Richmond Journal of Law and Technology

Volume 20 | Issue 2 Article 6

2014

Understanding and Contextualizing Precedents in e-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance

Jonathan M. Redgrave

Keltie Hays Peay

Mathea K.E. Bulander

UNDERSTANDING AND CONTEXTUALIZING PRECEDENTS IN E-DISCOVERY: THE ILLUSION OF STARE DECISIS AND BEST PRACTICES TO AVOID RELIANCE ON OUTDATED GUIDANCE

Jonathan M. Redgrave,[*] Keltie Hays Peay,[**] and Mathea K.E. Bulander[***]

Cite as: Jonathan M. Redgrave, Keltie Hays Peay, & Mathea K.E. Bulander, *Understanding and Contextualizing Precedents in e-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance*, 20 RICH. J.L. & TECH. 8 (2014), http://jolt.richmond.edu/v20i2/article8.pdf.

> *But as precedents survive like the clavicle in the cat, long after the use they once served is at an end, and the reason for them has been forgotten, the result of following them must often be failure and confusion from the merely logical point of view.*[1]
>
> Oliver Wendell Holmes, Jr.

[*]Jonathan Redgrave is a partner with Redgrave LLP in Washington, D.C. He is Chair Emeritus of The Sedona Conference's® Working Group on Best Practices for Electronic Document Retention and Production. The views expressed in this article are solely those of the authors and may not be attributed to any other persons, the Firm or any of the Firm's clients.

[**] Keltie Hays Peay is a Senior Attorney with Redgrave L.L.P. in the Firm's Washington, D.C. office.

[***] Mathea Bulander is an Attorney with Redgrave L.L.P. in the Firm's Minneapolis, Minnesota office.

[1] Oliver Wendell Holmes, *Common Carriers and the Common Law*, 13 AM. L. REV. 608, 630 (1879).

I. INTRODUCTION

[1] It can be said, without hyperbole, that the data swell of the last two decades catalyzed a seismic shift in the constitution of discoverable information in civil litigation. The volcanic rise of the data labyrinth dramatically affected our culture, and has produced critical impacts on the legal rights of individuals and organization, as well as on the legal system as a whole.[2] In the wake of exponential data growth, e-Discovery case law materialized in fits and starts[3] and only began to coalesce by the early

[2] The advent of social media networking alone has dramatically changed the way that individuals and companies communicate, and thus create ESI. Facebook has grown from 12,000,000 users in 2006 to over a billion in 2012; Twitter had a mere 1,000 users in 2006, but by 2012 had nearly half a billion. Pintrest saw a compound annual growth rate of 4,900 from 2010 (10,000 users) to 2012 (25,000,000 users). *See* D. Steven White, *Social Media Growth 2006 to 2012*, ALL THINGS MARKETING (Feb. 9, 2013), http://dstevenwhite.com/2013/02/09/social-media-growth-2006-to-2012/.

[3] *See, e.g.*, Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 113 (2d Cir. 2002) (finding that spoliation sanctions may be imposed for the negligent, gross negligent, or bad faith destruction of discoverable information); McPeek v. Ashcroft, 212 F.R.D. 33, 34, 37 (D.D.C. 2003) (denying further discovery after analysis of a single backup did not yield valuable discoverable information); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 218-20 (S.D.N.Y. 2003) (finding that responsive e-mail should be produced, even if on backup tapes, and that compelling the responding party to restore and produce responsive documents from only a minimal sample of the requested backup tapes is, in general, sensible); Tulip Computers Int'l B.V. v. Dell Computer Corp., No. 00-981-RRM, 2002 U.S. Dist. LEXIS 7792, at *11, *16, *19-20 (D. Del. Apr. 30, 2002) (granting order to compel defendant to provide the computer hard drives utilized by specific company executives for key word searching after defendant failed to answer various discovery); Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 650-52 (D. Minn. 2002) (finding that discoverable and relevant information could be found in deleted documents residing on defendant's computer systems and that it was reasonable for plaintiff to attempt to recover such information); Trigon Ins. Co. v. United States, 204 F.R.D. 277, 289-90 (E.D. Va. 2001) (finding draft reports and communications between defendant's litigation support company and third-party expert were discoverable and the destruction of same was spoliation); Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (finding that production of employee hard drives was not unduly burdensome where defendant's employees deleted relevant e-mail during the course of litigation); Dodge, Warren, & Peters Ins. Servs. v. Riley, 130 Cal. Rptr. 2d 385, 388-89 (Cal. Ct. App. 2003) (granting a preliminary injunction against defendants in a misappropriation of trade secrets case and ordering them to preserve electronic evidence

2000s in district court orders and opinions that focused on a party's duty to preserve unique relevant information, such as electronically stored information ("ESI") and sanctions that followed insufficient efforts to preserve ESI.[4]

[2] While case law of the burgeoning electronic age provided nascent pathways for e-Discovery, the decisions were, by their nature, based upon rudimentary assumptions regarding the character of ESI. Moreover, the decisions are inevitably related to the unique technologies at issue in each case. As such, the seminal e-Discovery cases largely focused on issues such as "PROFS" mail[5] and magnetic media backup tapes.[6] At that time, approximately in the early 1990s and early 2000s, smartphones had yet to emerge,[7] Facebook was still the idea of a college student at Harvard, a tweet was merely a sound that a bird made, and cloud computing had not been rolled out to individuals and small businesses.

---

and appointing an expert to recover lost or deleted files, copy data, and perform key word searches).

[4] *See Residential Funding*, 306 F.3d at 113; Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 436 (S.D.N.Y. 2004); Thompson v. United States HUD, 219 F.R.D. 93, 104-05 (D. Md. 2003); Wiginton v. CB Richard Ellis, No. 02 C 6832, 2003 U.S. Dist. LEXIS 19128, at *18-21, *26 (N.D. Ill. Oct. 24, 2003).

[5] *See* Armstrong v. Exec. Office of the President, 1 F.3d 1274, 1278-80 (D.C. Cir. 1993) (challenging the proposed destruction of certain federal records, and referred to colloquially as the PROFS case, taking its name from the IBM PROFS (Professional Office System) e-mail system used in the White House).

[6] *See* Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 429 (S.D.N.Y. 2002) (evaluating the burden for each defendant to produce e-mail based, in part, upon whether the e-mail was stored on backup tapes).

[7] The PalmOne Treo 600 and the BlackBerry were introduced to the market in 2003. *See The Evolution of Cell Phone Design Between 1983-2009*, WEBDESIGNER DEPOT (May 22, 2009), http://www.webdesignerdepot.com/2009/05/the-evolution-of-cell-phone-design-between-1983-2009/.

[3] As many have noted, technology has continued its rapid expanse over the past ten years;[8] the law, however, fails to adequately address the increasingly advanced and often complex technologies, as it lumbers behind the pace of innovation. But what of that fact? How is a practitioner to take that piece of information and use it to better her practice, improve her skill, and serve as a superior advocate for her clients? The authors of this Article have observed that the collision between the measured evolution of law under stare decisis and precipitous changes in technology has yielded assumptions, or legal myths, that shade legal decisions long after the initial supposition has been debunked, undermined, or rendered irrelevant. Indeed, many contemporary judicial decisions rely on this historic body of e-Discovery folklore, notwithstanding the facts of ESI as they now exist. Recognizing the treacherous nature of relying on prior cases in the area of e-Discovery is a critical skill for today's litigators.

[4] This Article seeks to 1) identify select examples of "old world" assumptions, 2) demonstrate how new technologies confound these initial assumptions when it comes to e-Discovery, and 3) offer practitioners "best practices" advice on how to avoid the pitfalls of relying on outdated assumptions in e-Discovery practice. We start with a review of stare decisis' role in American Jurisprudence, and follow with a discussion of the evolution of e-Discovery case law and the nature of technological change. We then examine five assumptions that exist within the e-Discovery domain.

A. The Role and Value of Stare Decisis in e-Discovery

[5] Stare decisis is a foundational principle of the common law system of American Jurisprudence.[9] As translated from Latin, stare decisis means

[8] *See, e.g.*, Vivek Wadhwa, *Why I Believe That This Will Be the Most Innovative Decade in History*, FORBES (June 25, 2012, 7:00 AM), http://www.forbes.com/sites/singularity/2012/06/25/most-innovative-decade-in-history/.

[9] Todd E. Freed, *Is Stare Decisis Still the Lighthouse Beacon of Supreme Court Jurisprudence?: A Critical Analysis*, 57 OHIO ST. L.J. 1767, 1767 n.3 (1996).

"to stand by things decided."[10] It is a legal principle of two parts: (1) that trial courts have to honor the precedents of higher courts,[11] and (2) that the Supreme Court of the United States must follow its own precedents.[12] Thus, trial courts have an obligation to follow the precedent of higher appellate courts, but opinions of other trial courts hold only persuasive authority.[13] Against this background it is important to note that because discovery disputes are a matter for trial courts, and opinions and orders on discovery matters are interlocutory in nature, few cases have been reviewed by appellate courts. Thus, issues in e-Discovery have been largely handled on a case-by-case basis, with little in the way of guiding precedent. It is true that the legal rules that guide discovery can be applied to ESI in a general fashion (e-Discovery is, in fact, merely discovery); in order to adequately execute such discovery, however, attorneys and judges must understand the technical underpinnings of relevant data and the practical results of applying the rules to specific technology. Thus, stare decisis has built, at best, only a skeletal framework for discovery, and is devoid of a legal blueprint that practitioners may follow as they execute discovery in the digital age. Moreover, the demands of properly describing and executing e-Discovery can require greater time and resources than are available to the average litigator or court. As a result, it is easy to rely, reflexively, upon prior opinions to try and solve a current problem, even when the factual comparison is inapt.

B. The Challenge of Ever-Evolving ESI to the Reasoned Development of Case Law

[6] Computers have been used in the context of business since the 1950s, but the volume of ESI created by early computer systems was

[10] BLACK'S LAW DICTIONARY 1537 (9th ed. 2009).

