ELECTRONIC DISCOVERY IN THE CLOUD

ALBERTO G. ARAIZA[1]

ABSTRACT

Cloud Computing is poised to offer tremendous benefits to clients, including inexpensive access to seemingly limitless resources that are available instantly, anywhere. To prepare for the shift from computing environments dependent on dedicated hardware to Cloud Computing, the Federal Rules of Discovery should be amended to provide relevant guidelines and exceptions for particular types of shared data. Meanwhile, clients should ensure that service contracts with Cloud providers include safeguards against inadvertent discoveries and mechanisms for complying with the Rules. Without these adaptations, clients will be either reluctant or unprepared to adopt Cloud Computing services, and forgo their benefits.

INTRODUCTION

¶1 The conventional use of personal computers is evolving as shared computing becomes mainstream.[2] A type of shared computing called "Cloud Computing" stores client data and applications in shared data centers around the world[3] so that clients can access their data or run applications from any location with an Internet connection.[4] A Cloud provider can offer access to seemingly unlimited applications, operating systems, and hardware as services of the Cloud.[5]

---

[1] Duke University School of Law, J.D. expected, 2012; Tulane University School of Science and Engineering, M.E. in Biomedical Engineering; UCLA Henry Samueli School of Engineering and Applied Science, B.S. in Electrical Engineering. I would like to thank Professor Jeremy Mullem for his guidance in the writing of this iBrief.

[2] *See* Chris Weitz, *Cloud Computing and the New Normal*, COMPUTERWORLD (Nov. 8, 2010, 1:42 PM), http://www.computerworld.com/s/article/9195468.

[3] *See* Complaint of Electronic Privacy Information Center at 4, In re Google, Inc. & Cloud Computing Servs. (F.T.C. Mar. 17, 2009) ("[A]pplications reside on third party servers, managed by private firms, that provide remote access through web-based devices."), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[4] David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2216 (2009).

[5] *See* Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH., 2 (Oct. 7, 2009),

¶2 Cloud Computing is becoming very popular with a broad base of consumers. Websites such as Facebook turn personal computers into portals for clients to access and share images, videos, and text online.[6] In December 2010, Google unveiled its Cloud-based notebook, and commentators noted "there are several things worth raving about. . . . The machine starts up fast, snaps to life in an instant from sleep mode and has superb battery life. . . . [A]ll your apps, documents, settings and then some will be securely housed in the cloud."[7]

¶3 Cloud Computing is also becoming popular with businesses and public organizations. These entities are beginning to use Cloud Computing because it can reduce the need for IT floor space by 80% and save 60% on power costs, while tripling usage of IT assets.[8] Cloud Computing also allows clients to penetrate the marketplace with relative ease because it requires less capital than would be invested in traditional location-dependent hardware.[9] It is also sufficiently flexible to adapt to growth and usage spikes.[10] New business models may emerge where using Cloud Computing is essential to remain competitive in the marketplace.[11]

¶4 The introduction of Cloud Computing to a variety of industries has presented new complexities in the discovery phase of litigation. Pretrial discovery procedures involve delineating the scope of discoverable electronically stored information (ESI) as potentially leading to relevant evidence.[12] In Cloud Computing, shared data centers housing ESI are central to discovery. Although the Federal Rules of Discovery (Rules) were

---

www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf; *see also* Jonathan Strickland, *How Cloud Computing Works*, HOWSTUFFWORKS, http://communication.howstuffworks.com/cloud-computing1.htm (last visited Nov. 16, 2010).

[6] FACEBOOK, http://www.facebook.com (last visited Nov. 15, 2010).

[7] Edward C. Baig, *Google Chromebook: Much to Rave About at First Look*, USA TODAY, http://www.usatoday.com/tech/columnist/edwardbaig/2010-12-16-baig16_ST_N.htm?csp=hf (last updated Dec. 16, 2010).

[8] Andrew C. DeVore, *Cloud Computing: Privacy Storm on the Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 367–68 (2010) (noting the federal government will push out data dramatically into the Cloud); *see also The Benefits of Cloud Computing: A New Era of Responsiveness, Effectiveness, and Efficiency in IT Service Delivery*, IBM (July 2009), ftp://public.dhe.ibm.com/common/ssi/ecm/en/diw03004usen/DIW03004USEN.PDF.

[9] *See* Weitz, *supra* note 2.

[10] *Id.*

[11] *See, e.g.*, DeVore, *supra* note 8, at 368 ("[M]ajor providers [Microsoft and Google] recognize that this may well be the future of computing, particularly in the corporate world.").

[12] *See* FED. R. CIV. P. 26(b).

designed with an inherent flexibility and applicability to technological developments in personal computing,[13] they cannot effectively be adapted to the Cloud Computing context.

¶5 Discovering ESI in a Cloud, where clients share resources, is complex for two significant reasons. First, Cloud Computing puts client data under the control of a third-party Cloud provider. Rule 34(a) of the Federal Rules of Civil Procedure state that a party may serve a request to produce ESI in the responding party's "possession, custody, or control."[14] These criteria are vague, and as a result of a third party's control over a client's data, key evidence residing in a Cloud may be outside the scope of discovery. Second, because Cloud Computing services deal with a large number of clients and may intermingle clients' resources, isolating or retrieving the physical storage medium of one client's data in a lawsuit may adversely affect other clients who are not involved in the litigation.

