2010

Using Computer Forensics to Enhance the Discovery of Electronically Stored Information

Franz J. Vancura

Bluebook Citation

This Note is brought to you for free and open access by UST Research Online and the University of St. Thomas Law Journal. For more information, please contact lawjournal@stthomas.edu.
NOTE

USING COMPUTER FORENSICS TO ENHANCE THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION

FRANZ J. VANCURA

"The duty to preserve relevant evidence is fundamental to federal litigation."1

I. INTRODUCTION2

Failing to preserve and produce electronically stored information is costly for attorneys and clients alike: incompetent or unethical attorneys risk disciplinary action and violate the rules of professional conduct, discovery disputes anger overburdened judges, and the offending parties often pay the price—literally and figuratively.3 The expansive and seemingly relentless growth of electronic discovery continues to radically alter the civil litigation landscape in terms of scope, mechanisms, cost, and complexity.4 Unfortunately, this landscape remains ridden with electronic discovery re-

---

* Gonzaga University, BA 2005, University of Saint Thomas, JD Candidate 2011. I am grateful to Mark Kosieradzki and Joel Smith for their help and encouragement in selecting this topic, to Laura Tushaus and the University of Saint Thomas Law Journal staff for all their hard work bringing this Note to publication, and to my parents and wife for their limitless encouragement, guidance, and support. Correspondence: franz.vancura@gmail.com


2. At the outset of this note, it is necessary to state what it does and does not attempt to accomplish. This note is solely limited to the discovery phase of pre-trial litigation. It does not deal with the eventual admissibility of any evidence gained through forensic imaging at trial. See Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007), which provides a thorough discussion of the issue of the admissibility of electronically stored information (ESI) and an exhaustive analysis of how ESI may be admitted into evidence. See also The Sedona Conference Working Group on Electronic Document Retention & Production, The Sedona Conference Commentary on ESI Evidence & Admissibility, 9 SEDONA CONF. J. 217 (2008) [hereinafter ESI & Admissibility].

3. See, e.g., Genworth Fin. Wealth Mgmt., Inc. v. McMullan, 267 F.R.D. 443, 448 (D. Conn. 2010) (“Plaintiff’s motion for sanctions is warranted by the fact that it had to seek Court orders to obtain that to which it has been entitled but which the Defendants unreasonably and dubiously refused and possibly intentionally made unavailable. . . . The Defendants have wasted the Plaintiff’s and the Court’s resources in necessitating the judicial resolution of this discovery dispute.”).


727
lated casualties or failures, which are ultimately preventable.\textsuperscript{5} Knowing and abiding by the rules of civil procedure are essential to conducting electronic discovery. At a minimum, this entails identifying when the duty to preserve electronically stored information arises, as well as the types of information that a litigant or potential litigant must maintain once the duty to preserve electronically stored information arises. Traditional discovery methods and knowledge of the federal rules of civil procedure are no longer sufficient for conducting competent electronic discovery.\textsuperscript{6} Competent representation in cases involving electronic discovery now requires a familiarity with a wide variety of technologies.\textsuperscript{7} One such technology of increasing importance is forensic imaging.\textsuperscript{8}

Computer forensics is “the art and science of applying computer science to aid the legal process.”\textsuperscript{9} Broadly speaking, computer forensics involves the location, examination, identification, collection, preservation, and analysis of computer systems and electronically stored information (ESI).\textsuperscript{10} A forensic image, then, is an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space.\textsuperscript{11}

The courts vary significantly in their approaches to forensic imaging in civil litigation.\textsuperscript{12} Judges are more likely to allow forensic imaging in cases where a party seeking a Rule 26(c) protective order has failed to adequately fulfill its discovery obligations\textsuperscript{13} or when relevant evidence is being destroyed through the normal operation of a computer.\textsuperscript{14} Conversely, requests to access an opposing party’s computer(s) without proof of wrongdoing or

