Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

E-Discovery and the Cloud: Best Practices in the New Frontier

ReedSmith

reedsmith.com

E-Discovery and the Cloud: Best Practices in the New Frontier

Authors

Jennifer Yule DePriest, Partner – jdepriest@reedsmith.com

Claire Covington, Associate – ccovington@reedsmith.com

Introduction

During the past five years or so, lawyers and their clients have struggled to reconcile their discovery obligations under federal and state discovery rules with the ever-expanding digital universe. Indeed, as technology continues to evolve, the *digital sea* of electronically stored information ("ESI") produced by companies continues to rise. Consequently, the costs associated with creating new information technology (or "IT") infrastructure, and with maintaining and preserving (or hosting) ESI, also continue to rise. In many cases, the duality of rising costs and increased technological complexity have led companies to look to third-party providers for some or all of their infrastructure and hosting needs. In fact, third-party hosts and IT service providers of varying sizes and offerings are essentially a ubiquitous reality in our digital economy today. Consequently, it should not be a surprise that cloud computing represents a natural, albeit somewhat different, model in the evolution of the use of IT.

Cloud computing is the term ascribed to the industry shift and transformation from companies either hosting and managing their own applications and data on local servers, or entering into micro-hosting arrangements with third-party providers to a grid computing model in which users access a shared computing environment typically being provided by large and well-entrenched technology companies such as Google, Microsoft, IBM and Amazon. For many companies that have embraced cloud computing for all or some of the IT and hosting needs, gone are the days of purchasing departments ordering server after server and rack after rack, or negotiating co-location agreements in which their servers sit within some third-party's server farm in downtown Toronto, Miami or Seattle. Rather, the cloud is an entirely virtual environment with digital tributaries that span the globe, moving data from one server to another to achieve optimal data storage and retrieval capabilities, bandwidth optimization, and overall IT cost-effectiveness, providing all of a company's data storage, data processing and distribution needs on an as-needed basis (think "utility"). This has already begun to transform the traditional IT model for multinationals, and continuing the trend that began with hosting and outsourcing, will effectively relieve companies of the burden and expense of maintaining their own electronic data and monitoring their own IT infrastructure.[1] While there were good reasons, pre-dating the commercial use of the Internet, that the old timesharing models of the 1960s fell by the wayside and gave way to corporate IT infrastructure development, the environment has changed and cloud computing is an idea whose time may have now arrived.

So, what is it about the new age of discovery and terms like "cloud computing" that leave lawyers (and perhaps some clients) with a great degree of caution? Put simply, it is the existence of a tremendous amount of electronic data, the potential for lack of control over its location and attendant uncertainty about the ability to find and process relevant information in connection with a lawsuit. This fear lies in the fact that for purposes of meeting discovery obligations, a company's data is likely considered to be in the company's *legal* "control," though a third party actually has the data. Also uncertain is what is considered "reasonable" with respect to efforts to identify, preserve and collect relevant information "in the cloud" under the discovery rules.

This paper will briefly discuss discovery obligations under the Federal Rules, specifically with respect to e-discovery[2]; the "reasonableness" standard as it relates to identification, preservation and collection of ESI; and particularly electronic information stored in the cloud. In that regard, this paper will highlight issues to address with your cloud provider that may help you minimize cost and burden, and

help establish "reasonableness" for purposes of meeting your discovery obligations.

Discovery obligations

Discovery involves the identification, preservation, collection, review and production of relevant information in a party's possession, custody or control.[3]

Though living in the digital age may have made certain aspects of modern life much easier—fewer bankers' boxes and paper cuts, for instance—it has undoubtedly made litigation, and discovery in particular, more difficult and costly. So much more difficult, in fact, that the Federal Rules of Civil Procedure were amended in 2006 just to accommodate the rising tide of e discovery in litigation.[4]

The 2006 amendments to the Federal Rules expanded the scope of a party's discovery obligations to account for the increasing amount of business conducted electronically. Notably, the 2006 amendments expanded the definition of "document" under Rule 34 to include ESI, such as Microsoft Word, Excel and PowerPoint files, Adobe PDF files, database records, and CAD/CAM files.[5] The 2006 amendments to the Federal Rules also reaffirmed a party's obligation to adequately preserve relevant documents, including ESI.

