems, dynamic databases, websites and voicemail ("digital audio files"), for example, can be discoverable whether found on individual or networked hard drives or on personal devices such as cell phones and PDAs.") (citations omitted).

If a court order is required, one approach to ensuring early preservation is to seek a preliminary injunction. An injunction entered under Rule 65 can bind the agents or servants of a party, and a court may use civil contempt sanctions to deter or punish third-party spoliation if preservation has been ordered by the court.[111] However, the evidentiary showing necessary to obtain such a preliminary injunction or TRO makes this a cumbersome method for ensuring the preservation of data held by a third party prior to the ordinary discovery process when, presumably, the extent of the relevant information available first comes to light.[112] In any event the pre-litigation duty to preserve is not enforceable against third parties in federal court under Rule 65—only an analogous duty can be imposed through an injunction when specific ESI can be identified for preservation against a manifest threat of destruction or deletion and a high likelihood of resulting prejudice. The extent of such a showing would likely have to approximate or exceed the cost of implementing the desired preservation unless the moving party voluntarily undertakes part of the cost. It remains to be seen if a party could meet this threshold to enjoin its own vendor to preserve evidence at the party's expense, but at the vendor's risk of contempt for spoliation. Increasing familiarity with cloud computing will shift standards of reasonableness over time, in terms of privacy expectations, accessibility and, potentially, culpability.[113] But even if customs develop to assume a quasi-duty to preserve on the part of third parties, judges will be hesitant if not stridently resistant to forcing any significant level of involuntary burden for preservation to a third party.

C. PRODUCTION TOOLS ARE INEFFECTIVE AT ENFORCING OR ENCOURAGING PRESERVATION

To the extent that third parties can be compelled to produce documents during discovery, procedures that do so are typically not

111. FED. R. CIV. P. 65(d)(2) (stating that "the order binds the parties, their officers, agents, servants, employees, and attorneys and other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)").

112. *See* Sierra Club, Lone Star Chapter v. F.D.I.C., 992 F.2d 545, 551 (5th Cir. 1993) (to obtain a preliminary injunction, a party must show that there is a substantial likelihood that it will succeed on the merits, that there is a substantial threat that it will suffer irreparable injury if the district court does not grant the injunction, that the threatened injury to the plaintiff outweighs the threatened injury to the defendant, and that granting the preliminary injunction will not disserve the public interest). CHARLES A. WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE § 2951 (2d ed. 2011) ("When the opposing party actually receives notice of the application for a restraining order, the procedure that is followed does not differ functionally from that on an application for a preliminary injunction and the proceeding is not subject to any special requirements.") Any temporary restraining order granted without notice must comply with the provisions of Rule 65(b).

113. *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619, 2929 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

effective means of ensuring preservation. A Rule 45 subpoena can be used to compel production of ESI, and is in fact usually required for the production of emails from third parties.[114] Amendments made to Rule 45 in 2006 were intended to explicitly recognize the existing practice of seeking Rule 45 subpoenas for such requests.[115] The issuance of a subpoena to a third party imposes a legal obligation on the third party to preserve information relevant to the subpoena, including ESI, at least until related issues are resolved.[116] In some circumstances, the subpoena itself could make the recipient a potential party in foreseeable litigation, but service of and compliance with a nonparty subpoena alone is generally not sufficient to create an independent duty to preserve.[117]

Many of the 2006 amendments to Rule 45 were simply borrowed language from Rules 26 and 34 with appropriate wording to clarify its applicability to subpoenas.[118] This fact reflects the general approach to nonparty production taken by the Sedona Conference and rule-makers—that it is essentially the same as production from parties. Naturally, the consequences for spoliation after the issuance of an injunction or a subpoena include the full range of penalties available for contempt of court including, in extraordinary cases, imprisonment.[119] But as with injunctions under Rule 65, subpoenas under Rule 45 suffer the basic flaw that they do not impose an obligation on a third party to preserve ESI or other evidence until after a lawsuit has been initiated, which can often be a considerable time after the duty to preserve has attached to the responding party.[120] Where subpoenaed evidence is not available due to spoliation, the question before the court is generally whether the third party complied with the terms of the subpoena, not whether the party properly preserved evidence prior to its issuance.[121] If it can be shown that the data was already lost prior to its issuance, the subpoena is of no consequence. In the meantime, the responding party or its counsel bear the sole burden of ensuring preservation of ESI in the cloud with little means of actually doing so.[122]

114. *See generally* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

115. *Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas*, *supra* note 91, at 3.