[11] This is known as "vertical stare decisis." *Id.*

[12] "Horizontal stare decisis" requires a court to follow its past decisions. *Id.*

[13] *See, e.g.*, Hart v. Massanari, 266 F.3d 1155, 1174 (9th Cir. 2001).

limited.[14] With the advent of the personal computer revolution in the late 1970s and early 1980s, the stage was set for an explosion of data. In the 1990s, personal "productivity" software such as Lotus 123, WordPerfect, and the Microsoft Office suite of programs became commonplace in corporate organizations, displacing reliance on mainframe and mini-frame computing systems.[15] At the same time, the ubiquity of e-mail in personal and business communications began to rapidly dwarf traditional methods of written correspondence; since 2000 the United States Postal Service has experienced a significant decline in volume of mail handled and now handles fewer letters and packages each year than the number of e-mails sent each day.[16] The travail left to courts in the face of these new technologies, and vast cultural shift in communicative behavior, was significant. During that time a great number of parties were reluctant to even produce ESI. Amid this uncertainty, in 1995 Magistrate Judge Peck issued an opinion and order regarding the discovery of "data processing files" that famously pronounced that "today it is black letter law that computerized data is discoverable if relevant."[17]

[7] By the early 2000s, the Internet was a dominant global communication medium, which in turn spawned the social media revolution, as well as the ability to use massive computing resources on a collective basis (through what we commonly refer to as "cloud computing"). Additionally, more individuals started using phones for messaging and the forerunners of today's smart phones, such as the Palm Treo and early Blackberry models, began to merge phone and messaging

[14] *See* PETER J. BIRD, LEO: THE FIRST BUSINESS COMPUTER 15 (1994).

[15] *See* Darryl K. Taft, *eWeek at 30: How Microsoft Won the 1990s Office Suite Wars*, EWEEK (Oct. 31, 2013), http://www.eweek.com/enterprise-apps/eweek-at-30-how-microsoft-won-the-1990s-office-suite-wars.html/.

[16] NORMAN J. MEDOFF & BARBARA K. KAYE, ELECTRONIC MEDIA: THEN, NOW, AND LATER 80 (2d ed. 2011).

[17] Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355, at *1, *4 (S.D.N.Y. Nov. 3, 1995).

capabilities with enhanced features and qualities.[18] Moreover, the reduced expense of audio and video transmission devices allowed for the incredible generation and retention of voice and image recordings across a plethora of devices and platforms.[19]

[8] In light of the variety of forms ESI may take,[20] prior to the 2006[21] it was unclear whether all ESI met the definition of discoverable "documents" under Federal Rule of Civil Procedure ("Rule") 34.[22] Debates regarding the discoverability of metadata arose before the 2006 change to the Federal Rules of Civil Procedure and continued thereafter.[23] The Federal Rules continue to "chase" ESI technology, and proposed

[18] *See* Julie Strietelmeir, *Handspring Treo 180 Review*, THE GADGETEER (Mar. 12, 2002, 12:00 AM), http://the-gadgeteer.com/2002/03/12/handspring_treo_180_review/.

[19] *See* Jarad Carleton, FROST & SULLIVAN, VIDEO & VOICE ARCHIVING 3, *available at* http://china.emc.com/collateral/analyst-reports/csg4870-video-voice-archiving-ar.pdf (last visited Feb. 23, 2014).

[20] ESI can take the form of a word processing document, a file that appears to the user in a form similar to a paper document, but it also takes the form of deleted information in slack space, application metadata, and system metadata. *Cf.* Thomas Y. Allman, *Managing Preservation Obligations After the 2006 Federal e-Discovery Amendments*, 13 RICH. J.L. & TECH 9, ¶ 7 (noting that "some types of ESI [are] not ordinarily visible to a user (such as metadata or embedded data)").

[21] From 1970 until the time that Rule 34 was amended in 2006, the Rule allowed for the production of "documents" which included "data compilations." FED. R. CIV. P. 34 at 2006 advisory committee's notes.

[22] *See* Hon. Shira A. Scheindlin & Jeffery Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 347 (2000) (discussing that deleted ESI, "embedded data" (i.e. application metadata), and log-on and network data (i.e. system metadata) may be relevant discoverable information, but does not fit neatly within the definition of documents in the prior version of Rule 34).

[23] *Compare id., with* Lucia Cucu, Note, *The Requirement for Metadata Production Under* Williams v. Sprint/United Management Co.*: An Unnecessary Burden for Litigants Engaged in Electronic Discovery*, 93 CORNELL L. REV. 221, 221-22 (2007) (discussing the perceived problems in defining metadata and that over preservation of metadata makes preservation and discovery needlessly more costly and difficult).

amendments addressing discovery seek to further clarify the place of ESI in the Rules' context.[24]

[9] This great and terrible assemblage of data—unmatched (and even previously unimagined) in the annals of human history—has particular import for lawyers charged with its handling, as it is all potentially discoverable evidence in the United States. The trailing case law has tried to define the parameters and terms laid out in the Federal Rules, set requirements for production and preservation, and create consequences for failures by parties to meet the both court-promulgated and rule-derived guidelines.

[10] From a sociological perspective, changing technology has also contributed profoundly to cultural norms in a way that greatly impacts the world of ESI; technology has afforded individuals the means and freedom to irreparably blur personal and professional roles and identities. Today, with the development of true "smart phone" devices, the possibilities of completely mobile, self-contained personal computing are boundless; Android and iOS platforms provide individual users with the genuine and nearly unfettered ability to communicate and work from a single, multi-functional hand-held device. The idea, and perhaps preferable business model, of the separation of roles (and devices) has been largely surrendered in favor of the convenience of single-device management. The consequences of this shift are significant and undercut many of the

[24] Whereas the 2006 amendments to the Federal Rules of Civil Procedure focused principally on "e-Discovery," the 2013 proposals aim to reform discovery in general; the core theme that animates the 2013 proposals is the need to reduce the burdens of modern discovery. Some of the more significant proposed changes include the statement regarding "cooperation" that has been introduced into the committee note for Rule 1 and the initial meet and confer required pursuant to Rule 26(f); changes that would limit the scope of discovery, including amendment to Rules 26(b), 26(c), 30, 31, 33, and 36; and the new spoliation sanctions rule in the proposed Rule 37(e). *See* COMM. ON RULES OF PRACTICE AND PROCEDURE OF THE JUDICIAL CONF., 113TH CONG., PRELIMINARY DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF BANKRUPTCY AND CIVIL PROCEDURE 281, 281, 289-93, 296, 300-05, 310-11, 314-17 (Comm. Print 2013), *available at* http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf [hereinafter "PRELIMINARY DRAFT AMENDMENTS"].

longstanding assumptions anchoring stare decisis in the context of e-Discovery.

[11] In some instances, courts are forced to make decisions on e-Discovery issues based on the arguments and best evidence before them, and issue orders that are almost immediately obsolete or are simply misguided when considered in light of the totality of the technological facts of a specific issue and the potential wide-spread ramifications of even a seemingly narrow ruling in a single case. For example, in *National Day Laborer Organizing Network v. United States Immigration & Customs Enforcement Agency*, Judge Scheindlin, one of the best known and most learned judges on this topic, originally ruled that the federal government must include certain "key" metadata fields when producing electronic data that is maintained by the agency as part of the electronic record when responding to Freedom of Information Act ("FOIA") requests. [25] Amidst much hue and cry by the government Judge Scheindlin withdrew her opinion, stating that based upon later submissions on the issue the "decision was not based on a full and developed record."[26] The judge further specified that the previous "decision [would hold] no precedential value."[27]

[12] *National Day Laborer* serves as a stark example of the problem facing litigants and courts. Judge Scheindlin was acutely aware of the need for concrete and practical guidance, and her efforts to set forth rules of the road in the FOIA context was clearly intended to also guide civil litigants.[28] Despite this admirable goal, however, briefing by the parties

[25] Opinion and Order, Nat'l Day Laborer Org. Network v. United States Immigration & Custody Enforcement Agency, No. 10 Civ. 3488 (SAS), 17-18 (S.D.N.Y. Feb. 7, 2011), ECF No. 41, *withdrawn*, Order Withdrawing Opinion, Nat'l Day Laborer Org. Network v. United States Immigration & Custody Enforcement Agency, No. 10 Civ. 3488 (SAS) (S.D.N.Y. June 17, 2011), ECF No. 98.

[26] Order Withdrawing Opinion, *supra* note 25.

[27] *Id.*

[28] *See* Order and Opinion, *supra* note 25, at 7, 11, 15-16, 24.

left the court with an incomplete record of the technical considerations that ultimately undercut the validity and viability of the proposed guidance.[29] Simply put, courts are in the unenviable position of either applying stare decisis, using the best established law available to decide issues related to cutting edge technology (about which they are not subject matter experts, relying, in part, on the arguments presents by litigants who typically lack such expertise as well), or must evade important issues as they arise. It is within this perfect storm of boundary-pushing technology and chasing jurisprudence that fallacious assumptions about ESI and e-Discovery arose, became ingrained, and now subtly work to undermine the emergence of a cohesive body of law for resolving e-Discovery disputes.

[13] What follows is an examination of select e-Discovery myths and assumptions that serve to extend this schism between law and reality. We present the origins of each assumption and discuss how each became a part of the precedential history guiding courts and practitioners today. We then attempt to demonstrate why these assumptions embedded in our law must be approached with caution and skepticism. Finally, we provide guidance regarding best practices for addressing these complex issues in litigation. In the end, and perhaps not surprisingly, we conclude that stare decisis will likely never develop to guide e-Discovery in the ways in which it may have developed for other species of legal disputes of substantive or procedural origin.

[29] *See* Order Withdrawing Opinion, *supra* note 25; *supra* text accompanying notes 26-27.

II. EXEMPLAR DECISIONS REFLECTING THE TRIUMPH OF SWIFT TECHNOLOGY EVOLUTIONS OVER THE ILLUSIVE QUEST FOR JUDICIAL GUIDANCE IN E-DISCOVERY

A. Case Assumption #1: The Defining Issue for Discoverability of Relevant Electronic Information Is Accessibility.

Truth: Accessibility changes with technologies; the key is proportionality in the requirements of production.

[14] In early ESI decisions, such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, *Zubulake IV*, *Thompson v. United States HUD*, and *McPeek v. Ashcroft*,[30] there was an implicit, if not explicit, focus on whether a source of ESI was "accessible." If it was determined, in fact, that the requested information existed, even in a form that required "restoration," and could therefore be accessed, courts were likely to allow at least some sampling of the restored data to see what might be found.[31] Oftentimes the legal analysis and inquiries focused on the retrieval of information from magnetic media backup tapes. Indeed, the notoriety surrounding such inquiries led the Civil Rules Advisory Committee to recommend, and the Supreme Court to adopt, a specific provision in the Federal Rules of Civil Procedure to address sources of ESI that are "not reasonably accessible."[32]

[15] The logic of this initial focus on accessibility is inescapable. In the early days of the explosion of data creation and storage, technological innovations had not yet fixed on the back-end solutions of managing what was being created and stored at such a feverish pace. Thus, the question

[30] Residential Funding Corp. v. DeGeorge Fin. Corp, 306 F.3d 99 (2d Cir. 2002); *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003); Thompson v. United States HUD, 219 F.R.D 93 (D. Md. 2003); McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001).