Whether a party's efforts to identify, preserve and collect relevant information are sufficient under the Federal Rules is judged against a standard of reasonableness. When dealing with e discovery, the starting point for determining what is reasonable begins with the famous *Zubulake* decisions, authored by Judge Shira Scheindlin of the Southern District of New York. Most recently, in *Pension Committee v. Banc of America Securities, LLC*, Judge Scheindlin reiterated that "the duty to preserve means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence,"[6] and sanctioned numerous plaintiffs, some with an adverse inference. And yet despite the guidance given to litigants during the past five years or so from "think tanks" such as the Sedona Conference and the ever-expanding body of case law, reasonableness remains relatively undefined and dependent on the facts and circumstances of each case.

What *is* known is that the failure to take reasonably appropriate steps to preserve relevant information and to perform a reasonable search of pertinent repositories could result in sanctions for spoliation of evidence.

And though there is a dearth of case law about what is "reasonable" in terms of identifying, collecting and preserving data in the "cloud," the reasonableness standard undoubtedly applies to efforts in the cloud as well as other locations of ESI.

Rule 26(f) issues

Knowledge of the cloud provider's policies related to the identification, preservation and collection of your data is crucial for purposes of meeting your Rule 26(f) obligations. Rule 26(f) requires that parties meet early in the case to discuss, among other things, "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."[7] In today's discovery landscape, it is critical to come to Rule 26 conferences with a full understanding of potential e-discovery issues. If disputes about the reasonableness of preservation and/or collection efforts of ESI arise, the parties should raise them with each other and the court, if necessary, early in the case. Given the fact-specific inquiry with respect to reasonableness of your preservation and collection efforts (and the potential for severe sanctions for failure to adequately comply), it is likewise important to address ESI issues in the cloud, as discussed below, early in the case. These issues include, among others, identification of cloud provider(s) and sub-contractors, data retention and preservation policies for data in the cloud, and terms of access and ability to collect information from the cloud. It is important to raise problems in these areas before you are too far into the litigation and potentially subject to spoliation sanctions.

Notably, Rule 26(b)(2)(B) sets forth specific limitations with respect to ESI: "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." The burden is on the party from whom the discovery is sought to show that the ESI is not reasonably accessible. However, blanket assertions that data is inaccessible merely because it resides in a cloud will not pass muster. Understanding the terms of the cloud provider's policies regarding identification, preservation and collection of ESI will help determine the extent to which it is "reasonably accessible," and will provide a basis for negotiating cost shifting, production formats and production timelines.

Getting a handle on what you have

he threshold task in identifying, preserving and collecting relevant information is finding the information. Traditionally, identification of such information involved reviewing the contents of file cabinets and desk drawers for relevant paper documents. And although the process as it relates to

paper discovery is undeniably laborious, there are only so many file cabinets, desk drawers and boxes in which potentially relevant paper documents might be stored. In short, the locations are defined and finite.

The process of identifying relevant ESI, on the other hand, presents a multitude of challenges. Businesses today rely on a variety of electronic solutions for data creation, storage and maintenance. A quick review of the programs installed on an employee's desktop probably reveals an email exchange program such as Microsoft Outlook, document processing software such as Microsoft Word, and a database application such as Oracle for inventory management, customer contact information and accounts receivables. Relevant information might reside in any or all of these locations. And although possibly numerous, these locations are readily known, or ascertainable, by a company's IT personnel and database administrators.

A company's electronic infrastructure typically is created and managed by in-house IT personnel. As such, involving your IT personnel in locating relevant ESI is critical, as these individuals are the masters of data mapping,[8] in that they are responsible for setting up and administering individual user accounts, email accounts, networks, share drives and e-rooms. Thus, they know, or are able to find out, where ESI resides within (and outside of) the company. A party can comply with its discovery obligations by creating a data map, locating and conducting a reasonable search of the data repositories on the data map, and taking appropriate steps to preserve any responsive information.

e-Discovery and the cloud: identification, preservation and collection issues

So what happens when a company decides to outsource data services and storage to a cloud provider? The electronic landscape shifts, leaving a company's data map a little less clear. Unlike documents and traditionally maintained ESI, information in the cloud is not limited to finite areas. A company's data is no longer hosted and managed on networks and servers owned by the company. In fact, a single company's data may be stored on a variety of servers, each on a separate network, and potentially housed in a different country.[9] Identifying and collecting potentially relevant ESI is no longer as easy as having IT walk down the hall to copy someone's "My Documents" folder off of his or her desktop or laptop computer (to use a simple example).