116. *Id.*

117. *Id.*

118. *Id.*

119. *See* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 537 (D.Md. 2010).

120. *See, e.g.*, *In re* Cree, Inc. Sec. Litig., 220 F.R.D. 443, 447 (M.D.N.C. 2004) (preservation subpoena served without leave of court quashed despite risk that routine document destruction policy might destroy relevant evidence).

121. Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 607 (2010).

122. To get around the restrictions of the SCA, a federal magistrate in the Middle District of Tennessee proposed the parties "friend" him on Facebook, thus providing mutual access to disputed photos and emails. *See* Terry Baynes, *Should You Friend the Judge?; Social media presents a new front for discovery battles*, THE AMERICAN LAWYER, Sept. 1, 2010, http://www.law.com/jsp/tal/PubArticleTAL.jsp?id=1202472760856&slreturn=1.

As a result any penalties against the non-party for contempt, even if remedial in some cases, are an ineffective incentive for pre-litigation preservation. Perhaps more importantly, injustice to an actual litigant is a likely result whenever the requesting party is substantively prejudiced by the unsanctioned loss of crucial evidence,[123] or if a sanctioned party is simply a stand-in for the third party and thereby itself becomes the victim of negligent or willful spoliation.[124]

The use of production methods to preserve and obtain information from the cloud is further complicated by the fact that data may be difficult to separate from confidential or proprietary information of the party, the vendor, or other third parties. Though a party generally does not have standing to challenge a nonparty subpoena, a party whose information is sought can move to quash under the SCA as to its own privacy interests.[125] Courts seem willing and able to protect messages that are inherently private while distinguishing and protecting those that are not,[126] notwithstanding the general rule that any person who does not provide an electronic communication service, or a remote communication service, can "disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.[127]

The third party can likewise move to quash or modify a subpoena to protect privacy interests.[128] For example, information about how a party uses a cloud-based platform might only be derivable through information residing exclusively in the data structures or processes of the cloud not set out in any particular data output available to the user.[129] The vendor may in

123. Consider, for example, the plight of Monica Lips, whose products liability case against the manufacturer of her defective hip replacement suffered an initial setback when the hospital that removed the prosthesis from her body destroyed the pieces. Lips' claim against the hospital was dismissed and the decision was affirmed by the Arizona Supreme Court, which decided not to recognize an independent tort for intentional spoliation. Lips v. Scottsdale Healthcare Corp., 229 P.3d 1008, 1009 (Ariz. 2010); *see also* Pat Murphy, *Arizona Supreme Court: Is hospital liable for losing key evidence?*, LAWYERS USA, May 10, 2010, http://lawyersusaonline.com/benchmarks/2010/05/10/is-hospital-liable-for-losing-key-evidence/. The court declined to comment on the viability of a negligent spoliation tort in the state since Lips had only alleged intentional spoliation on the basis that her surgeon had requested the preservation of the prosthesis. It remained to be seen what effect the decision would have on the underlying suit against the manufacturer, but the spoliation claim alleged that the underlying suit was compromised by the destruction of crucial evidence.

124. *See* Keir v. Unumprovident Corp., No. 02 Civ. 8781, 2003 WL 21997747 at *13 (S.D.N.Y. Aug. 22, 2003) (defendant sanctioned for accidental spoliation of emails by third-party vendor).

125. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973–76 (C.D. Cal. 2010).