\begin{itemize}
  \item 5. \textsuperscript{Id.}
  \item 6. \textit{See} Alan J. Ross & Gregory J. Krabacher, \textit{Electronic Discovery in 2007: Discovering How Little We Know} 1 (2007) (“The prevalent use of technology in business . . . has unsettled the formerly well-established procedures by which parties to federal litigation prepared their case in the pre-computer era.”).
  \item 7. \textit{See} Mark L. Tuft, \textit{Ethical Challenges in Emerging Technology}, 24 No. 4 GPSOLO 64, 64 (June 2007) (“A lawyer’s duties of competence and diligence could take on a new meaning as the practice of law becomes increasingly paperless. Competent representation requires more than legal knowledge. It also requires the skill, thoroughness, and preparation reasonably necessary for the representation.”).
  \item 8. Forensic imaging is also known as mirror imaging or forensic copying. It is different from forensic examination.
  \item 9. \textit{ESI & Admissibility}, supra note 2, at 228.
  \item 10. \textit{Id.}
  \item 12. \textit{See}, e.g., John B. v. M.D. Goetz, Jr., 531 F.3d 448, 459 (6th Cir. 2008) (“Because litigants are generally responsible for preserving relevant information on their own, such procedures, if at all appropriate, should be employed in a very limited set of circumstances.”). The Goetz court, however, went on to state in dicta that forensic imaging is not uncommon in civil discovery and that parties may choose on their own to preserve information through forensic imaging. \textit{Id.}
  \item 13. Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1054–55 (S.D. Cal. 1999) (allowing plaintiffs to forensically image defendant’s hard drive where defendant had a habit of regularly deleting relevant files from her computer).
other exceptional circumstances are often unsuccessful. Courts, commentators, and litigating attorneys alike cite concerns about attorney-client privilege, confidentiality, relevance, and cost when arguing against granting an opposing party direct access to personal or work computers in order to obtain a mirror image. Though not lacking a rational basis, these fears are all readily dismissible if counsel cooperate and employ effective procedural methods to protect their client’s private, irrelevant, or protected information.

Yet, in the oft-quoted words of a federal judge, “[t]oo often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.” Thus, the thesis of this note is that foreseeable litigants should, and will likely be required to, forensically image relevant digital storage devices at the onset of litigation to remedy the negligent, grossly negligent, and intentional discovery abuses that waste the court’s time, wantonly increase the cost of litigation, and prevent the merit-based adjudication of a lawsuit. This note will further argue that courts should liberally grant a party’s request to forensically image and examine an opponent’s digital storage devices when there is strong evidence of spoliation or other discovery abuses.

To this end, Part II of this note will discuss when the duty to preserve ESI arises as well as the extent of that duty. Part III will address the privacy, attorney-client privilege, relevance, and cost related concerns that often arise when forensic imaging is a potential component of civil litigation. In Part IV, this note will discuss how voluntary or court-ordered imaging at the onset of litigation can help to solve the problems of Parts II and may have relevant information, on their computer equipment, which is being lost through normal use of the computer . . . .

15. See, e.g., Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fla. Jan. 18, 2007) (“Plaintiff’s requests simply seek computer hard drives. Plaintiff does not provide any information regarding what it seeks to discover from the hard drives nor does it make any contention that Defendants have failed to provide requested information contained on these hard drives.”).


17. See Goetz, 531 F.3d at 460 (“The district court’s compelled forensic imaging orders here fail to account properly for the significant privacy and confidentiality concerns present in this case.”).


19. Citizens for Responsibility & Ethics in Wash. v. Exec. Office, No. 07-1707, 07-1577, 2008 WL 2932173, at *3 (D.D.C. July 29, 2008) (denying defendant’s request to image defendant’s hard drive failed after the court subjected plaintiff’s request to a cost/benefit analysis and determined that a large portion of data was already irretrievably lost).

III. Finally, Part V will advocate for liberal judicially ordered direct access when a producing party has failed to image its relevant digital storage devices or is otherwise negligent in its duties to produce relevant ESI.