[31] Judge Facciola described one such foray into the complexities of data retrieval as a "test run." *McPeek*, 202 F.R.D. at 34.

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

of accessibility became the natural linchpin in determining whether certain data could be "discovered" at all. This seeming "bright line" also appeared as a visage of hope in the effort to reign in potentially unbounded discovery of oceans of data. However, conflating the concepts of accessibility and discoverability did not serve the law well when technology broke through most of the barriers to accessibility present in early cases.

[16] In practical terms, the speed of technology left these past cases and even the Rule 26(b)(2)(B) "not reasonably accessible" test in the dustbin of history as many organizations no longer use magnetic media back-up tapes (having been replaced with mirrored servers or cloud storage for disaster recovery) and a number of vendors have developed solutions to more easily and less expensively access data on magnetic media back-up tapes. These developments render a focus on "accessibility" moot inasmuch as the issue does not help to frame the boundaries of discovery.

[17] Courts have said, primarily in dicta, that data preservation does not require Herculean efforts to maintain the universe of "preservable" data.[33] Unfortunately, the reality is that the underlying assumption of the earliest cases was that if information was "accessible" then it could be discoverable—without regard to the reality that new technologies would provide an unmanageable ocean of data that could threaten to swallow civil discovery.[34] This reality has been hammered home in recent years by the Duke Conference Subcommittee and the Discovery Subcommittee of the Advisory Committee on Civil Rules, which have each concluded that proportionality is one of the most important (but often overlooked) tenants that must be used to guide the scope of discovery.[35]

[33] *See Zubulake IV*, 220 F.R.D. at 217.

[34] *See* Rachel K. Alexander, *E-Discovery Practice, Theory, and Precedent: Finding the Right Pond, Lure, and Lines without Going on a Fishing Expedition*, 56 S.D. L. REV. 25, 26-27 (2011).

[35] *See generally* Memorandum from Hon. David G. Campbell, Chairman, Advisory Comm. on Fed. Rules of Civil Procedure, to Hon. Jeffrey S. Sutton, Chair, Standing Comm. on Rules of Practice and Procedure (May 8, 2013), *available at*

[18] In short, the breadth of "accessible information" dwarfs the needs of most any case. We as practitioners must not start by requesting the entire universe of potentially relevant data wholesale, but begin to focus on the discoverable information that is really needed and is proportional to the case. This requires little more than an exercise in textbook discovery practice. In order to conceive and craft narrowly drawn discovery requests that are intended to elicit unique relevant data that makes an element of the case we are pressing more or less likely, attorneys and clients must know and understand their cases to the extent practicable. This shift in practice requires restraint. It requires the practitioner to ignore the historical norms of engaging in haphazard free-for-all discovery grabs, which inevitably lead back to disputes about accessibility, rather than critical import. It requires reasonable cooperation between the parties to identify, first, what data and material each party really is seeking, and second, the best means for the production of information that is accessible and proportional to the case. It may even require greater judicial involvement to make proportionality a reality. Ironically, in Judge Scheindlin's conclusion in the now-withdrawn opinion of *National Day Laborer*, she eloquently made this very point:

> Once again, this Court is required to rule on an e-discovery issue that could have been avoided had the parties had the good sense to "meet and confer," "cooperate" and generally make every effort to "communicate" as to the form in which the ESI would be produced. The quoted words are found in opinion after opinion and yet lawyers fail to take the necessary steps to fulfill their obligations to each other and the court . . . [S]uch conduct certainly shows that all lawyers—even highly respected private lawyers, Government lawyers, and professors of law—need to make greater efforts to comply with the expectations that courts

http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV05-2013.pdf (reporting on the advisory committee notes on proposed amendments to the Rules from a meeting at the University of Oklahoma and discussing a similar conference in 2010 at Duke University).

> now demand of counsel with respect to expensive and time-consuming document production. Lawyers are all too ready to point the finger at the courts and the Rules for increasing the expense of litigation, but that expense could be greatly diminished if lawyers met their own obligations to ensure that document production is handled as expeditiously and inexpensively as possible. This can only be achieved through cooperation and communication.[36]

[19] In practice, counsel, whether requesting discovery or responding to discovery requests, must tie proportionality to the pedestal of relevance. Indeed, oft-ignored Rule 26(g) requires that attorneys certify that discovery is being conceived and executed in a proportional fashion.[37] In addition to raising the issue of proportionality, wise counsel will specifically analyze the discovery requests at a micro-level, determining whether the specific deposition, computer recovery, or interrogatory is "worth the candle" when propounding discovery. Next, counsel must present concrete examples and evidence of the need or burden associated with the discovery request. Generalized statements about the size of a case or unsubstantiated notions of burden should be, and will be, quickly discarded by the court. Finally, wise counsel should actively engage their adversary in dialogue and, if that proves unsuccessful, walk into court with a singular focus of presenting the more reasonable—and proportionate—approach to the discovery dispute.

[36] Order and Opinion, *supra* note 25, at 25.

[37] FED. R. CIV. P. 26(g).

B. Case Assumption #2: Possession, Custody, or Control Is an Effective Way to Establish the Scope of Discovery for Relevant Electronic Information.

Truth: The emergence of a blended world of personal and business information on devices and in the cloud confounds the usefulness of the traditional test.

[20] Federal Rule of Civil Procedure 34 has always provided that parties have a duty to produce discoverable information that is within their "possession, custody, or control."[38] Early case law in the area of discovery clearly established that the standard is disjunctive; that is, the party must not only produce discoverable information in its possession, but also such information that is merely within its control.[39] Nonetheless,

[38] In 1936 the text of Rule 34 read:

> Upon motion of any party showing good cause therefor and upon notice to all other parties, the court in which an action is pending may (1) order any party to produce and permit the inspection and copying or photographing by or on behalf of the moving party, of any designated documents, papers, books, accounts, letters, photographs, objects, or tangible things, not privileged, which constitute or contain evidence material to any matter involved in the action and which are in his possession custody, or control; or (2) order any party to permit entry upon designated land or other property in his possession or control for the purpose of inspecting, measuring, surveying, or photographing the property or any designated relevant object or operation thereon. The order shall specify the time, place, and manner of making the inspection and taking the copies and photographs and may prescribe such terms and conditions as are just.

Federal Rule of Civil Procedure 34 was amended in 1946, 1970, 1980, 1987, 1991, 1993, 2006, and 2007. In August 2013, the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States released for public comment proposed amendments to the Federal Rules of Civil Procedure, including Rule 34. If adopted, the proposed amendment to Rule 34 would amend procedures regarding responses and objections to requests for production governed by Rule 34(b)(2). *See* PRELIMINARY DRAFT AMENDMENTS, *supra* note 24, at 306-08.

while many cases parrot the test and existing precedent, there is little discussion in such cases regarding the distinction between possession and custody versus control.[40]

[21] In the modern era of discovery, disputes regarding whether evidence is within a litigant's possession or custody are dispatched with relative ease,[41] but the issue of control has been frequently and fervently

[39] *See, e.g.*, Stewart-Warner Corp. v. Staley, 4 F.R.D. 333, 335-36 (W.D. Pa. 1945) (finding that a moving party must at a minimum aver that documents *are in the control of the plaintiff*) (emphasis added); United Mercantile Agencies v. Silver Fleet Motor Express, 1 F.R.D. 709, 712 (W.D. Ky. 1941) (finding that business documents of defendant are within its possession, custody, or control, if "defendant would either have actual physical possession of its own records *or* would be in a position to obtain them from someone who has temporary custody of them.") (emphasis added). Moreover, possession, custody, or control is a legal standard that pre-dates the Federal Rules of Civil Procedure. *See* Stephen N. Subrin, *David Dudley Field and the Field Code: A Historical Analysis of an Earlier Procedural Vision*, 6 LAW & HIST. REV. 311, 332-33 (1988). The Field Code contained provision regarding the inspection and copying of papers in the possession or custody of the opposition. *See id.* at 332. In addition, the concept of possession, custody, and control is not unique to discovery law. For example, the same concept can be found in criminal law, bankruptcy law, and in the law applicable to estates and trusts. *See, e.g.*, Wilson v United States, 221 U.S. 361, 377 (1911) (finding that the president of a corporation could be personally held in contempt of court for failure to produce letters he wrote in his capacity as president to the grand jury because a subpoena was properly served upon the corporation, and the letters were documentary property subject to the control of the corporation); Foster v. United States, 265 F.2d 183, 185 (2d Cir. 1959); Van Antwerp v. Hulburd, 28 F. Cas. 941, 942-43 (C.C.N.D.N.Y. 1871) (finding that bonds that were allegedly taken into receivership and paid to the federal government under a bank liquidation were not in the possession, custody, or control of the receiver, his duties being limited by statute).

[40] *See, e.g.*, Garrett v. Faust, 7 F.R.D. 650, 651 (E.D. Pa. 1948) (failing to differentiate among "possession, custody, or control"); Thomas French & Sons, Ltd. v. Carleton Venetian Blind Co., 30 F. Supp. 903, 905 (E.D.N.Y. 1939).

[41] Where possession is the issue, the court has little need to provide findings or analysis beyond the fact that the item in question is or is not in the party's possession. *See, e.g.*, United States v. Int'l Union of Petroleum & Indus. Workers, 870 F.2d 1450, 1452 (9th Cir. 1989).

litigated.[42] Courts presume that "records which are normally kept in the business of the party . . . are presumed to exist, absent a sworn denial, and a prima facie case of control is all that must be established to justify issuance of the order."[43] While it is clear that control constitutes more than the ability to obtain discoverable information, the definition of control varies by jurisdiction.[44] In some jurisdictions, such as the Ninth Circuit, control is defined as the legal right to obtain discoverable information.[45] Other courts have found that control exists where a party has "the right, authority, or practical ability[] to obtain the documents from a non-party to the action."[46]

[22] While these standards are not always black and white, they are relatively simple to apply to paper documents, physical evidence, or even data on servers owned and operated by a business. This was true of the backup tapes in *McPeek*, the e-mail at issue in *Zubulake IV*, and the data in the off-site warehouse in *Tulip Computers International B.V. v. Dell Computer Corporation*.[47] When a device is used for a mix of personal and business purposes, however, and particularly when a business allows an employee to use technologies and devices that are not owned by the

[42] *See, e.g.*, Bough v. Lee, 29 F. Supp. 498, 501 (S.D.N.Y. 1939).