126. For example, in *Crispin*, the court quashed a subpoena as to Facebook and MySpace postings filtered so they could only be viewed by "friends" rather than the general public, while remanding for development of the record as to whether wall posting and comments would be similarly protected from discovery. *Id*. The private messages were likened to videos not marked for public access in Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

127. *Crispin*, 717 F. Supp. 2d at 973 (quoting Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del.1997)).

128. *See* FED. R. CIV. P. 45(c)(3)(A)(iii), (d)(2).

129. Chris Reed, *Information "Ownership" in the Cloud*, QUEEN MARY SCHOOL OF LAW LEGAL

fact have proprietary interests, or even copyright, in creatively structured databases.[130] Even identifying the correct vendor may be challenging if a cloud provider incorporates proprietary services of other companies as part of its own service or allows other companies to use its platform to provide services directly to the end user.[131] Though spoliation is not the primary concern in such instances, the confidentiality concerns that can attend production of proprietary information make the use of subpoenas to reveal flaws in preservation unwieldy at best.

IV. PRESERVATION PROPHYLAXIS

Rule makers are still undecided whether a new preservation rule is necessary, let alone what form it would take.[132] While consideration of the topic provides a useful opportunity to examine how control and accessibility of data in the cloud shape the application of proportionality to preservation, the answers to the types of questions posed earlier by the introductory hypothetical depend in the meantime on the contract between the insurer and its cloud service provider. Cloud computing is a service industry, and therefore, the businesses in this space are constantly under pressure to modify their offerings to the perceived needs of the market. Given that a third party's obligations to preserve data on their servers is generally limited to their terms of service agreements, these agreements are a natural place to start when looking for peace of mind[133] regarding data in the cloud. With the exception of a relatively few niche service providers, however, contracting for data integrity may come at the cost of some of the features that attract businesses to cloud computing in the first instance.

A. TERMS OF SERVICE AND THE COST OF "PEACE OF MIND"

As a starting point, most cloud service providers expressly disclaim liability for lost data.[134] Some promise "best efforts" to preserve data, but assert a general disclaimer and keep on the end user the responsibility for

STUDIES RESEARCH PAPER NO. 45/2010 1, 8 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

130. Reed, *supra* note 129, at 15 (citing *Feist Publications, Inc. v. Rural Telephone Services Co., Inc.*, 499 U.S. 340 (1991)).

131. *Id*. at 5–6.

132. *Agenda for April 2011 Meeting*, *supra* note 29, at 194.

133. Rackspace, a data backup service, advertises on their website that their solutions "deliver nothing less than peace of mind." *Unmetered Managed Backup*, RACKSPACE HOSTING, http://www.rackspace.com/managed_hosting/services/storage/managedbackup (last visited July 31, 2011).

134. Simon Bradshaw, Christopher Millard, & Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, QUEEN MARY SCHOOL OF LAW LEGAL STUDIES RESEARCH PAPER NO. 63/2010 1, 21–22 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

preserving the confidentiality and integrity of its own data.[135] The disclaimers of most vendors make clear that there is no warranty as to the quality or fitness of their service for any particular purpose.[136] From here, many service providers provide further guarantees if the end user agrees to purchase separate backup services.[137] Others provide data backup and integrity services without additional charge, but also without any express guarantee of preservation.[138] Few take any effort to ensure that data is stored in any particular location or jurisdiction, though some have servers configured in regional zones in which data can be corralled with predictability.[139]

If standard backup packages are not enough to provide satisfaction about one's remotely stored data, another option is to negotiate a bespoke contract with a variety of additional guarantees and indemnifications.[140] If, for example, the hypothetical insurer had gone to this length, it might have the option of either settling the case with the homeowner on the basis of monies paid by the provider or litigating with the knowledge that some form of indemnification or contribution could be available. But relying on this sort of feature of a terms of service agreement in cases involving significantly larger claims than a single homeowner's insurance policy would likely be problematic; custom arrangements can include liquidated damages clauses for the relatively predictable business consequences of data loss or disclosure of proprietary information, but will likely not extend to court ordered sanctions for spoliation or failure to comply with an order to produce. In any event, most terms of service agreements have limitations on liability ranging from the amount paid for a single month of service to a multiple of the total amount paid for service to date.[141] Another challenge might be learning of a claim in time to bring it under a terms of service agreement that contains a limitation period of two years or less.[142] The process of getting the vendor "on the hook" for the preservation of data appears to be as much about providing peace of mind for the vendor as for its customer.