II. D U TY TO P R E S E RV E

The destruction, intentional or otherwise, of non-privileged ESI relevant to anticipated or ongoing litigation is unethical and subverts the long-standing common law principal that “[m]utual knowledge of all the relevant facts gathered by both parties is essential to proper litigation.”21 Failing to preserve relevant evidence also violates the Model Rules of Professional Conduct’s prohibition against obstructing a party’s access to evidence.22 Forensic imaging all potentially relevant digital storage devices in anticipation of litigation will help ensure full compliance with the Rules of Civil Procedure and Professional Conduct. This section explains when a party’s duty to preserve relevant, non-privileged evidence arises. It also explains what kinds of evidence a party must preserve, and argues that forensic imaging can be an efficient and cost-effective way to competently manage the earliest stages of a lawsuit involving the discovery of electronically stored information.

A. When the Duty to Preserve Arises

Although the duty to preserve evidence is well recognized at common law,23 many electronic discovery related casualties stem from counsel’s failure to adequately administer a timely litigation hold.24 Identifying the boundaries of the duty to preserve involves two related inquiries. First, a litigant must determine when the duty to preserve arises.25 The duty to preserve evidence “arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.”26 This means that the obligation to preserve
documents necessarily begins at the onset of a lawsuit, but may arise before the initiation of any litigation.

The concept of “future litigation” in the Federal Courts is largely undefined. Courts apply a case-by-case approach to determine whether a party has satisfactorily fulfilled its preservation duties. Therefore, it is impossible to provide a definitive list of factors that will trigger the duty to preserve, but litigants are not without some guidance from the courts. The mere contemplation that an employee may sue sometime in the future does not generally trigger a firm-wide duty to preserve. Courts will look at the level of awareness among employees that future litigation may arise to determine if a party should have reasonably anticipated litigation. Conversely, a potential plaintiff is under a duty to preserve evidence where she anticipates or considers filing a lawsuit. In tax litigation with the federal government, the circuit courts are split as to whether an audit triggers the duty to preserve in anticipation of litigation.

As a general guideline, courts use the following factors to resolve a conflict about whether a duty to preserve exists: (1) the extent to which the producing party’s conduct was intended to affect the opposing party, (2) the foreseeability of harm to the opposing party, (3) the degree of certainty that the opposing party suffered injury, (4) the closeness of the connection between opposing party’s conduct and the requesting party’s injury, (5) the moral blame attached to the opposing party’s conduct, and (6) the court’s desire to prevent the conduct in the future. When applying these criteria, courts seem especially focused on the disposition of the litigant (whether it is the plaintiff or the defendant) and the likelihood of litigation to determine whether a party was under an obligation to preserve.

---


28. United States v. Grammatikos, 633 F.2d 1013, 1019–20 (2d Cir. 1980). See also Conso. Edison Co. of N.Y., Inc. v. United States, 90 Fed. Cl. 228, 239 (2009) (“[T]he facts and circumstances of the individual case must be assessed to decide when litigation should be deemed by a court to be anticipated . . . .”); Mohrmeyer v. Wal-Mart Stores East, L.P., No. 09-69-WOB, 2009 WL 4166996, at *3 n.1 (E.D. Ky. Nov. 20, 2009) (holding that Wal-Mart did not violate discovery rules by destroying a restroom cleaning log as part of the company’s standard document retention policy where plaintiff waited over a year after a slip and fall accident to file a lawsuit. In many cases, notice and/or knowledge of the realistic threat of litigation will evolve more slowly, making the precise trigger date more difficult to determine).


30. *Id*.


Attorneys should begin formulating a litigation hold plan as soon as potential litigation becomes more likely than not. With a litigation hold plan in place, attorneys can monitor events to determine if any further action is necessary. As the probability of litigation turns from a mere possibility to likely, attorneys should begin to implement a litigation hold in order to avoid sanctions and ensure that all relevant evidence is available for production.