Though cloud computing is a relatively new frontier, for purposes of e-discovery, the goal is to be able to demonstrate to a court that your efforts at all points in the process of identifying, preserving and collecting relevant information were *reasonable*. The following practices will help allow you to argue "reasonableness" at each step, and potentially reduce both costs and burden in doing so. For any of these steps, be prepared to work with a vendor who is knowledgeable about cloud computing issues.

Locating information in the cloud

As with traditionally stored ESI, *know where to find your data*. Before finding yourself in anticipation of litigation, consult with IT personnel to identify a comprehensive list of the company's cloud providers and potential locations of data. In this regard, follow up with the cloud provider to try to determine whether the cloud provider uses any sub-contractors for storing data. Also, be sure to inquire about where the cloud provider physically stores data and whether or not there are any specific issues regarding that data storage that you should be aware of, such as storage format and archiving schedules and capabilities.

Preserving information in the cloud

Cloud-stored data should be addressed in your document retention and destruction policies, as well as in litigation holds. As Judge Scheindlin decreed, the preservation obligation is triggered once a company reasonably anticipates litigation.[10] The first step in preserving data is the issuance of a litigation-hold notice to key custodians as well as to IT; in this new frontier, the hold notice should also be sent to the cloud provider(s). But the mere issuance of a litigation hold is not, in itself, sufficient—companies must take affirmative steps to preserve relevant ESI. Typically, companies must identify the key data custodians and take reasonable steps to preserve their data, be it through the imaging of their hard drives or the targeted copying of their user-created files, ceasing automatic deletion of email, and potentially preserving back-up tapes.

Follow-up steps within the cloud require that companies have a detailed understanding of various cloud provider policies. *First*, what, if anything, will the cloud provider do to implement your legal hold? If the cloud provider will not agree to implement a legal hold (including with respect to any sub-contractors it may use to provide services), it may be necessary to immediately "self-collect" the data before it gets lost or destroyed.[11] *Second*, what are the provider's data-retention and back-up policies? Will it suspend any data-destruction policies with respect to your data? Does the cloud provider outsource its data backup? Try to find out which parties are responsible for conducting, executing

and maintaining the data and backup. *Third*, what is the manner in which the data is maintained? On what kind of cloud is a party's data resident—public, private or hybrid? Is it kept separately from other companies' data? If not, how are different retention policies reconciled (assuming the cloud provider will follow its customers' retention policies)? Is the data "co-mingled" with other data on back-up tapes? If so, how can your data *reasonably* be extracted?

Knowing the answers to these questions will allow legal and IT personnel to make recommendations for data-retention policies and determinations about the need for backing up critical data upon reasonable anticipation of litigation. If the cloud provider will not agree to suspend destruction of relevant information once you find yourself in anticipation of litigation, work with your IT staff or a vendor to make alternate arrangements to preserve data maintained in the cloud.

Accessing and collecting information in the cloud

Collection of relevant electronically stored information can be one of the most costly, technologically demanding and labor intensive parts of the discovery process. Regardless of whether you self-collect or rely on a third-party vendor to perform a collection for you, several issues need to be addressed:

First, know *how* to access and collect your information. Ensure that the cloud provider has access to all data centers used for data storage, so that you are not faced with a situation in which your provider (or you) cannot access your data. Is the company's existing IT infrastructure compatible with the infrastructure of the cloud? If not, costs and the burden of retrieving information can greatly increase. Who can retrieve the information? Does your cloud provider allow for self-collection of custodian files? Are there access restrictions? Who is responsible for the costs to retrieve it—if the company bears the cost, what is it? If self-collection is not an option, you will likely incur the added expense of engaging a vendor to perform your data collections for you. In this regard, you will need to determine if the cloud provider will work with a vendor if necessary.

Second, in what format will the data be collected? As maintained in the ordinary course of business? As with any ESI, if metadata (*i.e.*, creation date, last modified date, etc.) is potentially important to the case, a vendor may be needed in order to preserve the modification, access and creation dates of the collected data. In that regard, costs and the burden of retrieving can greatly increase.