At least one popular provider of premium preservation services offers managed backup on a daily, weekly, or incremental basis to physical media such as tapes or discs.[143] Far from some technological innovation, this service is essentially identical to the types of backups businesses have been

135. Bradshaw, et al., *supra* note 34, at 21–22.
136. *Id*. at 32–33.
137. *Id*. at 22.
138. *Id.*
139. *Id*. at 27–28.
140. *Id*. at 2.
141. *Id*. at 36.
142. *Id*. at 18.
143. *Rackspace Managed Backup: Technical Overview*, RACKSPACE HOSTING, (2009), http://broadcast.rackspace.com/downloads/pdfs/ManagedBackupTechOverview.pdf.

making in-house for decades, and suffers the same restoration challenges. The difference is that once computing infrastructure itself has been outsourced, backup and preservation must follow. Unless there are significant scalability issues, wildly variant peak and trough usage periods, or a profound need for remote access, it becomes less clear whether outsourcing the company's entire information technology department actually provides the risk-adjusted benefits originally perceived. This realization is particularly acute for large concerns that are subject to frequent litigation and exist under virtually perpetual threat of foreseeable litigation.

Thus, the final and, ultimately, only way to tailor the terms of service to offset the risks of preservation in the cloud is to limit use. Mature companies with more predictable information flows and computing needs may prefer to retain much of their information technology infrastructure in-house or to maintain private clouds with outsourced support. Such companies might use public cloud resources for limited categories of data only, focusing on those that require little access (essentially leasing storage space) or those that benefit most from shared access, such as early-stage development projects. Limiting the potential types of data losses to those that are best compensated by liquidated damages clauses likely provides the mix of scalability, flexibility, integrity, and security that most closely approximates actual peace of mind.

B. NEW RULES

Since the 2010 Civil Litigation Conference at Duke University, the Advisory Committee on Civil Rules has taken a serious look at further amending the Federal Rules with respect to discovery. Though agreement on the need for such a rule has not been completely unanimous, the general consensus seems to be that the principle of proportionality that now governs the scope of production should also be incorporated into considerations of preservation.[144] It is beyond the scope of the current work to discuss the methods by which this might occur other than to briefly discuss some of the potential implications in the cloud computing paradigm and to suggest that a practical understanding of access to and control of data in the cloud should be the foundation of any normative framework for proportionality in preservation.

A preservation standard incorporated into the Federal Rules would likely emphasize reasonableness and proportionality as essential contours of the duty to preserve.[145] "Whether preservation or discovery conduct is acceptable in a given case depends on what is *reasonable,* which itself

144. *Agenda for April 2011 Meeting*, *supra* note 29, at 194.
145. Allman, *supra* note 30, at 145.

depends on whether the requested discovery efforts are *proportional* to the case and consistent with established standards."[146] In other words, the duty to preserve will always be determined by an analysis that "depends heavily on the facts and circumstances of each case and cannot be reduced to a generalized checklist of what is acceptable or unacceptable."[147] In the context of this amorphous obligation on courts, parties, and counsel, a practical understanding of control and accessibility in the cloud computing paradigm has a profound potential for creating some level of objectivity and predictability in preservation and e-discovery.