B. What Parties Must Preserve

We have already seen that a litigant or potential litigant must first determine when the duty to preserve arises. The second relevant inquiry is what must be preserved.\textsuperscript{34} Under the Federal Rules, opposing counsel is entitled to obtain discovery regarding "any non-privileged matter that is relevant to any party’s claim or defense."\textsuperscript{35} Parties must retain all relevant documents in existence at the time the duty to preserve arises in order to adequately comply with Rule 26(b)(1).\textsuperscript{36} The duties to preserve and produce relevant documents are ongoing throughout discovery and do not end after the initial disclosure.\textsuperscript{37} Litigants have a continuing duty to supplant disclosure of documents throughout the discovery phase of a trial.\textsuperscript{38}

Because of the vast amount of potentially discoverable ESI, civil discovery and its corresponding duty to preserve and produce information has become increasingly complex and expensive.\textsuperscript{39} A typical company with 20,000 employees can expect to store a total of approximately 4.5 billion e-mails in little more than a decade’s time.\textsuperscript{40} This means that a company with even a fraction of 20,000 employees is capable of producing a staggering amount of ESI. Given the massive amount of potentially discoverable information, the courts cannot and do not expect that parties will attain perfection in their preservation efforts.\textsuperscript{41} The standards for sufficient discovery have been set by years of judicial decisions analyzing misconduct and determining what a party must do to determine and meet its obligation to participate meaningfully in the discovery phase of a proceeding.\textsuperscript{42}

\textsuperscript{34} Zubulake, 220 F.R.D. at 216.
38. Id. at 433; Fed. R. Civ. P. 26(e).
40. Goss, supra note 27, at 799.
42. Id. at 464.
A party or potential party to litigation is free to choose how to preserve documents, and is not required to preserve every document in its possession. However, it is well established that parties have a duty to preserve what they know or reasonably should know is relevant to the action, is reasonably likely to be requested in discovery, or is subject to a pending discovery request. To ensure a good faith effort in preserving all relevant documents, parties need to be proactive. This requires identifying privileged documents as well as locating “key players” to determine the location of non-privileged relevant documents for preservation. Once a party has fulfilled these obligations, it must produce any and all relevant, unprivileged documents that an opposing party properly asks for in a request for production.

C. Producing Documents

Rule 34 grants a litigating party the power to inspect, copy, test, or sample documents and other tangible things, yet this power is not absolute. All discovery is governed by the “proportionality principal” of Rule 26(b)(2)(C).

The proportionality principal provides that a party need not preserve or produce documents when the potential benefits are outweighed by the burden or costs. Determining whether the production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format. Active data, online data, near-line data, and off-line storage or archived data are all typically classified as accessible.

43. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (Zubulake IV). However, the 2006 Amendment to the Advisory Committee Note to Rule 34(a) makes clear that FED. R. CIV. P. 34(a) requires the producing party to translate in a readily usable form any documents not stored in readily accessible forms.

44. Id. at 217; see also Malletier v. Dooney & Bourke, Inc., No. 04 Civ. 5316, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (holding company had no additional duty to install equipment to preserve the conversations in a chat room).

45. Zubulake, 220 F.R.D. at 217 (“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’.”).

46. Id. at 218 (the duty to preserve extends to those employees likely to have relevant information—the “key players.”).


48. See FED. R. CIV. P. 34.

49. Additionally, Rule 26(b)(2)(B) limits the preservation and production of ESI. “A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.” FED. R. CIV. P. 26(b)(2)(B).


52. Id. at 319–20.
Conversely, data on backup tapes and erased, fragmented, or damaged data are usually deemed inaccessible. The main difference between accessible and inaccessible data is the format and speed of accessing the stored data. Accessible data is simply stored in a more readily usable format.

Federal Rule 37(e) also governs a party’s duty to preserve relevant ESI. Rule 37(e) provides a safe harbor by limiting a court’s ability to sanction a party “for failing to provide electronically stored information lost as the result of the routine, good-faith operation of an electronic information system.” At least one court has recently applied Rule 37(e) in a traditional discovery context and held that courts should apply Rule 37(e) narrowly. Litigants are still required, however, to preserve all relevant non-privileged documents. Rule 37(e) only protects genuinely surprised—as opposed to unwary—parties when they fail to preserve documents in the normal course of business and they could not reasonably foresee the impending litigation.

In many cases involving electronic discovery, forensic imaging relevant digital storage devices at the onset of a litigation is a safe, efficient, and cost effective way to guarantee that a party adequately maintains all discoverable documents. The forensically imaged drives, like their original counterparts, are subject to the same discovery restrictions as traditional discovery. Thus, wary clients and attorneys can be assured that they will not be forced to produce trade secrets or irrelevant, confidential, or work-product-protected material to an opponent absent any future discovery abuses.