¶6 The Rules are not flexible enough to encompass the technological paradigm shift to Cloud Computing. Specifically, the Rules do not provide guidelines for the production, preservation, and spoliation of ESI in a shared environment. This problem may be mitigated through technological means or by changing the Rules. Further, negotiating the terms of a contractual relationship between a Cloud provider and client may provide sufficient protection for both parties. Clients should consider whether their service contracts include sufficient safeguards against inadvertent discoveries of data, accurate indications of costs, and mechanisms for complying with the Rules.

I. THE FUTURE OF CLOUD COMPUTING

A. Technical Features

¶7 The phrase "Cloud Computing," under which the decentralized service is marketed, suggests that it is user-friendly and strips away any semblance of complexity from the minds of consumers.[15] The service, though intangible and novel, is extremely accessible, and the underlying

---

[13] *See* FED. R. CIV. P. 34 advisory committee's note.
[14] FED. R. CIV. P. 34(a).
[15] *See* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199–1200 (2010) ("This structure closely resembles the early mainframe computing model; instead of a 'dumb terminal' designed solely to access a mainframe's resources, the personal computer is beginning to serve as a 'dumb terminal' to access cloud computing's resources via the Internet.").

technology of Cloud Computing encompasses several familiar technologies, collectively deployed in new ways.[16]

¶8 Cloud providers essentially virtualize the same physical resources (such as processors and storage servers) to service multiple dispersed clients.[17] Cloud providers also divide "the tasks of running applications and storing data into small chunks," and then allocate the chunks among various distributed resources.[18] These resources are dynamically partitioned according to client demand.[19] That is, computing resources are divided according to what clients need, when they need them. Thus, one benefit includes maximizing access to seemingly limitless computing resources.

¶9 Familiar computer applications are making their way into the Cloud, arguably increasing the productivity of their users. Early email services relied on applications residing on storage devices contained in personal computers, but localized email is increasingly migrating to webmail.[20] Webmail resides in remote data centers shared by clients, and is accessible from anywhere, over the Internet.[21] Productivity software, such as Microsoft Office, is also shifting into the Cloud.[22] Pushing its Office suite into the Cloud allowed Microsoft to compete with Google Docs, which was released in 2007 and has always resided in the Cloud.[23]

---

[16] *Id.*

[17] Tyrone Grandison et al., *Towards a Formal Definition of a Computing Cloud*, 2010 IEEE 6TH WORLD CONGRESS ON SERVICES 191.

[18] *See* Robison, *supra* note 15.

[19] Mell & Grance, *supra* note 5, at 1.

[20] *See* George Jiang, Note, *Rain or Shine: Fair and Other Non-Infringing Uses in the Context of Cloud Computing*, 36 J. LEGIS. 395, 413 (2010) ("A number of public cloud applications are already available for tasks such as word processing, e-mail, video storage and playback, and data storage.").

[21] *See* Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 5 (2008) ("Computing power was first highly centralized with mainframes, and then decentralized through the switch to minicomputers and PCs. With the cloud, content and computing power will increasingly be managed centrally.").

[22] *See, e.g.*, *Microsoft Web Apps: Office Goes to the Web*, MICROSOFT NEWS CENTER (Sept. 17, 2009), http://www.microsoft.com/presspass/features/2009/sep09/09-17officewebapps.mspx ("Our mission with the upcoming release of Microsoft Office 2010 is to deliver a great productivity experience . . . . With Office Web Apps people can access, share and work on Office documents from virtually anywhere with an Internet connection.").

[23] *See* Ian Paul, *Microsoft Office vs. Google Docs: A Web Apps Showdown*, PCWORLD (Jul. 13, 2009, 9:50 AM), http://www.pcworld.com/article/168309 ("[Microsoft] unveiled as a part of Office 2010 a suite of Microsoft Office Web apps that will compete directly with Google Docs."); *see also* Kevin Cross et al.,

¶10 Cloud services make it possible to share resources located throughout the world.[24] For example, Microsoft, Sun Microsystems, and Google have contemplated placing data centers in Siberia, abandoned coalmines, and on ships at sea, respectively.[25] Interestingly, Google acquired a patent for placing data centers on ships to obtain power from the "natural motion of the water" and to use seawater to carry heat away.[26] Placing data centers in unusual locations may make Cloud Computing even more appealing because of the technical benefits of using the natural environment to power the data centers and to control their temperatures.

B. Economic Benefits

¶11 Analysts predict that 9% of all IT consumer spending will be for Cloud Computing services by 2012, which reflects a doubling of demand from 2008.[27] Cloud Computing offers businesses lower costs and accommodates growth with dynamic access to resources and flexible purchasing plans.[28] The cost benefit of outsourcing while maintaining instant and seemingly unlimited access to computing resources will provide businesses with a competitive edge.[29] Cloud providers, such as Amazon, Google, and Microsoft, only charge about $0.10 per hour for basic

---

Google Docs, WEB 2.0 TOOLS – NEW POSSIBILITIES FOR TEACHING AND LEARNING (July 8, 2010), https://wiki.itap.purdue.edu/display/INSITE/Google+Docs#GoogleDocs-what ("Beginning in February 2007 all Google users had were allowed access to Google Docs, which has many of the same abilities as MS Word or Openoffice.org Writer.").