Third, can self-collection be accomplished with minimal upset to your daily computing environment? Or must the collection take place after hours so as not to interfere with server access and bandwidth needs, and if that is the case, what are the costs?

Again, knowing the answers to these questions will help with meeting Rule 26 obligations.

Negotiating with the cloud provider

There are various types of "clouds," including private, public and hybrid clouds. While most public cloud providers offer "take it or leave it" contracts, some cloud providers, depending on the type of provider and/or size of the account, for example, offer more flexibility in negotiating provisions with respect to data retention and preservation, implementation of a legal hold and data collection. At the outset of a relationship with a cloud provider, legal and IT should coordinate to ensure that these bases are covered. If you are able to negotiate, keep in mind the following points (and if you are not able to negotiate, make sure you are aware of the following issues so that you can address them as part of a reasonableness inquiry):

- For purposes of *identification*, know where your ESI will be located at all (or at least most) times. Ask the cloud provider to let you know the location of the servers on which your information will be stored. If you have an issue with certain information being hosted in certain states or countries, make that known to the cloud provider at the outset. Find out who is responsible for maintaining those servers and your data. Determine whether or not any sub-contractors are involved. If so, try to ensure that there is transparency as to who is handling your data, where your data is located, and further, that these sub-contractors will implement the identification, preservation and collection (as well as security and privacy) terms upon which you have agreed with the primary cloud provider. Similarly, the primary cloud provider should have the right to audit any data maintained by sub-contractors to ensure that these policies are properly enforced.
- For purposes of *preservation*, ensure that the cloud provider will implement, or at least adhere to, your data-retention and back-up policies according to your retention schedules. Try to secure agreement that the cloud provider (and any sub-contractor) will take steps

to preserve data within a reasonable time frame after receiving notice. Provide the cloud provider with a copy of your draft litigation-hold letter, and inform the cloud provider of your expectations regarding data preservation once you anticipate litigation. At a minimum, try to get a commitment that the provider will follow your instructions regarding preservation and ceasing deletion of data, including with any third-party sub-contractors. Also, ensure that you can conduct periodic quality control audits to assess the integrity of ESI hosted in the cloud.

- For purposes of *access and collection*, you should also make sure you know how to actually get to your data. Identify any limitations on access to your data once it has migrated into the cloud. Make sure the cloud provider's infrastructure is compatible with your existing IT infrastructure, that metadata will be preserved if necessary or important to your case, and that you will be able to access and collect your data, perhaps on short notice, as it is kept in the ordinary course of business. If your company is subpoenaed, you may need access to your data as it is maintained in the ordinary course of business within a short turn-around time.
- If the cloud provider is subpoenaed for your data, ensure that the cloud provider will notify you immediately upon receipt of the subpoena. You will also want to secure the cloud provider's cooperation in connection with any motion to quash or any protective order necessary to prevent the disclosure of your data. The contract should spell out the cloud provider's obligations in this regard.
- You will also want to ensure that the cloud provider will provide affidavits, declarations, or other testimony as necessary to establish chains of custody and authenticity for purposes of admissibility.
- Finally, try to incorporate provisions that shift associated costs to the cloud provider, especially those costs associated with preserving and collecting data maintained in the cloud.

The failure to address these issues up front could increase your costs in the context of your discovery obligations, and potentially offset any cost savings associated with using the cloud in the first instance. In addition, although untested as of yet, a company that had the opportunity to negotiate these provisions, but either missed the opportunity during the negotiations or otherwise waived these rights, may be subject to sanctions and penalties at a later date.

Call to action

Meeting discovery obligations when data is stored in the cloud need not be daunting. As a preliminary matter, identification, preservation and collection efforts can be more "reasonably" managed, reducing costs and lessening the inevitable burden, by managing data-retention pre-litigation. Reed Smith's e-discovery and technology specialists can provide guidance, create accurate and up-to-date data maps, and draft retention policies that comply with all laws governing retention of particular information, thereby helping to minimize e-discovery costs down the road, including costs associated with retrieving data from the cloud.