III. Barriers to Forensic Imaging: Cost, Privilege, Privacy, and Relevance

The proportionality principal has many implications for a party wishing to forensically image a digital storage device. Chief among these implications is cost. Other considerations include the inadvertent production of work product, privileged communication, irrelevant documents, and invasion of a party’s privacy. This section will address the issues precluding a more liberal attitude toward forensic imaging and will offer proposals to deal with these issues.

53. Id. at 320.
54. Id. See Citizens for Responsibility & Ethics in Wash. v. Exec. Office of the Pres., Nos. 07-1707 (HHK/JMF), 07-1577 (HHK/JMF), 2008 WL 2932173, at *3 (D.D.C July 29, 2008), for a good example of how a court will apply the proportionality principal to decide whether to allow a party to access certain relevant ESI.
57. See supra notes 16–19 and accompanying text.
A. Cost

Cost is the one factor in forensic imaging that is difficult to mitigate. Market forces determine the cost of imaging and searching a digital storage device. In relatively small cases, the cost of imaging a single drive may be cost prohibitive. In larger cases, the cost of hiring an expert to forensically examine or reconstruct files on imaged storage devices can easily exceed hundreds of thousands of dollars. Yet, there are steps that parties to a lawsuit can take to make forensic imaging both feasible and a best practice during the discovery phase of litigation.

First, the party requesting a forensic image can agree to pay the production costs. This is a particularly attractive option in cases where an opposing party cannot afford an expert to image or examine its digital storage devices; ordinarily, the producing party is responsible for all production costs. Courts have ordered cost shifting when the documents sought are relevant but not readily accessible or the producing party has committed egregious discovery abuses. Cost shifting takes the financial burden off of the producing party and encourages the requesting party to act efficiently in order to keep costs down. If the requesting party is unable or unwilling to bear the entire cost of production, courts may order, or the parties can agree, to share the costs of production.

Aside from cost shifting, forensically imaging relevant storage devices at the outset of discovery can help reduce costs stemming from subsequent motion practice. Many discovery related casualties occur when parties fail to produce or preserve relevant documents. Such incomplete discovery disclosures increase the overall cost of litigation because the offended party

58. But see Zubulake, 217 F.R.D. at 318 (“Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.”).

59. Citizens, 2008 WL 2932173, at *3 (“[T]he ‘typical cost of forensic imaging a 100 GB hard drive is between $400 and $1,000 and it takes approximately two to three hours to complete the imaging.’”).

60. Id.

61. Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1058 (S.D. Cal. 1999) (granting plaintiff’s request to mirror image defendant’s hard drive but requiring plaintiff to pay all costs associated with the production of the mirror image).

62. See Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978) (noting that under the discovery rules, “the presumption is that the responding party must bear the expense of complying with discovery requests . . . .”).

63. See Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 284 (S.D.N.Y. 2003) (Zubulake III) (“[C]ost-shifting is potentially appropriate only when inaccessible data is sought. When a discovery request seeks accessible data—for example, active on-line or near-line data—it is typically inappropriate to consider cost-shifting.”).

64. See In re Two Appeals Arising Out of San Juan Dupont Plaza Hotel Fire Litig., 994 F.2d 956, 965 (1st Cir. 1993) (“Rule 26(f) expressly authorizes trial judges, following discovery conferences, to enter orders for ‘the allocation of expenses as are necessary for the proper management of discovery.’”).
will inevitably file time-consuming and expensive motions to compel or motions for sanctions. The Sedona Conference has recognized that cooperation between opposing counsel can greatly reduce the overall cost of litigation. Thus, if parties agree to forensically image relevant online storage devices and work cooperatively to set the search parameters, forensic imaging could reduce the overall cost of litigation.

B. Privilege and Work Product

Parties often object to forensic imaging on the ground that an opponent could gain access to material that is privileged or protected by the work product doctrine. There are methods parties can employ, however, to ensure that privileged or work-product-protected material is not produced. This section will explain how parties can protect the inadvertent production of privileged and work-product-protected material when forensic imaging is part of the discovery process.