[43] Norman v. Young, 422 F.2d 470, 473 (10th Cir. 1970) (citations omitted); *see also* Mullen v. Mullen, 14 F.R.D. 142, 143 (D. Alaska 1953) (requiring that defendant trustee produce tax returns of the trust because "[n]ot only is the state of the record such as to warrant the inference of possession, custody or control, but there is no denial thereof").

[44] *See* Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993) ("But the fact that a party could obtain a document if it tried hard enough . . . does not mean that the document is in its possession, custody, or control.").

[45] *See In re* Citric Acid Litigation, 191 F.3d 1090, 1107-08 (9th Cir. 1999).

[46] Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000) (quoting Bank of N.Y. v. Meridien Biao Bank Tanz., Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997)).

[47] McPeek v. Ashcroft, 212 F.R.D. 33, 35 (D.D.C. 2003); *Zubulake IV*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003); Tulip Computers Int'l B.V. v. Dell Computer Corp., No. 00-981-RRM, 2002 U.S. Dist. LEXIS 7792, at *5 (D. Del. April 30, 2002).

organization[48] in the course of employment, issues of control between employer and employee[49] or a business and its business partner can arise.[50] Because technologies are no longer tethered to an office or a home base, the ESI is not necessarily within the possession or custody of the business. Likewise, the widespread availability of computing resources and ubiquitous Internet connectivity has led to a world where multiple organizations may share common access to data platforms and systems, while little or no consideration is given to data security or control rights. These trends trigger questions of control in a new light.[51]

[23] Aptly illustrating this point is *Carrillo v. Schneider Logistics, Inc.* In *Carrillo*, the defendant organization was sanctioned when it failed to produce e-mail authored by its employees using the e-mail facilities of its business partner.[52] The court rejected the organization's claim that it did not control the e-mail because it did not own the e-mail servers.[53] In 2013, a similar e-mail issue arose in *Ubiquiti Networks, Inc. v. Kozumi*

[48] Such as smartphones, tables, and even personal computers.

[49] *See, e.g.*, Hatfill v. N.Y. Times Co., 242 F.R.D. 353, 355 (E.D. Va. 2006) (finding that the newspaper ceded control of its reporter's notes and other unpublished materials to the employees per the joint bargaining agreement and employee handbook and that the paper had no obligation to produce same).

[50] *See, e.g.*, Carrillo v. Schneider Logistics, Inc., No. CV 11-8557-CAS (DTBx), 2012 U.S. Dist. LEXIS 146903, at *34, *51 (C.D. Cal. Oct. 5, 2012) (sanctioning a retail distributor for not producing e-mails its employees' sent using the e-mail system of its client, Wal-Mart).

[51] Historically issues of control involved issues of non-employee agents of an organization or parent-subsidiary corporate relationships. *See, e.g.*, Caremark, Inc. v. Affiliated Computer Servs., Inc., 192 F.R.D. 263, 264 (N.D. Ill. 2000) (discussing whether the attorney-client privilege applies to a non-employee agent's communications with a corporation's attorneys); Nears v. Holiday Hospitality Franchising, Inc., 295 S.W.3d 787 (Tex. Ct. App. 2009) (determining whether a parent corporation exercised sufficient control over an individual employee to implicate liability in a tort claim).

[52] *See Carrillo*, 2012 U.S. Dist. LEXIS 146903, at *34-35, *51-52.

[53] *See id.* at *34-35.

USA Corp., where an individual used a private Gmail account to send work related e-mails. [54] In that case, the court found that absent evidence that the company had a legal right to the documents contained in the e-mails, the organization could not be compelled to produce e-mails from the private Gmail account because the Gmail account was not in the control of the organization.[55]

[24] Additionally, in *Cotton v. Costco Wholesale Corp.* the court found that Costco did not have control of text messages on its employees personal cell phones because there was no evidence "that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand."[56] In a similar case, the United States District Court for the District of Kansas found that a board of directors did not have the legal right to demand discoverable information from former employees or former board members.[57] On the other hand, in a 2013 opinion in the *Pradaxa* litigation, the court sanctioned a company for not preserving text messages on all of its employees' mobile devices, including personal devices.[58]

[25] These cases illustrate the emerging conflict and confluence involving data systems and devices. Moreover, in regard to best practice guidance, these disputes make clear that companies must do a better job of setting forth clear employment guidelines and enforcing them. While it

[54] *See* Ubiquiti Networks, Inc. v. Kozumi USA Corp., No. 12-cv-2582 CW (JSC), 2013 U.S. Dist. LEXIS 53657, at *7 (N.D. Cal. Apr. 15, 2013).

[55] *Id.* at *7-8.

[56] Cotton v. Costco Wholesale Corp., No. 12-2731-JWL, 2013 U.S. Dist. LEXIS 103369, at *17-18 (D. Kan. July 24, 2013).

[57] *See* Kickapoo Tribe of Indians of Kickapoo Reservation in Kan. v. Nemaha Brown Watershed Joint Dist. No. 7, 294 F.R.D. 610, 613-14 (D. Kan. 2013).

[58] In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig., No. 2385; 3:12-md-02385-DRH-SCW, 2013 U.S. Dist. LEXIS 173647, at *61 (S.D. Ill. Dec. 9, 2013).

may seem beneficial for an organization to control less discoverable information, the lack of control can result in a loss of power and the ability to manage discovery.

[26] Finally it is important to note that potential evidence is not exempted from discovery merely because it is not within the possession, custody, or control of a party.[59] When ESI is not within the organization's control, the organization will likely miss the opportunity to review the ESI for relevance and privilege. Thus, an organization may wish to establish policies and practices that allow it to work with employees and business partners to control ESI so that it can maintain a defensible position as to its own organizational control of responsiveness and determinations of privilege. Regardless of the path chosen, however, it is critical that the policies are clear and well enforced. Otherwise, the scope of preservation and production obligations will be unclear, and the resolution of disputes will be made with little predictability as to the outcome.

C. Case Assumption #3: Preservation of Electronically Stored Information Is Getting Easier with the Passage of Time.

Truth: Although the capacity for data storage expands, the complexity of preservation and retrieval considerations increases concurrently.

[27] The duty to preserve relevant, unique evidence is a well-established common law doctrine;[60] "[t]he common law imposes the obligation to preserve evidence from the moment that litigation is reasonably anticipated."[61] There is no duty-to-preserve explicitly codified

[59] FED. R. CIV. P. 45(b)(1) provides that "[a]ny person who is at least [eighteen] years old and not a party may serve a subpoena."

[60] *See, e.g.*, Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494, 517 n.12 (D. Md. 2009).

[61] Victor Stanley, Inc., v. Creative Pipe, Inc., 269 F.R.D. 497, 521 (D. Md. 2010).

in the Federal Rules of Civil Procedure in current form,[62] but the duty has long existed as an inherent duty for all parties.[63] Courts have relied both on their authority under Rule 37 and their inherent powers[64] to impose sanctions on litigants for failure to preserve and produce evidence in accordance with this inherent duty.[65]

[28] As ESI volumes began to swell, the duty to preserve became an increasingly litigated issue. The early cases that addressed the preservation of ESI are deeply rooted in assumptions about data structures that are contrary-to-fact when it comes to navigating the obligations and burdens of data preservation today. While the basic doctrine of the common law duty to preserve does not deviate significantly from Circuit to Circuit, there is wide variation in the standard for imposing sanctions for the failure to uphold that duty. Willful, grossly negligent, or merely negligent destruction of documents or data may prompt a court to impose spoliation sanctions.[66] This uncertainty causes many organizations to default to a standard of undifferentiated, wholesale preservation—that is the unattainable goal of preserving nearly every "scrap" of evidence.

---

[62] In the proposed changes to Rule 37 regarding sanctions, currently under consideration by the Judicial Conference Advisory Committee on Civil Rules (the period for public comment on these proposed changes ended Feb. 15, 2014), section (e), currently titled "Failure to Provide Electronically Stored Information," would be amended to read "Failure to Preserve Discoverable Information," thus formally incorporating the duty into the Rules. *See* PRELIMINARY DRAFT AMENDMENTS, *supra* note 24, at 314.

[63] *See Goodman*, 632 F.Supp. 2d at 505 (quoting Thompson v. United States HUD, 219 F.R.D. 93, 100 (D. Ms. 2003)); *see also* Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001).

[64] *See Victor Stanley*, 269 F.R.D. at 517-18 (quoting *Goodman*, 632 F. Supp. 2d at 505); *see also* Adkins v. Wolever, 554 F.3d 650, 652 (6th Cir. 2009).

[65] *See* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002); *see also Victor Stanley*, 269 F.R.D. at 541.

[66] *See Victor Stanley*, 269 F.R.D. at 529, 532 (detailing different standards used by federal courts throughout the country).

[29] The underlying assumption perpetuating this preservation myth is that the increasingly sophisticated systems controlling the creation and storage of ESI allow an organization's IT department to flip a switch and send out an appropriate legal hold to preserve identifiably relevant data. During the ongoing saga of the missing, deleted, or withheld e-mails in *Zubulake*, the court summarily restated this basic formulation of a party's duty to preserve:

> [O]nce the duty to preserve attaches, counsel must identify sources of discoverable information. This will usually entail speaking directly with the key players in the litigation, as well as the client's information technology personnel. In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media (*e.g.*, backup tapes) that the party has a duty to preserve.[67]

[30] The assumption that all ESI can be preserved generally comes into play when litigants argue that the electronic nature of the discoverable information makes it infinitely *easier* for the producing party to comply with discovery. The argument is fatally seductive in its simplicity: "*It's just a matter of pushing the right buttons*." While there may have been some validity supporting such a conclusion in the context of *Zubulake V*, there is no question that the utility of this position has been worn thin over the past ten years by the vast changes in data volume, data types, and data systems that are pervasive in today's business models.