[24] *See* DeVore, *supra* note 8 ("[C]ompanies are very interested in having services that make it easy for workers across the organization and across the world to use those services collaboratively.").

[25] Murad Ahmed, *Google Search Finds Seafaring Solution*, THE TIMES, Sept. 15, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4753389.ece; *see* U.S. Patent No. 7,525,207 (filed Feb. 26, 2007).

[26] U.S. Patent No. 7,525,207 col.2 l.27–31 (filed Feb. 26, 2007).

[27] Frank Gens, *IT Cloud Services Forecast – 2008, 2012: A Key Driver of New Growth*, IDC EXCHANGE (Oct. 8, 2008), http://blogs.idc.com/ie/?p=224.

[28] *See* Jiang, *supra* note 20 ("[C]loud service providers have control over the content that they make available and can monitor usage statistics. . . . These attributes provide different access plans, such as the pay-per-use model or an ad-supported free access model.").

[29] *See* DeVore, *supra* note 8 ("Cloud computing also offers potentially significant advantages with regard to cost savings and efficiency."); *see also* Weitz, *supra* note 2 ("Growth of cloud computing adoption is indeed rapid when the price of entry approaches zero for the smallest subscribers.").

processing requests.[30] Some analysts predict that these costs will soon decline by 5% to 20%.[31] These benefits allow businesses to "be competitive and to react faster to the market demands."[32]

C. The Legal Implications

¶12 Although sharing resources produces positive externalities, it also gives rise to many legal issues. For example, the data in data centers may be subject to foreign laws or no laws at all.[33] Cloud providers may also limit the control a business has over data it places in a Cloud.[34] These factors will complicate a client's effort to defend itself against discovery requests.

¶13 Attorneys recommend that their clients "have [a] clear understanding of what [a] cloud provider will do in response to legal requests for information" and "[n]egotiate roles for response to [electronic] discovery requests."[35] Clients should "[u]nderstand and negotiate where [their] data will be stored, what law controls and possible restrictions on cross-border transfers."[36] Unfortunately, such advice may fail to reach the

---

[30] Udayan Banerjee, *Cloud Economics – A Platform Comparison*, UDAYAN BANERJEE'S BLOG – FROM THE OTHER SIDE (Jan. 21, 2010, 1:12 PM), http://setandbma.wordpress.com/2010/01/21/cloud-economics-a-platform-comparison.

[31] *See, e.g.*, Rachel Lebeaux, *What's Behind Declining Prices for Application Hosting Services*, TOTALCIO (Apr. 3, 2009, 1:45 PM), http://itknowledgeexchange.techtarget.com/total-cio/what's-behind-declining-prices-for-application-hosting-services ("[A]nalyst firm Gartner Inc. predicts that the cost of outsourcing IT infrastructure will decrease 5% to 20% during the next two years.").

[32] Giuseppe Minutoli et al., *Virtual Business Networks with Cloud Computing and Virtual Machines*, INT'L CONF. ON ULTRA MODERN TELECOMM. & WORKSHOPS, Oct. 2009, at 1, *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5345440.

[33] *See* Paul T. Jaeger et al., *Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, 14 FIRST MONDAY 5 (2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2456/2171 ("The laws of any nation where a data center is located will apply, and many nations do not have nearly the civil rights safeguards that the United States does.").

[34] Jiang, *supra* note 20.

[35] Laurin H. Mills, *Legal Issues Associated with Cloud Computing*, NIXON PEABODY, 16, 21 (2009), http://www.secureit.com/resources/Cloud%20Computing%20Mills%20Nixon%20Peabody%205-09.pdf.

[36] *Id.* at 22.

masses of inexperienced clients using Cloud services, who do not know what to anticipate during litigation.

II. AN OVERVIEW OF ELECTRONIC DISCOVERY

¶14 Electronic discovery is "any process in which electronic data is sought, located, [and] secured, with the intent of using it as evidence in a civil or criminal legal case."[37]

A. Electronically Stored Information

¶15 The Rules state that "a party must . . . provide to other parties . . . a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses."[38] A party may request the production of ESI "in the responding party's possession, custody, or control . . . stored in any medium from which information can be obtained."[39] A party does not have to provide discovery of ESI "from sources that the party identifies as not reasonably accessible because of undue burden or cost."[40] The use of the phrase "electronically stored information" was "intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."[41]

B. Discovery of Metadata

¶16 Metadata is a type of discoverable ESI.[42] Metadata is information attached to the data it describes, which may include a user name, comments, document versions, the names of servers storing saved data, and the like.[43] Another form of metadata is "tagging, which gives you the ability to

---

[37] Stephen Biggs & Stilianos Vidalis, *Cloud Computing: The Impact on Digital Forensic Investigations*, INT'L CONF. FOR INTERNET TECH. & SECURED TRANSACTIONS, Nov. 2009, at 2, *available at* http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5402561.