Because courts differ in their treatment of inadvertently produced privileged or protected material, attorneys need to be familiar with their juris-

65. See, e.g., Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I). In the Zubulake cases cited throughout this note, UBS failed to preserve and produce relevant e-mails after they reasonably anticipated a lawsuit in an employee discrimination case. Zubulake was forced to file repeated motions to compel and motions for sanctions as a result of UBS' actions. Consequently, the discovery process dragged on for years. In the end, UBS was ordered to produce, at great expense, responsive e-mails from backup tapes. Id. at 324. UBS was also required to pay the costs for re-depositions required by the late production and received a sanction in the form of an adverse inference jury instruction with respect to the deleted e-mails. Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 437–38 (S.D.N.Y. 2004) (Zubulake V). See also 33 Am. JUR. 3d Proof of Facts § 1 (2009) (noting the trend toward severe sanctions for discovery failure since the Supreme Court decided Nat'l Hockey League v. Metro. Hockey Club, 427 U.S. 639 (1976)). In National Hockey League, the Supreme Court strongly upheld a district court's order and dismissal of plaintiff's case for failing to comply with a discovery order in timely fashion and encouraged similar action in other cases. Id. at 643.

66. The Sedona Conference is a highly regarded legal think tank that brings together leading jurists, lawyers, experts, and other professionals to promote the best practices and to otherwise move the law forward in a just and reasonable way. The Sedona Conference, http://www.thesedonaconference.org/ (last visited March 29, 2010).


68. See Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 261 n.10 (D. Md. 2008) (order denying defendant’s assertion of attorney-client privilege) (“[P]arties worried about the cost of employing properly designed search and information retrieval methods have an incentive to keep the costs of this phase of discovery as low as possible, including attempting to confer with their opposing party in an effort to identify a mutually agreeable search and retrieval method. This minimizes cost because if the method is approved, there will be no dispute resolving its sufficiency, and doing it right the first time is always cheaper than doing it over if ordered to do so by the court.”).

One way to minimize the risk of waiving privilege, regardless of the jurisdictional rules, is to use a claw-back agreement. Claw-back agreements protect responding parties from the most damaging consequences of inadvertent waiver by allowing them to “claw-back” the privileged material within a given time frame. Claw-back agreements can either be court ordered or take the form of a private agreement between litigating parties. Some claw-back agreements are so thorough that they do away with the need for privilege review altogether. To ensure the timely implementation of a claw-back agreement, parties can stipulate to a claw-back agreement at the initial discovery conference, which they can later adopt as a case management order.

When forensic imaging is or could be a factor in discovery, parties can explicitly agree that any privileged or protected information viewed by a third party vendor does not waive the privilege. However, absent an additional agreement, a producing party must still review documents to screen for protected material.

---

70. Victor Stanley, 250 F.R.D. at 257 (explaining the three ways courts decide if inadvertent production of protected or privileged material constitutes a waiver).
71. Claw-back agreements are also called non-waiver agreements.
73. Fed. R. Evid. 502(d) (“A federal court order that the attorney-client privilege or work product protection is not waived as a result of disclosure in connection with the litigation pending before the court governs all persons or entities in all state or federal proceedings, whether or not they were parties to the matter before the court, if the order incorporates the agreement of the parties before the court.”).
74. Fed. R. Evid. 502(e) (“An agreement on the effect of disclosure of a communication or information covered by the attorney-client privilege or work product protection is binding on the parties to the agreement, but not on other parties unless the agreement is incorporated into a court order.”).
75. Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (Zubulake III) (“Many parties to document-intensive litigation enter into so-called ‘claw-back’ agreements to allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents.”). However, under the Federal Rules of Evidence, only those agreements that are court-ordered are enforceable against third parties and parties not presently involved in the action. See Fed. R. Evid. 502(d). If a non-waiver agreement is merely a private agreement between two or more parties, it is not enforceable against third parties. Thus, in order to guarantee the effectiveness of a claw-back agreement, litigating parties should have their agreement adopted by the trial judge in the form of an order.
76. Fed. R. Evid. 502(d).
78. Id. at *4 (“Plaintiff shall identify for deletion any information that is irrelevant and create a specific privilege log . . . . The expert shall remove the information claimed as privileged and provide all other information to Defendants.”).
C. Relevance and Privacy