[31] The preservation myth is fallacious for two major reasons. First, it assumes a certain level of possession, custody, and control based on our

[67] *Zubulake V*, 229 F.R.D. 422, 439 (S.D.N.Y. 2004).

antiquated notions about where and how data is stored.[68] This assumption is derived from the false premise that the data ecosystem for any given organization is largely an updated, but equivalent, system built and organized in the same way that the paper-office organizational system was set up and mirrored by the early computer/ESI transition. The idea that current data ecosystems are merely a modern, albeit transformed, version of "the paper office" as we know it is simply false. Second, this assumption fails to account for the fact that we are dealing with incomparably more data, and with types of data that have never before existed before, in any form, in any office.[69]

[32] The fallacy of regarding electronic offices as high-tech mirrors to traditional offices has long been recognized, but persists nonetheless. As early as 2001, long before the institution of today's marvels of data collection, Judge Facciola considered this fallacy in the context of a dispute about "backup tapes":

> Using traditional search methods to locate paper records in a digital world presents unique problems. In a traditional "paper" case, the producing party searches where she thinks appropriate for the documents requested under Fed.R.Civ.P. 34. She is aided by the fact that files are traditionally organized by subject or chronology . . . such as all the files of a particular person, independent of subject. Backup tapes are by their nature indiscriminate. They capture all information at a given time and from a given server but do not catalogue it by subject matter.[70]

[68] *See supra* Part II.B.

[69] *See* Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12, ¶ 3 (2013), http://jolt.richmond.edu/v19i4/article12.pdf (noting that "for most organizations, information volume doubles every eighteen to twenty-four months").

[70] McPeek v. Ashcroft, 202 F.R.D. 31, 32-33 (D.D.C. 2001).

[33] This analogy concerning the overall construct of data systems gave rise to the false premise that data can be preserved at any moment in time simply by taking a "snapshot" of "the computer system" at issue at the instant the duty to preserve attaches, thereby "freezing" in time a mirror image of all data existing within that system. Take, for example, *Playboy Enterprises, Inc. v. Welles*, a straightforward trademark infringement case from the 1990s.[71] In that case, in light of potential data destruction, specifically e-mail deletion, the court appointed a "computer expert who specializes in the field of electronic discovery to create a 'mirror image'" of the alleged infringer's hard drive.[72] The entirety of this court-ordered solution to counter spoliation of evidence was based on the notion that the defendant's physical workstation could be copied onto a "disk," reviewed for privilege by defense counsel, and that "recovered" non-privileged files responsive to previous discovery requests could then be printed and produced to plaintiff.[73] While this was perhaps feasible in an era when the volume of data was smaller and ESI was tethered to physical devices, it nonetheless required the best (and most expensive) forensic preservation tools available.

[34] Although this scenario seems downright quaint from the vantage-point of 2014, it is a mistake to believe that a similar result can be achieved on larger, more technologically-advanced scale. The idea of data preservation cannot be shifted simply from its moorings in the replication of the contents of a physical device to the replication of a "system." Despite the fact that the concept of "mirror image" replication retains an ongoing allure for parties who think that such forensic wizardry can capture materials they believe an opposing party has not produced, such a conclusion is generally based solely on the requesting party's subjective analysis of what *has* been produced.[74] Parties often adopt this posture,

[71] *See generally* Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

[72] *Id.* at 1051, 1055.

[73] *See id.* at 1055.

[74] *See* Kickapoo Tribe of Indians of Kickapoo Reservation in Kan. v. Nemaha Brown Watershed Joint Dist. No. 7, 294 F.R.D. 610, 613, 618-19 (D. Kan. 2013) (declining the

which amounts to a way of saying: "If you just give me everything you have, I will find what I am looking for." Not only is this the very definition of the oft-condemned discovery fishing expedition, but it flies in the face of the well-accepted standard set forth in *Zubulake*—that the preservation duty does not require the preservation of, nor entitle a requesting party to get, all possible evidence.[75]

[35] Consider two specific items much in the fore of e-Discovery commentary today: BYOD devices[76] and Shadow IT.[77] Both potentially contain discoverable data, as both are systems that exist outside of the company-controlled data-ecosystem, either overtly or covertly. Additionally, both are subject to company policies, regulations, and prohibitions but are fertile ground for the rogue actor/employee.[78] Both elude any easy analogy to the "mirroring" technologies of the past. The

plaintiffs' request for an order requiring the mirror imaging of the computers and other electronic devices personally owned by the defendant's employees and former employees, citing both concerns about "possession, custody, and control," and the significant intrusion such imaging would impose on the individuals' privacy when considered against the remote likelihood of the discovery of new evidence).

[75] *See Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

[76] Gartner defines Bring Your Own Device (BYOD) as "an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Typically, it spans smartphones and tablets, but the strategy may also be used for PCs." *IT Glossery: Bring Your Own Device (BYOD),* GARTNER, http://www.gartner.com/it-glossary/bring-your-own-device-byod (last visited Feb. 10, 2014).

[77] Shadow IT, or "Rogue IT," is the businessperson's deployment of software or hardware that is not directly under the control of the IT department. *See* Jennifer Lonoff Schiff, *6 Tips to Help CIOs Manage Shadow IT,* CIO (Nov. 13, 2013), http://www.cio.com/article/743114/6_Tips_to_Help_CIOs_Manage_Shadow_IT.

[78] To what extent they are subject to these restrictions and prohibitions, at least in the case of BYOD devices, is, thus far, a case-by-case factual inquiry. *See* Cotton v. Costco Wholesale Corp., No. 12-2731-JWL, 2013 U.S. Dist. LEXIS 103369, at *6-7 (D. Kan. July 24, 2013).

struggle a company faces when confronted with preservation and Shadow IT is manifest: the "company" may not know of its existence yet the shadow data may contain potentially discoverable information that may be under the possession, custody, and control of the organization. "[T]he slippery slope down the life of rogue IT begins [by] downloading unauthorized apps[,] using Dropbox, Google Docs, or any other SaaS; the consequences of which are document leakages, lost business and financial penalties."[79] In the context of e-Discovery, Shadow IT can make it difficult to identify and preserve unique, relevant ESI. Yet, a court, working from years of knowledge about how conventional systems can be preserved or forensically replicated, seeks to apply the same preservation and production requirements on the company's "shadow data" once a party (on either side) realizes the possibility of its existence. The very nature of Shadow IT, however, makes it impossible for a company to use the tools it has developed or has available to it for preservation of its official data infrastructure to rein in the parallel, unsanctioned information infrastructure.[80]

[36] Practitioners' potential pitfalls when it comes to the "easy preservation" assumption are not isolated to situations involving "rogue" elements like Shadow IT. An ongoing risk for litigants is that the courts and other parties will remain unaware that some of the basic tools essential for electronic preservation in a specific area will not translate to a different or emerging technology. Courts could potentially penalize litigants for failing to accomplish the *impossible* act of superimposing a preservation

[79] Ben Kepes, *Rogue IT, a Rogues Gallery. Highlighting the Perils of "Shadow It"*, FORBES (Nov. 30, 2013, 12:18 PM), http://www.forbes.com/sites/benkepes/2013/11/30/rogue-it-a-rogues-gallery-highlighting-the-perils-of-shadow-it/ (quoting *Winners of the harmon.ie Rogue IT Horror Contest Announced!*, HARMON.IE, http://harmon.ie/blog/winners-harmonie-rogue-it-horror-story-contest-announced (last visited Dec. 15, 2013)).

[80] *See FAQ: How Does Shadow IT Complicate Enterprise Regulatory Compliance?*, SEARCHCOMPLIANCE, http://searchcompliance.techtarget.com/guides/FAQ-How-does-shadow-IT-complicate-enterprise-regulatory-compliance (last visited Feb. 10, 2014) (noting that Rogue IT is not subject to the same security controls or safeguards, making compliance even more difficult).

technique used routinely for saving one kind of data upon a different set of data in a manner for which it was not designed or is simply not effective.

[37] *In re Pradaxa Products Liability Litigation* illustrates this problematic paradigm.[81] Preservation of certain business text messages on employee-owned phones and employer-issued phones had become one of the hotly contested discovery issues in the case.[82] In the district court's December 2013 opinion, the court explained that no distinction could be made between the defendants' duty to preserve e-mails and texts, stating that both mediums are electronic communications and are therefore subject to the same duty to maintain, regardless of differences in usage or durability.[83] Thus, in the view of the court, the failure of the company to intervene and suspend "auto-delete" functions on employee phones was sanctionable.[84] Critically absent in the court's opinion and consideration is the fact that e-mail and text communication environments are dramatically different.[85]

[38] In a corporate e-mail environment, deletion and retention policies can be set and managed by the organization at the global, systemic level. Today, there is rarely a need to have individual users manipulate personal e-mail settings to achieve the desired preservation. On the other hand, text messaging is a vastly different environment. Each mobile device may have multiple applications capable of sending/retrieving SMS and or MMS text messages. Each mobile device has a specific messaging interface with the mobile device carrier. Some may have a linkage to a

[81] *See In re* Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig., No. 2385; 3:12-md-02385-DRH-SCW, 2013 U.S. Dist. LEXIS 173674, at *2-4 (S.D. Ill. Dec. 9, 2013).

[82] *See id.* at *3.

[83] *See id.* at *57-58, *62, *64.

[84] *See id.* at *63-66.

[85] *See id.* at *57-58, *61 ("[T]ext messages are electronically stored information, it does not matter that text messaging is a less prominent form of communication. . . .There is no question the defendants owed a duty to preserve this material.").

corporate messaging server, such as the Blackberry Enterprise Service (BES), that can be configured to capture messages, but those instances of captures are the vast minority in practice.[86] Thus, in the text message environment, the ability to save messages, and how many can be saved, is largely device- and carrier-dependent; there is no one answer and certainly no safe "auto-delete" switch. The reality is that each custodian will necessarily undertake the preservation task with varied and potentially incriminating consequences for failure.[87]

[39] Best practice guidance dictates that business organizations must stay on top of the legal ramifications of new data environments, systems, applications, and devices. The text message versus e-mail example is but one illustration of the dramatic technological underpinnings that differentiate two technologies that have a similar use. Even under the simplest paradigm of data architecture within a company where, for example, a company operates primarily on a physical server located at the company's brick-and-mortar headquarters and has some well-defined contractual usage of a "cloud" server, instant gratification preservation—either by flipping a switch, sending the right legal hold, or through forensic replication—is unachievable. It is critical to have knowledge of what can and cannot be preserved, and how that preservation would be undertaken, on hand in order to effectively advocate in court and avoid the imposition of sanctions based upon fundamental misapprehensions of technology. Regular reviews of ESI data maps and ESI systems profile descriptions, quarterly meetings of e-Discovery counsel (usually in-house e-Discovery and technical specialists, IT representatives, RIM

[86] *See Mobile Device Management for Compliance: Archiving & Compliance for Smartphones*, GLOBAL RELAY, http://www.globalrelay.com/resources/files/Global-Relay-Mobile-Device-Management.pdf (last visited Feb. 10, 2014) (discussing that customers of Global Relay's SMS archiving service will not have to rely on systems such as BlackBerry Enterprise Servers to capture and archive text messages).