[38] FED. R. CIV. P. 26(a)(1)(A)(ii).

[39] FED. R. CIV. P. 34(a).

[40] FED. R. CIV. P. 26(b)(2).

[41] FED. R. CIV. P. 34 advisory committee's note.

[42] *See* Charles R. Ragan et al. eds., *The Sedona Guidelines: Best Practice & Commentary for Managing Information & Records in the Electronic Age*, SEDONA CONF. WORKING GROUP SERIES, 13, 29–30 (Sept. 2005), http://www.sedonaconference.com/content/miscFiles/TSG9_05.pdf.

[43] *Find and Remove Metadata (Hidden Information) in Your Legal Documents*, WORD HELP AND HOW-TO, http://office.microsoft.com/en-us/word-help/find-and-remove-metadata-hidden-information-in-your-legal-documents-HA001077646.aspx (last visited Feb. 12, 2011).

identify and reference people in photos, videos and notes."[44] The Rules state that metadata "may be among the topics discussed in the Rule 26(f) [pretrial] conference,"[45] but the Rules Advisory Committee's description of metadata does not offer much guidance for targeting such information through discovery:

> Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image.[46]

¶17 The lack of direction from the Rules is troubling because computer programs routinely generate metadata and such data may be crucial in litigation.[47] Operating systems "enrich files with metadata" to improve search and organization capabilities,[48] and metadata has already proven to serve as key evidence in some trials.[49]

¶18 Although the Rules suggest the production of metadata absent an affirmative showing of need should be denied,[50] federal courts have attempted to devise frameworks for compelling its production.[51] In

---

[44] Tom Occhino, *Tag Friends in Your Status and Posts*, THE FACEBOOK BLOG (Sept. 10, 2009, 3:01 PM), http://blog.facebook.com/blog.php?post=109765592130.

[45] FED. R. CIV. P. 26 advisory committee's note.

[46] *See id.*

[47] *See* Scott Nagel, *Embedded Information in Electronic Documents: Why Metadata Matters*, LAW PRACTICE TODAY (July 2004), http://www.abanet.org/lpm/lpt/articles/ftr07044.html; *see also* Damian Vargas, Note & Comment, *Electronic Discovery: 2006 Amendments to the Federal Rules of Civil Procedure*, 34 RUTGERS COMPUTER & TECH. L.J. 396, 398–99 (2008).

[48] *Windows Vista metadata*, VISION (Jan. 2006), http://www.lcbridge.nl/vision/vistametadata.htm.

[49] *See, e.g.*, Krumwiede v. Brighton Assocs., LLC, No. 05-C-3003, 2006 U.S. Dist. LEXIS 31669, at *26–31 (N.D. Ill. May 8, 2006) (entering a default judgment against a former employee for breach of a restrictive covenant based on metadata showing the employee had deleted and altered thousands of files).

[50] Shannon M. Curreri, Note, *Developments in the Law: II. Defining "Document" in the Digital Landscape of Electronic Discovery*, 38 LOY. L.A. L. REV. 1541, 1548 (noting that a prior draft of the advisory committee note quoted the Manual for Complex Litigation (4th) § 11.446 that "production requests seeking files with all associated meta data 'should be conditioned upon a showing of need or sharing expenses.'").

[51] *See, e.g.*, Williams v. Sprint/United Mgmt., 230 F.R.D. 640 (D. Kan. 2005).

Williams v. Sprint/United Management, a federal district judge interpreted the phrase "[a] party must produce documents as they are kept in the usual course of business" in Rule 34(b)[52] to mean electronic files "with their metadata intact."[53] It was further ruled that metadata is to be produced even if it is not explicitly part of a request for production.[54]

¶19 Transient data, including metadata, may constitute discoverable ESI. For example, in *Columbia Pictures, Inc. v. Bunnell*, the court ruled that data stored on RAM constitutes ESI.[55] The court held that RAM data is "'stored' [information] under the plain meaning of the unambiguous language of Rule 34."[56] Therefore, even metadata that is temporarily stored may constitute ESI.

C. The Duty to Preserve

¶20 There is generally no duty to preserve documents, but a "preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order . . . in the case."[57] A "litigation hold" is a notice to a party that triggers the preservation of ESI by requiring "intervention in the routine operation of an information system" to suspend the normal destruction of material.[58] The duty to preserve may also arise without notice when litigation is "reasonably anticipated."[59]

¶21 Under a good faith requirement, a party is "not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve."[60] Litigants may separate out ESI (by transferring ESI to another storage device) to comply with the retention and access requirements of discovery and to avoid sanctions for spoliation.

---

[52] FED. R. CIV. P. 34(b).
[53] *See Williams*, 230 F.R.D. at 653–54.
[54] *Id.*
[55] 245 F.R.D. 443, 447 (C.D. Cal. 2007); *but see* Vargas, *supra* note 47, at 410 ("RAM is not used to store or record data. . . . Data processed in RAM is constantly overwritten.").
[56] *Columbia Pictures, Inc.*, 245 F.R.D. at 447.
[57] *See* FED. R. CIV. P. 37 advisory committee's note.
[58] *Id*.
[59] *See, e.g.*, Trigon Ins. Co. v. United States, 204 F.R.D. 277, 287 (E.D. Va. 2001) ("[I]f a party has notice (by discovery request, by the provisions of a rule regarding disclosure, or otherwise) . . . , that party is under a duty not to take actions that would result in the destruction of the evidence.").
[60] *See* FED. R. CIV. P. 37(f); *see also* FED. R. CIV. P. 37 advisory committee's note.