One of the most attractive features of cloud computing to business users is its scalability, which refers to the ability to purchase only as much or as little storage, processing and bandwidth as needed at any given time. The pay-per-use model allows users to limit their costs to the amount of storage and bandwidth actually used. But this model turns against a party seeking to implement a litigation hold with respect to data in the cloud to the extent doing so would require the purchase and use of extra bandwidth, processing, or storage to identify, collect, and preserve data related to foreseeable litigation. Unlike the restoration of backup tapes, which only becomes an issue with respect to production, the cost of exercising control over data in the cloud would likely result in significant costs at the initial preservation stages, cost which might someday replace the restoration of backups as the main object of discovery cost-shifting disputes. Given that the cloud computing paradigm encourages users to maintain relatively little onsite storage capacity, even the theoretical ability to re-route ESI may not necessarily translate into actual control of the data or a practical ability to do so.[148]

Even where parties carefully manage their information, it's not clear that cloud computing users necessarily have ready access to all potentially relevant information, particularly metadata. The general rule is that there is no duty to preserve material on inaccessible media,[149] and metadata is presumptively inaccessible unless there is a particular showing of relevance. Where the issue is one of authentication or creating a timeline

146. Allman, *supra* note 30, at 145 (quoting Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (2010) (emphasis in original)).

147. *Rimkus*, 688 F. Supp. 2d at 613 (citing Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 464–65 (S.D.N.Y. 2010)).

148. *See* Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 453 (C.D. Cal. 2007) ("data in issue which is currently routed to a third party entity under contract to defendants and received in said entity's RAM . . . is within defendants' possession, custody or control by virtue of defendants' ability to manipulate at will how the data in issue is routed").

149. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no'. Such a rule would cripple large corporations."). *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, *supra* note 73, at no. 8.

of access to a particular file, metadata will clearly be important and, therefore, should be within the scope of production. Increasingly, metadata will typically be in the category of information generated inside the cloud, the ownership of which is potentially subject to dispute.[150] A showing of special need and relevance by a requesting party says nothing about the practical ability of a party to produce metadata in a meaningful form or the foreseeability of its eventual need to do so from within the pre-litigation context. Nevertheless, a narrow "front end" preservation rule is less likely to consistently produce just results than a broad "back end" rule that gives judges the discretion to tailor sanctions based on the centrality or importance of the evidence sought by the requesting party and the apparent culpability of the responding party.[151]

It's also not clear that the distinction between active data and disaster backup is a particularly effective distinction for evaluating accessibility in the cloud computing paradigm.[152] The approach to accessibility articulated by Judge Scheindlin in *Zubulake IV* defines certain formats of digital media, like backup tapes, as *per se* inaccessible.[153] "A party need not provide discovery of electronically stored information from sources that the party identifies as not *reasonably accessible* because of undue burden or cost."[154] But even inaccessible data sources must be preserved if they store documents of "key players" to the existing litigation or where the responding party can identify where on the inaccessible sources the relevant[155] information is stored.[156] The principle of proportionality is then used to determine whether the likely probity of the information justifies the cost of production.

But while this *per se* distinction is explicitly predicated on concerns related to cost, it actually becomes unmoored from cost when the burden of

150. Reed, *supra* note 129, at 8–9.

151. *See Agenda for April 2011 Meeting*, *supra* note 29, at 194–95. For example, where the missing evidence is so important as to make it eminently foreseeable that it would have to be preserved for production, failure to do so—or arrange to do so with a service provider—should be sanctionable even though the actual destruction, loss, or modification of the evidence might not be intentional. On the other hand, where missing data would not have been particularly identifiable for its importance prior to a discovery request, there should be less inclination to impose sanctions on the same negligent action or inaction.

152. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, *supra* note 73, at no. 5.

153. *Zubulake*, 220 F.R.D. at 217–18 (S.D.N.Y. 2003).

154. FED. R. CIV. P. 26(b)(2)(B) (emphasis added).

155. "Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." FED. R. CIV. P. 26(b)(1). For purposes of admissibility "'[r]elevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." FED. R. EVID. 401.