[87] For example, on December 18, 2013 a former BP engineer was convicted by a federal jury on one count of obstruction of justice for deleting potentially incriminating text messages from his cell phone. *See* Michel Kunzelman, *Ex-BP Engineer Convicted on 1 Obstruction Charge*, ASSOCIATED PRESS (Dec. 18, 2013, 3:23 PM), http://www.bigstory.ap.org/article/jury-standstill-ex-bp-engineers-trial.

representatives, and dedicated outside e-Discovery counsel), early escalation of key ESI discovery disputes to knowledgeable and able advocates, and the development of reasoned and evidentially-supported positions are critical recommendations that business organizations should consider.

D. Case Assumption #4: Standard Federal Rule 26(c) Protective Orders Automatically Provide Effective Protections to Address Privacy Rights and Interests.

Truth: Rule 26(c) was not originally designed to address individual privacy rights, and certainly not with a view to global laws and expectations that are dramatically different from US rules and laws.

[40] The Federal Rules of Civil Procedure provide that upon a showing of "good cause" the court may issue an order to forbid, limit, or make secret from the public specified discovery.[88] Such orders, termed "protective orders," may be issued upon the motion of one party or pursuant to the stipulation of all parties to the litigation.[89] Protective orders that limit the disclosure of trade secrets, or other information a business is compelled to keep private, have become more common in various types of litigation. Such orders serve myriad objectives, including: the protection of corporate secrets; stemming dissemination of discoverable information from passing to other potential litigants; preventing embarrassment; and keeping adverse parties from releasing discoverable information to the public where the same may prejudice the potential jury pool.[90] While the scope of Rule 26(c) is broad, it does not specifically acknowledge that a litigant may have an obligation to protect the privacy of third parties such as customers or employees during the

[88] FED. R. CIV. P. 26(c)(1).

[89] *See id.*

[90] *See* Jacqueline S. Guenego, *Trends in Protective Orders Under Federal Rule of Civil Procedure 26(c): Why Some Cases Fumble While Others Score*, 60 FORD. L. REV. 541, 542-52 (1991).

course of discovery. The sections below illustrate the emerging complexity of privacy considerations in a world of extensive ESI, and why litigants must carefully craft and deploy proper protective order provisions that will appropriately guard private information.

1. Common Law

[41] The tort of intrusion on seclusion provides a right to privacy[91] in most states.[92] The Restatement (Second) of Torts defines the tort of intrusion on seclusion as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[93] Courts adopting this tort have variously operationalized it in two, three, or four element tests.[94] In addition, other torts such as public disclosure of private

[91] Stengart v. Loving Care Agency, Inc., 900 A.2d 650, 660 (N.J. 2010) (stating "the common law source [of a right to privacy] is the tort of 'intrusion on seclusion'"); *see also* Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 760-61 (N.D. Ohio 2013) (discussing the common law source of a right to privacy as established by the tort of intrusion into seclusion).

[92] The Illinois Supreme Court recently recognized the tort in *Lawlor v. North American Corp. of Illinois* and listed the follow other states as recognizing the same claim: Alaska, Arkansas, California, Connecticut, Delaware, Florida, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Texas, Utah, Vermont, and West Virginia. 983 N.E.2d 414, 425 n.5 (Ill. 2012). Other states have codified this tort in statute. *See, e.g.*, WIS. STAT. ANN. § 995.50 (West 2007).

[93] RESTATEMENT (SECOND) OF TORTS § 652B.

[94] *See e.g.*, Martin v. Guevara, 464 F. App'x 407, 410 (5th Cir. 2012) ("The elements of a cause of action for invasion of privacy by intrusion on seclusion are 1) the defendant intentionally intruded on the plaintiff's solitude, seclusion, or private affairs, and 2) the intrusion would be highly offensive to a reasonable person.") (citing Valenzuela v. Aquino, 853 S.W.2d 512, 513 (Tex. 1993)); Thomas v. Corwin, 483 F.3d 516, 531 (8th Cir. 2007) (stating the claimant "must demonstrate (1) the existence of a secret and private subject matter, (2) the plaintiff's right to keep that subject matter private, and (3) the obtainment by the defendant of information about that subject matter through unreasonable means") (citing St. Anthony's Med. Ctr. v. H.S.H., 974 S.W.2d 606, 609-10

facts[95] or conversion of intangible property[96] may be applicable in some jurisdictions.

[42] While the legal principles underlying an individual's privacy interest may be varied, in many cases courts have sought to find a balance between an organization's legitimate business interests and the privacy interests of the individual constituent.[97] Various courts have identified the following factors that have weighed to some extent on their determination of whether an employee has a reasonable expectation of privacy in their electronic communication files:

(Mo. Ct. App. 1998)); Johnson v. K mart Corp., 723 N.E.2d 1192, 1196 (Ill. App. Ct. 2000) (recognizing the tort in the district and adopting four elements: "(1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is offensive or objectionable to a reasonable person; (3) the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering") (citing Melvin v. Burling, 490 N.E.2d 1011, 1013-14 (Ill. Ct. App. 1986)).

[95] *See* 103 AM. JUR. PROOF OF FACTS 3D *Invasion of Privacy By Public Disclosure of Private Facts* 159 § 1 (2008).

[96] *See, e.g.*, Eysoldt v. ProScan Imaging, 957 N.E.2d 780, 786 (Ohio Ct. App. 2011).

[97] *See* Bogie v. Rosenberg, 705 F.3d 603, 610-611 (7th Cir. 2013) (finding that in order to survive a motion to dismiss a claim for invasion of privacy under Wisconsin law, the plaintiff had to show that "a reasonable person could have an expectation of privacy when visiting a celebrity performer's backstage area where the general public, of which [plaintiff] was a member, was not allowed"); Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998) (noting that intrusion on seclusion "is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source"); Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 760-61 (N.D. Ohio 2013) (to demonstrate an intrusion into seclusion "the affairs or concerns must be private to rise to be actionable as an invasion of privacy. . . . 'In order to establish a wrongful intrusion into private activities, a plaintiff must show that he or she had a reasonable expectation of privacy in the area allegedly intruded'") (quoting Moore v. Univ. Hosp. of Cleveland Med. Ctr., No. 1:11-CV-00508, 2011 U.S. Dist. LEXIS 131854, at *11-12 (N.D. Ohio Nov. 15, 2011) (internal citations omitted)).

(1) Ownership of the device upon which the communications were made or viewed;[98]
(2) Ownership of the account with the service provider;[99]
(3) Ownership of the supporting infrastructure, such as computer networks used to transmit the communication;[100]
(4) Steps the employee took to secure the communication/information, such as creating a password on the device, encrypting the information, or deleting copies of the information;[101]
(5) Communication or information made, accessed, or stored in a public place where it could be observed by an onlooker;[102]
(6) Employer policies or notices regarding whether personal use is allowed and employee expectations of privacy and whether the employee was aware of these policies; and[103]

[98] *See, e.g.*, Sitton v. Print Direction, Inc., 312 718 S.E.2d 532, 537 (Ga. Ct. App. 2011) (explaining that an employer's review of employee's e-mail on employee's personal laptop computer that employee used in conducting employer's business, even if "surveillance," did not constitute such an unreasonable intrusion of employee's seclusion or solitude as to rise to level of invasion of privacy).

[99] *See, e.g.*, Mintz v. Mark Bartelstein & Assocs., 906 F. Supp. 2d 1017, 1033 (C.D. Cal. 2012) (stating that a reasonable jury could only find that plaintiff had an expectation of privacy in his personal e-mail account after employer defendant hacked his personal account despite the fact that plaintiff used a business account for business matters and only forwarded e-mails from his business account to his personal one when the e-mail concerned personal matters such as medical issues).

[100] U.S. v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007) (finding that a public employee did not have a reasonable expectation of privacy in his personal computer, in part because "he knowingly networked his machine to the city computer for the express purpose of sharing files").

[101] *See, e.g.*, *Mintz*, 906 F. Supp. 2d at 1033 (discussing plaintiff's use of a password on his personal e-mail account).

[102] *See, e.g.*, Sanders v. Am. Broad. Companies, Inc., 978 P.2d 67, 73-74 (Cal. 1999) ("[A]n employee may, under some circumstances, have a reasonable expectation of visual or aural privacy against electronic intrusion by a stranger to the workplace, despite the possibility that the conversations and interactions at issue could be witnessed by coworkers or the employer.").

(7) Routine practice regarding personal use, including whether any employer policies were routinely enforced.[104]

2. SCA & ECPA

[43] The Stored Communications Act ("SCA") protects an individual's right to privacy in specific electronic communications.[105] Specifically, the SCA gives network account holders statutory privacy rights against third-party access to information held by ISPs.[106] The private right of action under the SCA[107] establishes a civil cause of action against anyone who (1) accesses, (2) without authorization, (3) a facility through which an electronic communication service[108] is provided, and (4) thereby obtains access to a wire or electronic communication[109] (5) while it is in electronic

[103] *See, e.g., In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (developing a four prong test: "(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies").

[104] *See, e.g., id.*

[105] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213-14 (2004).

[106] *See id.* at 1213.

[107] *See* 18 U.S.C. § 2707(a) (2012).

[108] Under the statute, an "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." § 2510(15).

[109] "Electronic communication" includes transfer of data by electromagnetic system that affects interstate or foreign commerce. § 2510(12). E-mail is a form of electronic communication. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002) ("The legislative history of the ECPA [the larger act that encompasses the SCA] suggests that Congress wanted to protect electronic communications that are configured to be private, such as e-mail and private electronic bulletin boards."); *see also In re* Application of United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006) ("[T]here can be no

storage.[110] Courts have found that an organization violated the SCA when it used an employee's password stored on company-owned hardware to access an employee's private e-mail.[111] Similarly, employers have been found liable for violating the SCA when they coerced an employee to grant the employer access to electronic communications that would be protected under the SCA.[112]

3. NLRA

[44] The duty to bargain collectively under the National Labor Relations Act[113] "includes a duty to provide relevant information needed by a labor union for the proper performance of its duties as the employees' bargaining representative."[114] Nonetheless, privacy concerns may allow the employer to withhold certain information from the union, such as psychological aptitude tests,[115] medical information,[116] or information regarding strike replacements.[117]

---

doubt that [§ 2510(12)] is broad enough to encompass e-mail communications and other similar signals transmitted over the Internet.").