Two final, closely related objections to direct access for purposes of forensic imaging are relevance and privacy. Private or personal information is rarely relevant in litigation and has the potential to expose litigants to unnecessary embarrassment or harassment. Today, hard drives that have a storage capacity of 100 gigabytes or greater are not uncommon and the price of storing data in an online or near-line format has dramatically decreased. The amount of potentially discoverable ESI on an average personal computer is staggering. Many people use their computers for a variety of functions including work, entertainment, communication, and personal accounts management. All but a small—albeit critical—percentage of ESI is likely discoverable on any given computer. The goal of discovery, then, is to identify, collect, and cull responsive documents from a larger institutional data universe and then search for and retrieve all relevant, non-privileged data. An essential method to reach this goal on any storage device, whether it is forensically imaged or not, is to target specific concepts or terms through the use of keyword searches.

Keyword searches identify all documents containing a specified term regardless of context. Therefore, in all but the most straightforward elec-

79. Hedenburg v. Aramark Am. Food Servs., No. C06-5267 RBL, 2007 WL 1627116, at *1 (W.D. Wash. Jan. 17, 2007) (plaintiff objected to defendant’s demand to mirror plaintiff’s hard drive after plaintiff had already produced in good faith all relevant ESI. “Plaintiff objects to the discovery as a ‘fishing expedition’ and has to date refused to permit the Defendant from accessing her home computer’s hard drive.”).


82. Manual for Complex Litigation (Fourth) § 11.446 (2010) (“One gigabyte is the equivalent of 500,000 typewritten pages. Large corporate computer networks create backup data measured in terabytes, or 1,000,000 megabytes; each terabyte represents the equivalent of 500 billion typewritten pages of plain text.”).

83. In allowing defendant direct access to the plaintiff’s computer for forensic imaging, the judge divided the information on plaintiff’s computer into three categories: (1) information related to the representation of clients in other cases, (2) personal information, and (3) information related to e-mail and website advertising litigation. Of the three categories, only the third was relevant and thus discoverable. Ferron v. Search Cactus, L.L.C., No. 2:06-CV-327, 2008 WL 1902499, at *1 (S.D. Ohio Apr. 28, 2008).

84. Achieving Quality, supra note 47, at 201.

85. See Retrieval Methods, supra note 81, at 194 (“In many settings involving electronically stored information, reliance solely on a manual search process for the purpose of finding responsive documents may be infeasible or unwarranted. In such cases, the use of automated search methods should be viewed as reasonable, valuable, and even necessary.”).

86. Id. at 201 (illustrating that a search for “the term ‘strike’ could be found in documents relating to a labor union tactic, a military action, options trading, or baseball, to name just a few . . . .”).
Electronic discovery, the key to a successful and targeted keyword search is precision. Poorly planned keyword searches not only fail to return an acceptable amount of relevant ESI, but they also waste the court’s time and increase the producing party’s risk of turning over privilege or work-product-protected documents. Keyword searches are not without limitations, but these limitations may be somewhat mitigated through the sampling process.

The use of sampling in the ESI discovery process is particularly effective in improving quality and reducing costs. Simply put, sampling uses a specified or random subset of a population as a representative example of the whole population. After a party has run a series of specified keyword searches and reviewed the results of the searches, sampling allows a producing party to determine the likelihood that the search was effective. Attorneys can accomplish this by comparing the prevalence of targeted search terms in the designated batch to a random sampling of all ESI across targeted storage devices. While sampling does not guarantee that all non-relevant or private ESI has been identified or filtered out, it minimizes risk and serves as a best practice in the discovery of ESI.