If possible, you should negotiate "up front" the issues noted above, which will help minimize the burden and costs associated with e-discovery in the cloud, and also help to establish that you have taken reasonable steps in connection with meeting your discovery obligations. Reed Smith's e-discovery and technology specialists can work with your IT and purchasing departments and assist in negotiating these provisions.

Many providers, however, offer "take it or leave it" contracts. If that is the type of agreement you have already entered into with a cloud provider, it is still critical to know the terms of your contract, to take reasonable steps to identify, preserve and collect relevant data in light of these terms, and, as discussed above, to be able to demonstrate that you took reasonable steps given the terms of the cloud provider's contract. You must also be able to explain the terms of your agreement with the cloud provider to a judge if necessary (for example, to the extent a dispute arises regarding the reasonableness of any of these steps in connection with a Rule 26(f) conference). Again, Reed Smith's litigators and e-discovery authorities have deep experience in this regard, and can assist in investigating and taking the steps necessary to create this record.

Conclusion

In light of the discussion above, one conclusion an attorney advising business enterprises might reach is that cloud computing is far too complex and risky for adoption, especially given the legal risks inherent in electronic discovery and the production of evidence. While some may get away with that for a short time—fear of something new is often a powerful driver—companies may well soon discover that the benefits of cloud computing far outweigh the risks, and perhaps the risks are far more manageable with prudent counsel and some careful management than one might suspect on first impression. The key to

successful cloud computing is to understand the risks, address them as best as one can from the outset of a client/customer/cloud provider relationship, and continue to monitor the cloud, knowing and being fully informed of the risks and the rewards.

References

Wayne C. Matus, Todd L. Nunn and Tanya Forsheit. *Cloud Computing: Emerging E-Discovery Trends – Meeting the New Discovery Challenges in Electronically Stored Information*. Retrieved May 4, 2010, from http://www.straffordpub.com/products/cloud-computing-emerging-e-discovery-trends-2010-05-04. Webinar attended May 4, 2010.

Legal Implications of Cloud Computing – Part One (the Basics and Framing the Issues), http://www.infolawgroup.com/2009/08/tags/security/legal-implications-of-cloud-computing-part-one-the-basics-and-framing-the-issues/ (posted Aug. 18, 2009 by David Navetta).

Legal Implications of Cloud Computing – Part Two (Privacy and the Cloud), http://www.infolawgroup.com/2009/09/articles/breach-notice/legal-implications-of-cloud-computing-part-two-privacy-and-the-cloud/ (posted Sept. 30, 2009 by Tanya Forsheit).

Legal Implications of Cloud Computing – Part Three (Relationships in the Cloud), http://www.infolawgroup.com/2009/10/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-three-relationships-in-the-cloud/ (posted Oct. 21, 2009 by David Navetta).

Legal Implications of Cloud Computing – Part Four (E-Discovery and Digital Evidence), http://www.infolawgroup.com/2009/11/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-four-ediscovery-and-digital-evidence/ (posted Nov. 27, 2009 by Tanya Forsheit).

Trent Livingston and Richard Kershaw, *The Impact of Cloud Computing on Corporate Litigation Preparedness for Clients of Reed Smith*, LECG™ XPRT Forum™, March 2010, at 4.

Michael P. Bennett, *Negotiating Cloud Computing Agreements*, Law Technology News (March 11, 2010), available at http://eddblogonline.blogspot.com/2010/03/negotiating-cloud-computing-agreements.html.

Edward Pisacreta, *A Checklist for Cloud Computing Deals*, Law Technology News (April 9, 2010), available at http://eddblogonline.blogspot.com/2010/04/checklist-for-cloud-computing-deals.html.

Stuart Levi and Kelly Riedel, *Cloud Computing – Understanding the Business and Legal Issues*, printed in Vol. 2, Issue 2 of *Practical Law Journal*, March 2010, at 34.

Special thanks to Allison Jane Walton, Esq., E-Discovery Specialist at Applied Discovery, Inc., for her insights.

— Biographies of Authors and Editors —

Jennifer Yule DePriest, Partner – Chicago +1 312 207 6444 jdepriest@reedsmith.com

Jennifer is a litigator who focuses on intellectual property disputes involving patents, copyrights, trade secrets, trademarks and unfair competition under the Lanham Act. Jennifer has also successfully handled numerous complex commercial litigation matters, at the trial court level and on appeal, involving securities fraud, breach of contract, tortious interference, breach of fiduciary duty, and shareholder and member/manager disputes.