[110] "Electronic Storage" is intermediate storage incidental to the transmission of electronic communication and storage of that communication by the service provider for the purposes of backup. § 2510(17).

[111] *See, e.g.*, Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 755 (N.D. Ohio 2013).

[112] *See, e.g.*, Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 U.S. Dist. LEXIS 88702, at *8-9 (D. N.J. Sept. 25, 2009).

[113] *See* 29 U.S.C. § 158(a)(5).

[114] Detroit Edison Co. v. NLRB, 440 U.S. 301, 303 (1979).

[115] *See, e.g., id.* at 320.

[116] *See* Minnesota Mining & Mfg. Co., 1981-82 NLRB Dec. (CCH) P18,892, (1982).

[117] *See, e.g.*, Chicago Tribune Co. v. NLRB, 79 F.3d 604, 608 (7th Cir. 1996).

4. HIPAA & HITCH Act

[45] The Health Insurance Portability and Accountability Act ("HIPAA")[118] includes a privacy rule and a security rule that cover medical records and payment information defined as "protected health information" ("PHI") in both physical and electronic form.[119] The Privacy Rule regulates the use and disclosure of PHI by "Covered Entities," which includes health plans, health care clearinghouses and certain health care providers.[120] The Security Rule only applies to electronic PHI and specifies the administrative, technical and physical safeguards that covered entities must implement to secure electronic PHI.[121]

[46] Even if an organization is not a health care provider, it may acquire individual's PHI acquired through other business activities where PHI is collected from participating individuals. For example, a company that retains PHI for its employees is subject to the privacy and other safeguard requirements of HIPAA.

[47] The Health Information Technology for Economic and Clinical Health Act ("HITECH") augments HIPAA and imposes additional privacy and security provisions on the use and disclosure of electronic PHI. [122]

---

[118] Health Information Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 10 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C., 29 U.S.C., 18 U.S.C., and 26 U.S.C.).

[119] *See generally* U.S. DEP'T. HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAAPRIVACY RULE (2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf html.

[120] *See* 45 C.F.R. §§ 160.102, .104 (2013).

[121] *See Summary of the HIPAA Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Jan. 31, 2014).

[122] Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of Division A and Title IV of Division B of the American Recovery and

HITECH extends all of the privacy and security provisions of HIPAA to "Business Associates"[123] of Covered Entities.[124] To the extent a business associate holds electronic PHI, the organization is subject to the administrative, physical and technical safeguards imposed by HIPAA's Security Rule, meaning that it will need to take reasonable steps to safeguard the data.[125] This requirement also could extend to the BYOD service provider if an end-user stores any PHI at the provider through automatic back-up or other storage services.

5. Foreign Jurisdictions

[48] Finally, if ESI is stored in a location outside the United States, laws of foreign jurisdictions, such as the European Union, may come into play. The European Data Protection Framework contains many requirements and nuances that are outside the scope of this article. Nonetheless, the European Union, in contrast to the United States, considers personal privacy to be a fundamental right.[126] As a result, the European Union has promulgated directives providing for heightened privacy protections of sensitive personal data held by corporations operating within its borders. The current framework includes the Data

Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009) (codified at 42 U.S.C. § 17931 et. seq.).

[123] Services that a business associate may provide include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. 45 C.F.R. § 160.103; *Business Associates*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last visited Jan. 26, 2014).

[124] *See id.*

[125] *Summary of the HIPAA Security Rule*, *supra* note 121.

[126] *See* McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 651 (2012).

Protection Directive,[127] the complementary E-Privacy Directive,[128] and the Data Retention Directive[129]. In general, the Data Protection Directive governs the way in which an organization processes personal data. Member states then adopt local legislation addressing the means by which data controllers must protect personal information.[130]

[49] The European Union Article 29 Working Party (the standing committee that addresses data protection issues) construes the definition of "personal data" broadly. The Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject')."[131] Data need not refer to a person directly in order for authorities to construe the data as personal; rather, it may be any data that allows an entity to identify an individual. The data controller must comply with the key principles established by Article 6 of the Data Protection Directive when processing personal data. In general, these include fair and lawful processing,[132] collection for specified, explicit, and

[127] *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF [hereinafter Data Protection Directive].

[128] *See* Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF; Council Directive2009/136, 2009 O.J. (L337) 11 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

[129] *See* Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[130] *See, e.g.*, Loi 78-17 du 6 janvier 1978 d'informatique et libertes [Lqw 78-17 of January 6, 1978, on information technology, data files and civil liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Aug. 7, 2004 (Fr.), *amended by* Law No. 2004-801 of Aug. 6, 2004, Law No. 2009-526 of May 13, 2009, *available at* http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf.

[131] *See* Data Protection Directive, *supra* note 127, art. 2(a), at 38.

[132] *See id.* at art. 6(1)(a), at 40.

legitimate purposes,[133] data minimization,[134] data accuracy,[135] data retention,[136] and data security.[137] In addition, as a general rule, organizations cannot transfer personal data to a country outside the European Union unless that country provides an "adequate level of protection" for personal data.[138]

[50] The broad discovery mandates of the United States' legal system often clash with the European emphasis on privacy. The United States "lack what the [European] Commission would deem an 'adequate level'" of safeguards, a view that encompasses the legal system.[139] As noted above, an organization may not transfer data to a country that is not a member of the European Union unless it follows one of the accepted

[133] *See id.* at art. 6(1)(b).

[134] *See id.* at art. 6(1)(c).

[135] *See* i*d.* at art. 6(1)(d).

[136] *See* Data Protection Directive, *supra* note 127, at art. 6(1)(e).

[137] *See id.* at art. 17(1).

[138] *Id*. at art. 25(1). An organization can rely on one of several options to determine whether a country or entity within another country provides an adequate level of protection. These mechanisms include: Adequacy Determination (a country provides an adequate level of protection for personal data (this grouping does not include the United States)) Safe Harbor (privacy principles established by the United States Department of Commerce with which an organization can comply (an organization must apply to the Department of Commerce for a Safe Harbor designation)); Model Clauses (contractual clauses to which the exporting and importing controller (or processor) can agree); Binding Corporate Rules (BCRs) (legally binding rules that a multinational organization can adopt for transfers within its environment); Derogations (limited exceptions to requirements for adequate data protection).

[139] *See* Stephen A. Oxman, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?*, 24 B.C. INT'L & COMP. L. REV. 191, 199 (2000), http://lawdigitalcommons.bc.edu/iclr/vol24/iss1/8/ (citing Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 158 (1996)).

mechanisms.[140] These options do not address the situation in which personal information residing in the European Union may be relevant to a claim or defense in a court within the United States. Nonetheless, American courts may assume that these challenges can be managed, or are not decisive.

[51] As the intersection of personal versus business use of devices has become more expansive, the preservation and collection of *unique relevant business information* has become a challenge. The blending of business and personal data has undoubtedly beckoned the attention of member state data protection authorities. For example, the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), has taken an active interest in the privacy implications of the increased adoption of BYOD within French organizations.[141] Organizations should continue to monitor future guidance issued by the EU, the CNIL, and other national data protection bodies.

[52] Each of the illustrative sources of privacy rights examined above support the proposition that a "blanket protective order" may no longer be enough to secure and protect privacy rights that other laws and rules recognize. Best practice guidance dictates that lawyers and clients discard old boilerplate protective order forms in favor of new templates that adequately address the data at issue.[142] Terms of protective orders may

[140] *See* Data Protection Directive, *supra* note 127, at art. 25(1)-(6).

[141] *See European Data Protection Day: Progressing Towards More Reliable and Modern Regulation*, ASIP SANTÉ (Aug. 9, 2013), http://esante.gouv.fr/en/actus/services/rollout-the-cps-3-health-professional-card-complete.

[142] *See* Gibbons P.C., *New York Appellate Court Refuses to Amend Confidentiality Order to Address Runaway Data Issue*, E-DISCOVERY LAW ALERT (Feb. 28, 2011), http://www.ediscoverylawalert.com/2011/02/articles/legal-decisions-court-rules/new-york-appellate-court-refuses-to-amend-confidentiality-order-to-address-runaway-data-issue/; *cf.* Timothy Lendino et al., *Confidentiality and Protective Orders*, SMITH MOORE LEATHERWOOD (Aug. 5 2013), http://www.smithmoorelaw.com/Confidentiality-and-Protective-Orders-08-05-2013 (discussing generally how counsel should consider potential applicable issues before agreeing to a "standard, 'on size fits all' protective order").

need to be far more prescriptive regarding transmission, storage, retrieval and deletions of data—including deletions from disaster recovery systems. Any data, devices, system inspections, or data recovery efforts need to have detailed protocols that address the protection of domestic and foreign privacy rights (if applicable). In short, the dictates of procedural protection need to address the litigation information lifecycle from clients to vendors, to lawyers, to opposing parties, to courts. The procedural requirements to protect information may even affect the sequencing of discovery to avoid, unless necessary, transgressing privacy rights.

E. Case Assumption #5: Emerging Technologies Are Making It Easier to Isolate Relevant Discoverable Information and Decrease Preservation Burdens.

Truth: Emerging technologies make it easier to preserve data in bulk and in largely undifferentiated format. Yet as the capacity for preservation (i.e., storage) increases, the ability to discern, retrieve, and produce relevant discoverable data does not increase commensurately. In relative terms, it actually decreases.

[53] The subset of ESI likely to be relevant to any particular litigation that exists within the greater whole of data under the possession, custody, and control of the party is often miniscule. At the outset of discovery, however, most data architecture systems do not provide a reasonable method for identifying and preserving likely relevant data. At best, parties can choose to preserve, en masse, the systems (and their contents) that are typically used to conduct business of the nature of the subject litigation during the time period deemed relevant (from the date of the triggering event forward). The assumption that a party can easily discern, isolate, and collect the relevant discoverable information from this monolith of data is a persistent myth.[143]

[143] In reality, the sheer volume of data that now exists and can be preserved, or is being preserved, is such that the data often has limited utility in an organization's efforts to cull information that might be beneficial to its business operations. As a recent commentator noted, "absent investment in costly search technologies capable of federated searches across platforms and storage containers, these volumes of information may jeopardize the

[54] The duty to preserve relevant discoverable information does not give rise to an obligation to preserve every piece of information conceivably related to the general subject matter of the litigation. In *Zubulake IV*, Judge Scheindlin observed that the duty to preserve is not boundless, stating, "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 . . . that are almost always involved in litigation."[144]

[55] Implicit in Judge Scheindlin's observation is the notion of proportionality in preservation. Judge Lee Rosenthal of the Southern District of Texas explained the need for proportional preservation in *Rimkis Consulting Group v. Cammarata*, stating that a determination on whether a party had fulfilled its preservation obligations "depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case and consistent with clearly established applicable standards."[145]

[56] One challenge of proportionality is that the duty to preserve electronic data, and the possibility of sanctions for failure to uphold that duty, is tied directly to the relevancy requirements governing all discovery obligations under the Federal Rules of Evidence, which are determined at the time of trial. If a party affirmatively limits the scope of preservation, and it is later revealed that the party failed to preserve or produce relevant data previously available to that party, the defending party is forced to argue a logical negative: that it could not have reasonably anticipated that evidence would be relevant, so even the failure to preserve it in the face of

organization's ability to retrieve valuable information efficiently such that strategic opportunities are lost." Ragan, *supra* note 69, at ¶ 3.