D. Spoliation

¶22 Spoliation is the deliberate or inadvertent loss, modification, or destruction of evidence by a party on notice of litigation who failed to take appropriate steps to preserve data.[61] A popular test applied by federal courts to determine when sanctions for spoliation should apply requires showing that a spoliator had a duty to preserve, a culpable state of mind, and that the destroyed evidence was relevant to a party's claims or defenses.[62] The required level of culpability varies between courts.[63] For example, the Eighth and Tenth Circuits require intentional misconduct or bad faith, but the Second Circuit held that "neither bad faith nor intentional misconduct is required."[64] Some scholars claim that imposing sanctions for spoliation is necessary because failing to preserve evidence not only "prevents a party from adequately proving or defending a claim at trial" but also "undermines the efficacy of the adversarial system."[65]

¶23 Applying these spoliation tests to Cloud Computing may prove to be difficult, and therefore must be adapted to this new context. Notably, the Rules state, "the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part."[66] Further, "absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system."[67] Thus, litigants may be unsure how they are supposed to harmonize the Rules with federal appellate court tests.

III. DISCOVERY IN THE CLOUD

¶24 The Rules require litigants to "discuss any issues about preserving discoverable information[] and develop a proposed discovery plan" during a pretrial conference.[68] Litigants must discuss discovery issues unique to Cloud Computing to "reduce prices and resolve potential complications early in litigation."[69] These requirements create "an affirmative duty on outside counsel to investigate the document retention policies of their

---

[61] *See* Vargas, *supra* note 47, at 406.
[62] *Id.*
[63] *Id.*
[64] *Id.* at 408.
[65] James T. Killelea, Note, *Spoliation of Evidence: Proposals for New York State*, 70 BROOK. L. REV. 1045, 1046 (2005).
[66] FED. R. CIV. P. 37 advisory committee's note.
[67] *Id.*
[68] FED. R. CIV. P. 26(f)(2).
[69] *See* Lauren Katz, Note, *Current Development 2008-2009: A Balancing Act: Ethical Dilemmas in Retaining E-Discovery Consultants*, 22 GEO. J. LEGAL ETHICS 929, 934 (2009).

clients during the earliest stages of representation"[70] and place "a high burden of technical knowledge on attorneys."[71]

¶25 Clients rightfully fear adverse discovery of their ESI.[72] For example, if third parties get access to trade secret information stored in a Cloud through discovery, "that could destroy the legal protection of trade secrets."[73] The Rules are "expansive and include[] any type of information that is stored electronically."[74]

¶26 Discovering ESI in the Cloud may also create liabilities for clients of the Cloud by inadvertently retrieving ESI belonging to other clients. For example, a sector isolated from a shared storage medium may contain data from other Cloud clients. This data shared among clients of a Cloud is discoverable because it is "fixed in a tangible form" and "stored in a medium from which it can be retrieved and examined."[75] Although major Cloud providers may include safeguards to ensure security and privacy, an increasing demand for Cloud services may spawn discount providers offering fewer safeguards against the unintentional disclosure of other clients' data.

¶27 Storing ESI in the Cloud may also provide litigants with loopholes to avoid divulging certain information. Multiple layers of data are generated by various clients and managed by Cloud providers, and such ESI may not be in the possession, custody or control of the litigant.[76] The data layers may include client-specific data, client-specific metadata, and metadata common to several clients,[77] which may be unique to an application, generated by multiple clients, or stored in a shared repository.[78] Common metadata may be maintained in repositories shared between clients, which makes it a "major problem" to "isolate [that] data and maintain the security."[79] Therefore, that data may not be in the possession,

---

[70] Joseph Gallagher, Note, *E-Ethics: The Ethical Dimension of the Electronic Discovery Amendments to the Federal Rules of Civil Procedure*, 20 GEO. J. LEGAL ETHICS 613, 617 (2007).
[71] Katz, *supra* note 69.
[72] *See* Vargas, *supra* note 47, at 405; *see also* Mills, *supra* note 35, at 17.
[73] Mills, *supra* note 35, at 17.
[74] FED. R. CIV. P. 34 advisory committee's note.
[75] *Id.*
[76] Bhaskar Prasad Rimal & Mohamed A. El-Refaey, *A Framework of Scientific Workflow Management Systems for Multi-Tenant Cloud Orchestration Environment*, 2010 WORKSHOPS ON ENABLING TECHS.: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES 88, 90 (2010) [hereinafter *Multi-Tenant Cloud Orchestration Environment*].
[77] *Id.*
[78] *See id.*
[79] *Id.*

custody or control of a litigant, and thus not subject to discovery. Consequently, applying the Rules to a Cloud may create liabilities for clients of a Cloud and loopholes for litigants.