Claire N. Covington, Associate – Chicago +1 312 207 6504 ccovington@reedsmith.com

Claire is a member of the Midwest Commercial Litigation Group, practicing in the area of product liability litigation. In addition, Claire serves as E-Discovery Counsel to one of the firm's major clients, a Fortune 50 company. She has experience counseling clients about a variety of E-Discovery topics, which include document retention issues, litigation hold issues and email retention issues. Claire also has experience with the issues arising out of the incompatibility of United States discovery practice with the European Union Directive on Data Privacy.

— Cloud Computing Task Force Leaders —

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

Adam Snukal, Senior Associate – New York +1 212 549 0333 asnukal@reedsmith.com

Adam is a senior associate, based in New York, within the global Advertising Technology & Media Group at Reed Smith. Adam's legal background includes diverse, complex and extensive experience both in business law counseling and in advising on advertising, technology and media-related matters. Adam's experience in the area of information technology spans both strategic and commercial software licensing, large-scale procurement, e-commerce-related matters, financial services, health care and medical devices, wireless technology, outsourcing and gaming. In the area of advertising, Adam regularly counsels clients on traditional, online and mobile marketing/advertising related matters, advertising and marketing agreements, media buying, trademark/brand licensing, user generated content, privacy, sweepstakes, contests, gaming and advergaming, website and WAP site development, digital content development/distribution/aggregation, celebrity endorsements and more.

— Endnotes —

[1] For purposes of this article, “data” and “information” are used interchangeably.

[2] The process of identifying, preserving, collecting, reviewing and producing ESI is referred to as e-discovery.

[3] Once a party reasonably anticipates becoming involved in litigation, the party must take appropriate steps to preserve relevant information. Federal Rule 26(b)(1) provides: “Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party’s claim or defense…. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.”

[4] The 2006 amendments affected Federal Rule of Civil Procedure Nos. 16, 26, 33, 34, 37 and 45.

[5] Rule 34 obligates a party to produce or permit inspection of any “designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.” The advisory committee notes clarify that “[t]he Rule covers—either as documents or as electronically stored information—information ‘stored in any medium,’ to encompass future developments in computer technology” and that the Rule “is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes or developments.” Fed. R. Civ. P. 34 advisory committee’s notes (2006 amendments).

[6] *Pension Committee v. Banc of America Securities, LLC,* No. 05 Civ. 9016 (SAS), 2010 WL 184312, at *1 (S.D.N.Y. Jan. 15, 2010).

[7] *See* Rule 26(f)(3). Some jurisdictions have enacted rules that specifically require detailed knowledge of data identification, preservation and collection issues for purposes of the initial Rule 26(f) conference. For example, the Seventh Circuit recently implemented an e-discovery pilot program, the purpose of which is to evaluate and improve pretrial litigation procedures in the hopes of reducing the cost and burden of e-discovery consistent with Rule 1 of the Federal Rules of Civil Procedure. The pilot program committee created a set of principles that will eventually be incorporated into a standing order in the Seventh Circuit, to address commonly encountered e-discovery issues such as education, costs, preservation, collection and processing of ESI. Co-author Claire Covington, of Reed Smith’s Chicago office, serves as a member of the Seventh Circuit’s pilot program committee.

[8] Data mapping is a process that involves identifying the location of data across a company’s network, or outside the network, to the extent data-hosting is outsourced.

[9] Data security and privacy issues are generally beyond the scope of this paper. That said, companies should research the physical location of the cloud provider’s data center, as this could also have far-reaching legal effects on data privacy and portability. Awareness of and compliance with data protection regulations, such as HIPAA, usually remains the responsibility of the company, not the cloud provider. Furthermore, if the cloud provider is located offshore, ESI may be subject to the data protection laws of the country in which it is stored, thus affecting a company’s ability to retrieve and control its own data.

[10] *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003); *see also Pension Committee v. Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS), 2010 WL 184312, at *4 (S.D.N.Y. Jan. 15, 2010).

[11] Self-collection refers to the process of utilizing a company’s own IT personnel, as opposed to a third party, such as an e-discovery vendor or forensic collection specialist, to copy and collect potentially relevant ESI.