[144] *Zublake IV*, 220 F.R.D. at 217 (2003).

[145] Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (emphasis omitted).

its later-determined relevancy was not a breach of the duty.[146] The liability that parties may expect if left with no better defense than "we-didn't-realize-at-the-time" is potentially crippling.[147] Moreover, as practitioners, we know that trial courts have little fear of being overruled on appeal for imposing preservation requirements that are too broad. Indeed, the cruelty of the situation becomes apparent when one considers that of the most experienced judges who has opined on ESI uses, Magistrate Judge James Francis of the Southern District of New York, remarked that the attractive concept of proportionality in preservation is largely elusive because it cannot easily be defended:

> Reasonableness and proportionality are surely good guiding principles for a court that is considering imposing a preservation order or evaluating the sufficiency of a party's efforts at preservation after the fact. Because these concepts are highly elastic, however, they cannot be assumed to create a safe harbor for a party that is obligated to preserve evidence but is not operating under a court-imposed preservation order. Proportionality is particularly tricky in the context of preservation. It seems unlikely, for example, that a court would excuse the destruction of evidence merely because the monetary value of the anticipated litigation was low.[148]

[57] Thus, the circular nature of the preservation/sanction dichotomy unfolds. The recitation of the limits of preservation in cases such as *Zubulake* and *Rimkis* is entirely without practical import unless producing

[146] *See Zubulake IV*, 220 F.R.D. at 218, 220.

[147] *Cf.* 5 LEWIS S. MIKE EIDSON & SEAN M. CLEARY, LITIGATING TORT CASES § 58:29, *available at* Westlaw LITGTORT § 58:29 (last updated August 2013) ("Sanctions arising out of a charge of electronic spoliation of evidence, even pursuant to a regular business practice, can be extremely harsh." (citations omitted)).

[148] *See* Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 436 n.10 (S.D.N.Y. 2010).

parties have a reasonable method for extracting relevant discoverable information from the haystack.

[58] In short, this assumption is based on the idea that we can easily and accurately extract information meeting our desired criteria from the whole data universe available for preservation. First, this assumes some triage capability in initial preservation, which often does not exist in reality. Absent saving "every scrap," we must cede that there is a statistical likelihood that relevant discoverable data will not be preserved. The greater the piece of the data pie that is not saved the larger that error percentage becomes. We don't know what we don't know. Second, even in the most well-tailored and accurately targeted (but still overly-inclusive) preservation efforts, we do not yet have the search tools to guarantee the end product. Parties and courts cite new and marvelous developments in the methods available for the isolation of relevant discoverable evidence: from basic key word searches to more sophisticated predictive coding and sampling to brand-specific search platforms that combine multiple technologies.

[59] In terms of best practices developments, there is perhaps no more pernicious challenge than the search for a *reasoned* way to find what parties need for the fair and just resolution of a dispute without emptying every literal and figurative cupboard and hoping that all of the Crown's horses and soldiers (and computers) can find what you need. Today there are substantial market forces at work urging courts, companies, and litigants to deploy various software packages and systems to "efficiently" find the information sought. Yet, for all of the marketing splash and scholarly debate, the proof of improved results and efficiencies has not been fully established. We can only hope to improve those odds by employing increasingly advanced methodologies and technologies that cost more time and more money, diminishing any chance that the discovery process will even begin to comport with the dictates of Rule 1 of the Federal Rules of Civil Procedure. Notably, whether or not the parties propose extensive and sophisticated search terms or the deployment of extensive computer predictive analytics, courts are making

clear that they recognize the limits of their expertise and are starting to hold back from making decisions in the blind.[149]

[60] A key takeaway from this growing technological movement is that parties must take control of this area. For litigants with modest to significant dockets, having a comprehensive plan to approach search and retrieval (including various options depending on the size and complexity of matters) is critical to achieving courtroom and business process success (and budget sanity). This may require the selection of dedicated e-Discovery counsel (in-house and outside) to understand the company and the best deployment of methodologies to meet needs and engage the right vendors (and leveraging that understanding across cases and time). This imperative is all the more important when the judicial reluctance to decide in a vacuum is coupled with the mantra of cooperation—courts expect that parties, especially medium to large scale public and private enterprises, should be able to reach agreements on search and retrieval processes.[150] The flip side of this expectation is the likelihood that, in the event of a dispute, the party who took the most reasonable positions (with credible support) will prevail because the court will not have the time, expertise of patience to wade through the weeds of complex search methodology negotiations.

[61] Finally, while the authors believe that technology will provide better solutions, just as John Henry ultimately learned that the power of

[149] *See, e.g.*, Fort Worth Emp.'s Ret. Fund v. J.P. Morgan Chase & Co., No. 09 Civ. 3701 (JPO) (JCF), 2013 U.S. Dist. LEXIS 176384, at *15-17 (S.D.N.Y. Dec. 16, 2013); Kleen Prod. LLC v. Packaging Corp. of Am., No. 10 C 5711, 2012 U.S. Dist. LEXIS 139632, at *22 (N.D. Ill. Sept. 28, 2012); United States v. O'Keefe, 537 F. Supp. 2d 14, 23-24 (D.D.C. 2008).

[150] *See generally* The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009). As of October 2012, judges in the following states had endorsed the Proclamation: Alabama, Arizona, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Mississippi, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Washington, and Wisconsin.

technology is formidable,[151] the most important key to success in e-Discovery is the meaningful understanding of when technology will provide efficiencies, and when attorney expertise is required to guide the claims and defenses in the matter. The Supreme Court's directives regarding pleading from the past twenty years, which culminated most recently in the *Twombley* and *Iqbal* decisions, unmistakably indicate that litigants must articulate the foundational elements of claims (and by extension, defenses) in order to provide the framework for judicial resolution.[152] Without a sound understanding of the case, a lawyer cannot possibly articulate what needs to be found, whether using a basic human linear review or the most sophisticated algorithms. Indeed, even if she purchased the most effective search program ever developed, it cannot operate without her insight, direction and interaction. Likewise, she cannot meaningfully enter into the predicate Rule 26(f) discussions with her adversary concerning the necessary parameters of preservation and discovery in a case. And perhaps most importantly, a good argument can be made that she cannot competently represent her clients in the litigation.

III. CONCLUSION

[62] While case law may provide a starting point for analysis of a particular e-Discovery issue, because technology is not static, reliance on prior decisions must be approached with restraint. When The Sedona Conference Working Group 1 first met in the Fall of 2002, one of the prime concerns driving the formation of the group was the absence of case law guidance (stare decisis) on issues that were arising in the area of e-Discovery.[153] Into that void, The Sedona Principles were offered as best

[151] SCOTT REYNOLDS NELSON, STEEL DRIVIN' MAN: JOHN HENRY, THE UNTOLD STORY OF AN AMERICAN LEGEND 1-2 (2006).

[152] *See* Ashcroft v. Iqbal, 556 U.S. 662, 677-678 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 554-556 (2007).

[153] As noted in the introduction,

> [i]n Spring 2002, many of us who would later form the Sedona Conference Working Group on Electronic Document Production began

practice guidance, with a goal of guiding the development of legal standards.

[63] Nearly a dozen years later, it is now patently clear that the absence of case law guidance will likely be a recurring reality in the area of e-Discovery by virtue of the rapid evolution of technologies and connected social communication patterns that render the speed and nature of traditional case law guidance incapable of providing practical guidance to other courts, parties, and counsel. Indeed, as the examination of the exemplar assumptions in this article reveals, the notion of stare decisis in e-Discovery is like the disconnected collarbone highlighted in Justice Holmes' cat—it is no longer has utility.[154]

[64] Embracing this reality is critically important for all participants in the judicial process. For courts, it means that guidance in any given case should primarily be aimed at resolving the specific issue raised by the parties. To the extent that broader issues can be addressed to provide

> to discuss ways to develop "best practices" for lawyers to follow in addressing electronic document production. An industry of electronic discovery consultants and continuing legal education courses had developed, which suggested to some that all data ever generated electronically would be saved and made available for litigation. Courts handled ripe disputes, but with few decisions reported and a smaller number containing applicable guidance outside the context of the instant facts, organizations were uncertain as to their legal obligations. The collapse of Enron and Arthur Andersen, and the legislative response to these events, including the Sarbanes-Oxley Act of 2002, confirmed the importance of handling electronic document production in a defensible manner. It seemed doubtful to us that the normal development of case law would yield, in a timely manner, best practices for organizations to follow in the production of electronic documents.

THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATION & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 1 (Jonathan M. Redgrave et al. eds. 2003)

[154] *See* Holmes, *supra* note 1, at 630.

guidance, such guidance should be tailored to address fundamental legal principles untethered to the specific application of existing technologies or business processes. For parties and counsel, it means that reliance on prior cases addressing e-Discovery issues should be undertaken with more care and in fewer circumstances than may be done in other aspects of the case law. Citations to prior decisional law need to be carefully vetted to confirm reliance on stable legal principles rather than referral to technology-based results that are no longer valid or sustainable. Parties and counsel should also continue to look for (and develop) industry standards and best practices guidance as better starting points to guide the application of rules and technologies to a given circumstance in order to counsel clients and advocate positions to courts.[155]

[155] *See* Hon. Shira A. Scheindlin & Jeffery Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 up to the Task?* 41 B.C. L. REV. 327, 361 (2000)("[W]hile courts have managed to resolve motions that raise Rule 34 questions in the context of electronic discovery, they have generally approached these questions in a highly fact-specific manner, producing few general principles to aid in the resolution of similar disputes.").