A. Sharing Resources and Metadata

¶28 Inadvertently producing or preserving ESI belonging to other clients of a Cloud is likely to have significant repercussions. For example, "in many jurisdictions, inadvertent production of privileged data constitutes a waiver of privilege."[80] In *Marrero-Hernandez v. Esso Standard Oil Co.*, an "errant mouse click" led to the inadvertent production of "approximately 1500 potentially privileged documents" that merged with unprivileged documents.[81] Although the defendant claimed the documents were privileged,[82] the court stated that if parties "opt to use technological resources to store privileged information, they should also provide the necessary protection for precisely that information."[83]

¶29 Further, allowing parties to discover common metadata in a Cloud is problematic. The *Williams v. Sprint/United Management Co.* court held that "the producing party should produce the electronic documents with their metadata intact."[84] A party may move for a protective order when asked to produce metadata if it is "not reasonably accessible" and will result in "undue burden and cost."[85] However, common metadata may be readily accessible without undue burden or cost because it is stored in a common repository, yet its discovery may harm other clients.[86] If, however, courts grant protective orders to protect those other parties, they may incentivize clients to "hide" their information as common metadata in the Cloud. If courts do not grant protective orders, then discovery will reveal the common metadata, possibly disclosing private information about third parties.

¶30 Requiring the production of metadata attached to documents is particularly troubling because Cloud metadata is increasingly inseparable among clients.[87] Multiple Cloud providers may share metadata in an

---

[80] Vargas, *supra* note 47, at 405; *see* ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE 7–21 (2007).
[81] No. 03-1485, 2006 U.S. Dist. LEXIS 47738, at *6 (D.P.R. July 11, 2006).
[82] *Id.*
[83] *Id.* at *15.
[84] 230 F.R.D. 640, 652 (D. Kan. 2005).
[85] *See* FED. R. CIV. P. 26(b)(2)(B), 26(c).
[86] *See Multi-Tenant Cloud Orchestration Environment*, *supra* note 76.
[87] Lori MacVittie, *Who Owns Application Delivery Meta-data in the Cloud?*, DEVCENTRAL WEBLOG (Feb. 6, 2009, 4:39 AM), http://devcentral.f5.com/weblogs/macvittie/archive/2009/02/06/who-owns-application-delivery-meta-data-in-the-cloud.aspx [hereinafter *Who Owns Metadata*].

architecture optimized for interoperability and portability.[88] Interoperability is the ability to exchange and use client data between different Cloud providers, and portability is the ability to deliver data anywhere on demand.[89] If Cloud providers were forced to change their delivery and security policies to maintain these two functions, then clients may lose metadata or lose control over copies of metadata residing in multiple data centers.[90] For example, metadata generated by one Cloud provider may be inadvertently lost when a client accesses the same metadata through a second provider.[91]

B. Preserving Client Data

¶31 The duty to preserve ESI under an ongoing litigation hold conflicts with the "real advantage" of Cloud Computing, which is to increase "flexibility and responsiveness" of shared resources among clients.[92] For example, Cloud Computing dynamically allocates virtual storage volumes to clients, which may comprise multiple physical storage volumes partitioned according to client demand.[93] ESI from a single client can therefore be stored across multiple physical storage volumes, wherever there is available capacity.[94] Thus, preserving (or saving) ESI detracts from the elasticity of resources for other clients who may have a demand for the same resources.[95]

¶32 Implementing preservation techniques may require isolating Cloud resources, which can cause performance degradation for other clients because they are forbidden access to the same resources.[96] Further, a Cloud provider may isolate physical resources, rather than virtual ones, to ensure full compliance with the Rules. Isolating a physical resource may preserve data belonging to multiple clients who share that same physical resource; the data may have otherwise been routinely deleted at the request of clients who are not parties to a litigation hold. The subsequent release of the physical resource from the litigation hold may frustrate the routine business operations of other clients because their data will remain preserved. These problems are further complicated when multiple Cloud providers service the same clients.

---

[88] *See id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *See* Weitz, *supra* note 2.
[93] *See* Mell & Grance, *supra* note 5, at 1; *see also* Grandison, *supra* note 17.
[94] *See* Mell & Grance, *supra* note 5, at 1.
[95] *Id.*
[96] *See Who Owns Metadata*, *supra* note 87.

C. Identifying Who Controls Data

¶33 The Rules require that a client produce ESI in its possession, custody, or control. In Cloud Computing, it is a client's "control" that is most difficult to define because Cloud providers are custodians of the ESI they hold in data centers.[97] A client is deemed to have control over ESI "so long as the party has the legal right or ability to obtain the documents from another source upon demand."[98] Thus, clients may not have legal or actual control over common metadata that serves as key evidence.[99]