156. *Zubulake*, 220 F.R.D. at 218 (S.D.N.Y. 2003). *See also* FED. R. CIV. P. 26(b)(2)(B) (identification of a source by a party as "not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence").

preservation or production is due to a large volume of responsive data existing amongst many remote sources of otherwise reasonably accessible data. If, for example, data is located on "accessible" active media, but dispersed over several servers in multiple states or countries without a readily available means of downloading and segregating it, the cost of preserving and producing this information could exceed that of restoring backup tapes, and present all the same burdens, but would be required because the information is not *per se* inaccessible.[157] This is precisely the challenge many responding parties would likely face in the cloud computing paradigm. Unless the end user is proactively limiting the categories of data placed in the cloud as suggested above,[158] it is not clear that ESI stored in the cloud can be easily distinguished as that which is purely disaster recovery and that which is actively used for information retrieval—almost all data in the cloud is accessible to some degree. As a result, the practical burden of a reasonable, good faith preservation effort in the cloud seems unbounded by existing concerns of burden and cost unless proportionality is understood in terms of the types of accessibility and control available, and the cost thereof, in the third party paradigm.[159]

It may be possible in some cases to shift the cost of preservation to the requesting party, as already occurs when necessary with regard to production[160] and in the context of a Rule 45 subpoena, when preservation or production would impose an undue burden or expense on a nonparty.[161] Conversely, where negligence on the part of the third party generates cost burdens in collecting, processing or producing, it should be possible to shift the cost away from the parties altogether in pursuit of the underlying facts. Otherwise, the existing incentive to keep in an accessible format only that

157. The obvious solution to such a problem, however, would be to limit the scope of the discovery request pursuant to Rule 26(b)(2)(C). After discovery of the most likely relevant and probative information, the scope could broaden until the responding party was able to make a credible showing that any further production would be duplicative or cumulative.

158. *See supra* Section IV.A.

159. On a motion to compel production, an opposing party may assert undue burden, for which it must demonstrate that the time or expense involved in responding to requested discovery is unduly burdensome. *See, e.g.*, Oxford House, Inc. v. City of Topeka, Kansas, No. 06-4004-RDR, 2007 WL 1246200, at *4 (D. Kan. Apr. 27, 2007). But the mere fact that compliance will cause great labor and expense or even considerable hardship and the possibility of injury to the business of the responding party will not necessarily require denial of the motion, particularly if the information sought is highly relevant. *Id*. Though spoliation sanctions will not issue where a party cannot be compelled to produce lost ESI, at the preservation stage, the burden of determining where relevant material is stored is only examined under the rubric of "accessibility."

160. *See, e.g.*, Fendi Adele S.R.L. v. Filene's Basement, Inc., No. 06 CIV. 244RMBMHD, 2009 WL 855955, at *4 (S.D.N.Y. Mar. 24, 2009) (dispute over accessibility of backup tapes resolved by ordering production of electronic copies of backup databases at requesting party's expense).

161. *See, e.g.*, Dow Chem. Co. v. Reinhard, No. M8-85(HB), 2008 WL 1968302, at *2 (S.D.N.Y. April 29, 2008) (ongoing costs of attorneys' fees, privilege logs and other expenses assumed by complying with subpoenas to be shared between the subpoenaed party and the requesting party).

which is absolutely necessary for business purposes,[162] will serve as a disincentive to adoption of the cloud computing paradigm. Similarly, a *per se* rule for reasonably accessible data that excludes that stored in the cloud risks encouraging more frequent reduction to inaccessible formats where possible.[163] In either case, the result would be the vast reduction of discoverable information or, at least, a significantly heavier burden on requesting parties.

Another approach is to encourage the parties themselves to stipulate what media will be considered reasonably accessible or inaccessible.[164] Though it is not clear how often this tactic is already used, and it might only prove useful in symmetric cases where the potential costs of discovery are roughly equivalent, district court judges are likely to embrace such an approach, particularly in light of the explicit "meet and confer" requirements of the federal rules and the frequent exhortation that parties should conduct e-discovery in the spirit of cooperation.[165] Allowing the parties to determine as early as possible what is or is not reasonably accessible allows for better calibration based on the likely relevance of various media and allows the parties to create a hierarchy of relevant, cost-effective media from which responsive documents can be culled. And the effect is achieved without the creation of a "one size fits all" front-end rule that establishes a narrow framework for preservation obligations. The values served by stipulation are already emphasized under the existing Rule 16, but the benefits of this approach might justify further clarification and codification in the rules or committee notes.