¶34 The requirements imposed on Cloud providers under the Rules are ambiguous at best. The Stored Communications Act (SCA) provides safeguards for clients against compelled disclosures imposed on Cloud providers.[100] A client, however, will only benefit from the SCA "when a cloud provider expressly limits its access" to client data "for the purposes of providing computer storage or processing functions."[101] Inexperienced clients who allow Cloud providers access to their data "without specifying the limits of that authority" are generally not protected by the SCA.[102] For example, clients of Gmail are probably not protected because Google reviews emails to provide client-specific contextual advertising.[103] More generally, Cloud Computing clients may be disqualified from "seeking refuge from disclosure under the Act" when Cloud providers use a "service of retrieval" function "for using applications or data stored with the cloud provider" because this function permits Cloud providers to access client data content.[104]

---

[97] *See* Bifferato v. States Marine Corp., 11 F.R.D. 44, 46 (S.D.N.Y. 1951) (indicating that "the test is control and not possession"); *see also* Am. Rock Salt Co. v. Norfolk S. Corp., 228 F.R.D. 426, 460 (W.D.N.Y. 2005) ("Control [for FED. R. CIV. P. 34(a) purposes] is defined as 'the legal right, authority, or ability to obtain upon demand documents in possession of another.'") (quoting Florentia Contracting Corp. v. Resolution Trust Corp., 11993 U.S. Dist. LEXIS 5275, at *7 (S.D.N.Y. Apr. 22, 1993)).

[98] *See* Mercy Catholic Med. Ctr. v. Thompson, 380 F.3d 142, 160 (3d Cir. 2004).

[99] *See* Facebook, Inc. v. Power Ventures, Inc., No. 08-05780, U.S. Dist. LEXIS 93517, at *12–13 (N.D. Cal. July 20, 2010) (asserting a claim by Facebook.com that another social network cannot make a copy of a user's own data even if the user provides full permission).

[100] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711).

[101] *See* Robison, *supra* note 15, at 1222.

[102] *Id.*

[103] *See id.* at 1213.

[104] *See* Robison, *supra* note 15, at 1218–19; *see also* Flagg v. City of Detroit, 252 F.R.D. 346, 358–59 (E.D. Mich. 2008) (noting the SCA requires the provider not be "'authorized to access the contents of any such communications

D. Increased Legal Risks

¶35 Cloud Computing poses new challenges for litigants to avoid sanctions.[105] The inadvertent deletion of ESI, under a litigation hold, by a routine operation of a Cloud provider or through actions from clients of the same provider may result in spoliation claims.[106] It is unclear if the safe harbor provision[107] of the Rules will apply when clients share operations of computer systems. Even basic litigation holds may impose undue burdens and costs on a litigant or on multiple clients of a Cloud not associated with the matter.

IV. SOLUTIONS FOR DISCOVERY IN THE CLOUD

A. Contractual Relationships

¶36 One key to mitigating risks associated with discovery in a Cloud is negotiating the terms of a service contract to define the legal rights of a provider and client. Of course, this solution assumes equal bargaining power between a Cloud provider and client.[108] While powerful entities may successfully negotiate favorable terms of a contract, smaller or inexperienced clients may be subject to one-sided agreements.[109] For example, the city of Los Angeles negotiated a contract with Google to provide an email system for city employees.[110] The contract included

---

for purposes of providing any services other than storage or computer processing.'") (quoting 18 U.S.C. § 2702(a)(2) (2006)).

[105] *See, e.g.*, Phillip M. Adams & Assocs. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193 (D. Utah 2009) (finding sanctions were appropriate because the defendant's "system architecture of questionable reliability which has evolved rather than been planned, operates to deny . . . access to evidence"); *see also* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 215, 222 (S.D.N.Y. 2003).

[106] *See* COMM. ON RULES OF PRACTICE & PROCEDURE, REPORT OF THE JUDICIAL CONFERENCE, 32 (2005), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2005.pdf ("[I]t can be very difficult to interrupt or suspend the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete or update, on an ongoing basis, without creating problems.").

[107] *See* FED. R. CIV. P. 37(e) (noting that shelter from sanctions for spoliation under the safe harbor provision of the Rules is available when ESI is lost due to the "routine, good faith" operation of computer systems).

[108] *See* DeVore, *supra* note 8, at 373.

[109] *Id.*

[110] David Sarno, *Los Angeles Adopts Google e-mail System for 30,000 City Employees*, L.A. TIMES, Oct. 27, 2009, http://latimesblogs.latimes.com/technology/2009/10/city-council-votes-to-adopt-google-email-system-for-30000-city-employees.html.

provisions where Google would "compensate the city in the event that the Google system was breached and city data exposed or stolen."[111] In contrast, the standard Gmail service contract with individual customers allows Google to access client information and email; it also notes that Google "processes personal information" on servers in the U.S. and in other countries.[112]

¶37 Clients should also be cautious about using the services of smaller, less-expensive, competing Cloud providers who might lack the resources to properly accommodate discovery requests. However, clients may have more bargaining power with smaller Cloud providers. Still, clients ought to be aware that the providers will probably offer fewer reliable service features.