V. CONCLUSION

The cloud computing paradigm appears poised to create a future in which the custodians of ESI are frequently nonparties for whom the duty to preserve as currently conceived does not effectively attach. To the extent that data in the cloud is more fluid, more challenging to authenticate, and potentially exists as bits scattered in servers around the world, traditional

162. *See, e.g.*, Best Buy Stores, L.P. v. Developers Diversified Realty Corp., 247 F.R.D. 567, 569–70 (D. Minn. 2007) (database produced for separate litigation not reasonably accessible because of a downgrade in format).

163. One solution would be to simply require a responding party to transfer any data subject to a litigation hold to on-site servers or other local media, but this obligation would tend to undercut the benefits of cloud computing for any large companies that frequently find themselves in litigation. It would also create significant costs that might not be relevant to the court's determination of whether the data was "accessible."

164. *See, e.g.*, Agreed E-Discovery Protocol and Order at ¶ 7, Interval Licensing LLC v. AOL, Inc., (No. 2:10-CV-01385-MJP) 2011.

165. *See, e.g.*, *Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement Agency*, No. 10 Civ. 3488(SAS), 2010 WL 381625, at *8 (S.D.N.Y. Feb. 7, 2011) (the words "meet and confer," "cooperate," and "communicate" are found in opinion after opinion and yet lawyers fail to take the necessary steps to fulfill their obligations to each other and to the court).

notions of preservation do not apply neatly to the cloud computing paradigm. Because discovery sanctions are intensely fact-dependent and somewhat unpredictable, all stakeholders in litigation have an interest in minimizing the disruptive potential of third party custody of relevant information.

For a variety of reasons, the concerns expressed in this note may not ultimately motivate a significant departure from current practices. Cloud computing might not become as ubiquitous as currently expected, or technology may improve to the point where loss of evidence is no longer a significant issue. Service providers and their users may agree to terms of service that largely resolve these issues by better allocating the responsibility and cost of preserving data in the cloud in relation to the actual ability to do so. The diligence of ethics committees, bar associations and similar organizations may establish clear expectations that afford courts and attorneys sufficient confidence to navigate these issues with only modest difficulty. Or Congress could shift expectations by amending the SCA or other statutes that currently only create a preservation obligation for parties, such as the Private Securities Litigation Reform Act.[166]

But if preservation rulemaking is contemplated, the potential benefits of including third-party custodians in the calculus should be considered. From the costs to businesses in terms of sanctions or settlement, to the effect on the cloud computing model and the ability of service providers to pass those costs on to their users, the practical ramifications of cloud computing on e-discovery today is no longer an academic question. The implications are staggering given the current approach to third-party spoliation. The handwriting is no longer just on the wall—it is stored in thousands of servers in multiple jurisdictions spread across the globe.

Businesses considering adoption of cloud services should weigh the potential implication for litigation preservation and production, and seek solutions from competent vendors that meet these long-view expectations. Judges and rule makers should look realistically at access to and control of data in the cloud when identifying active, reasonably accessible media and incorporating proportionality into their expectations for preservation. Lawmakers should consider whether the business of storing data should include an obligation to preserve evidence for litigation. In all cases, the goal should be to find ways of shifting the burdens of preservation to where

166. *See* Mark A. Berman and Aaron E. Zerykier, *Preservation of Electronic Information by Nonparties under the Private Securities Litigation Reform Act*, 16 SEC. LITIG. J. 10, 10 (2006), http://web2.customwebexpress.com/ganshore/UserFiles/File/PreservationOfElectronicInfo.pdf (ensuring preservation by nonparties during discovery stay under PSLRA requires preservation subpoena, for which a party first must seek relief from the court of the automatic stay by requesting "particularized discovery" and showing that such discovery is necessary either to preserve evidence or to prevent undue prejudice to that party).

they are most appropriate and most easily borne rather than simply reducing expectations and undermining the litigation process.

* * *