¶38 A service contract should provide safeguards to protect clients from the inadvertent discovery of ESI and include procedural guidelines to facilitate the discovery process. Provisions should delineate the types and amount of metadata routinely preserved in a designated repository and define client rights to access that metadata. Provisions should ensure that clients remain protected under the SCA by preventing Cloud providers from unilaterally accessing, viewing, or providing client ESI to government agencies or other parties.[113] A contract should, at least, require Cloud providers to notify clients in advance of accessing client ESI, which would allow clients time to secure privileged information.[114] The contract should also impose restrictions on the location of data centers storing client ESI because the laws in some countries may trump U.S. security and privacy provisions.[115]

B. Technical Solutions

¶39 In addition to negotiating the terms of Cloud Computing services, there are several possible technical solutions. First, a client may adopt a hybrid approach to storing data by which the majority of data is stored in a public Cloud and sensitive ESI is stored in a private Cloud.[116] Of course,

---

[111] *Id.*
[112] *Privacy Policy*, GOOGLE (Oct. 3, 2010), http://www.google.com/intl/en/privacy/privacy-policy.html.
[113] *But see* DeVore, *supra* note 8, at 372 ("Most Terms of Service allow the provider of the cloud service access to data, the ability to view data, and the ability to turn data over in the event that the Government or a third party asks for it. Often that's true without any notice to the consumer.").
[114] *See id.*
[115] *See* Mills, *supra* note 35, at 7.
[116] *See* DeVore, *supra* note 8, at 373 ("[F]or truly sensitive and confidential information, think seriously before putting that information in the cloud at all in light of all the privacy and security issues that are arising.").

this requires private infrastructure and remains limited to clients with greater financial resources. A hybrid approach may also require redundant applications stored in different types of Clouds or require indexing and channeling of sensitive metadata into a private Cloud.

¶40 Second, Cloud providers may consider developing an application that automatically isolates specified ESI and associated metadata when there is a litigation hold. Cloud providers may then offer the application as an added service to clients. A client may try to avoid sanctions by using this software program because its use demonstrates a good faith attempt to comply with the Rules.

¶41 Third, Cloud providers may track metadata, especially when considering the possibility of replicating, moving, or losing metadata as clients migrate between Clouds to access ESI from remote locations, and through different devices.

¶42 Finally, another solution may be to encrypt all ESI and metadata with client-specific keys such that the ESI, and metadata, remain indecipherable by other clients in case of an inadvertent production.

C. Revising the Rules

¶43 While negotiated contracts and technical changes may help individual clients, a universal solution requires amending the Rules. The test for "possession, custody, or control"[117] in the Rules requires a clarification of what degree of control distinguishes data subject to discovery in a shared environment. "Control" should be limited to ESI, including metadata, over which a party has exclusive or substantial control. If "control" is not given such a circumscribed meaning, exceptions to the current liberal definition should exist to avoid the inadvertent production or destruction of ESI shared with other parties. Further, the Rules should not allow discovery of physical storage volumes in a shared environment, or they should limit discovery only to virtual volumes. If physical storage volumes remain discoverable, then Cloud providers should be required to provide fair notice to clients who may share the same resources.

¶44 The Rules should provide better guidelines for distinguishing different types of ESI (e.g., user-specific and common metadata) and define the scope of production and preservation owed by parties in a Cloud. The Rules should consider that clients may have limited control over key ESI and that Cloud providers control common metadata. Furthermore, safeguards to prevent the risk of inadvertently preserving ESI belonging to other Cloud clients should be addressed by the Rules. That is, they should provide for more procedural mechanisms than the mere ability to move for a

---

[117] FED. R. CIV. P. 34(a)(1).

protective order when clients are asked to produce metadata that is not reasonably accessible or results in undue burden and cost. There should be exceptions for reasonably accessible shared metadata that may unduly burden other clients.

D. Immediate Measures

¶45 Until the above remedies become commonplace and the Rules are amended, Cloud providers should devise procedural and usage guidelines to protect clients. The guidelines should aid clients to demonstrate a good faith effort to comply with the Rules and facilitate the discovery process. They should provide safeguards for clients and mitigate risks of sanctions by preventing the destruction of ESI after a litigation hold issues. To avoid claims of spoliation, a Cloud provider should provide a mechanism for gathering data fragmented across multiple data centers, isolating relevant data, and migrating that data to a repository where it will remain intact. Cloud providers should understand their roles as custodians of ESI they possess and outline instructions for their staff to respond to litigation holds.

V. CONCLUSION

¶46 The Federal Rules of Discovery do not effectively apply to clients of a Cloud. The shared nature of Cloud Computing requires limiting discovery to data in exclusive or substantial control by a client or whose discovery will not unduly harm other clients. In anticipation of the universal adoption of Cloud Computing, the Rules should provide guidance and exceptions for particular types of shared ESI. Meanwhile, clients should consider whether their service contracts include safeguards against inadvertent discoveries of data, indicate the costs for ongoing preservation, and provide mechanisms for complying with the duty to preserve and for securely applying and releasing litigation holds.[118] Inaction will stifle the adoption of Cloud Computing and deny the public its positive network effects.

---

[118] Venkat Rangan, *E-Discovery and the Cloud: The Duty to Preserve Electronically Stored Information (ESI)*, E-DISCOVERY BLOG 2.0 (May 28, 2010, 12:23 PM), http://www.clearwellsystems.com/e-discovery-blog/2010/05/28/e-discovery-and-the-cloud-the-duty-to-preserve-electronically-stored-information-esi.