The courts have adapted to the privacy and relevance perils inherent in direct access orders by developing robust protective orders. Key components of such orders require that the requesting party’s forensic experts: (1) sign a confidentiality agreement agreed to by both parties and submit to the court’s protective order, (2) image relevant devices at their primary locations under supervision of opposing counsel, (3) maintain exclusive control over imaged devices, (4) search only potentially relevant sectors of the forensically imaged devices, (5) produce a written report of all potentially

87. Id. (“[T]he experience of many litigators is that simple keyword searching alone is inadequate . . . .”).
89. Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 256–57 (D. Md. 2008) (denying defendant’s assertion of attorney-client privilege where defendant failed to secure a claw-back agreement and, because of overly broad search terms, produced a host of privileged documents. In the ruling judge’s words, “[W]hile it is universally acknowledged that keyword searches are useful tools for search and retrieval of ESI, all keyword searches are not created equal . . . .”).
90. See Retrieval Methods, supra note 81, at 201–02, for a comprehensive critique of keyword search technology.
91. Achieving Quality, supra note 47, at 326.
92. Id.
93. Id. at 329.
94. See Retrieval Methods, supra note 81, at 217–22, for a good explanation of technological advancements in search and retrieval technology.
relevant documents for inspection only by the producing party, and (6) require in camera review of any contentious documents. 96

When properly utilized, the advances in search retrieval technology, the Federal Rules of Civil Procedure, and the vigorously developed judicial protective orders work remarkably well to control litigation costs and protect privileged, private, or protected material. Attorneys can forensically image relevant storage devices to protect their clients from sanctions and the astronomical costs of discovery disputes. When forensic examination of the imaged drives is necessary, producing parties can be assured that the examination will not result in a “fishing expedition” or an unwarranted invasion of non-relevant, private information. The totality of rules, technology, and judicial orders developed specifically for e-discovery make forensic imaging a best practice in many disputes involving the discovery of electronically stored information.

IV. BEST PRACTICE: IMAGING RELEVANT DIGITAL STORAGE MEDIA

Litigants are generally free to choose how to manage electronic data. 97 As the cost, complexity, and volume of e-discovery increase, however, parties to a lawsuit must have procedures that ensure discovery responses are adequate. 98 When counsel and the parties they represent fail to adequately preserve and produce responsive, non-privileged ESI, the results tend to be increasingly disastrous. 99 The duty to preserve and produce documents ultimately falls on the party-client. 100 Attorneys should develop methods to help protect their clients from unnecessary hardship resulting from discovery violations. Forensic imaging is one easy and relatively inexpensive method attorneys can use to ensure their clients’ documents are adequately preserved and produced. This section proposes, as a best practice for competently managing e-discovery, that attorneys should forensically image all relevant digital storage devices after they reasonably anticipate litigation in any case where forensic imaging is an appropriate and realistic option.

A. The Zubulake Requirements

In her final Zubulake opinion, Judge Scheindlin highlights the steps counsel should take to ensure compliance with their clients’ preservation

98. See Achieving Quality, supra note 47, at 302.
obligations. First, counsel should issue a litigation hold at the outset of litigation or when litigation is reasonably anticipated. Second, counsel must identify and communicate directly with key players. This entails informing key players of the exact nature and duty of the litigation hold to ensure full compliance and preservation. Third, attorneys should instruct all employees to preserve and produce their relevant files. Finally, Judge Scheindlin advises counsel to locate, label, and safe-keep all backup media, which the party is required to maintain. This last requirement may be read to require, as a best practice, that attorneys image and protect relevant digital storage devices as part of a normal litigation hold.

The primary difference between data stored on backup tapes or similar devices and data stored on a forensically imaged device is that the former is generally categorized as inaccessible. Retrieving inaccessible data is laborious and time consuming. In Zubulake and many other ESI disputes, several key players deleted relevant e-mails from their computers after they were informed of a litigation hold. The e-mails were stored on backup tapes, however, and UBS was ordered to produce the e-mails from the backup tapes—at great cost.

Despite the key players’ malfeasance, UBS could have maintained and produced the relevant deleted e-mails quickly and cheaply if counsel had immediately imaged each key-player’s hard drive(s). Data that is stored on an imaged drive and is neither deleted nor fragmented is readily accessible because it is maintained in an online format. This means that parties can quickly and cheaply produce relevant, non-privileged documents. Additionally, counsel could have accomplished this feat with little or no disruption to the daily business practices of UBS. Thus, forensic imaging of relevant storage devices at the onset of litigation serves two important and essential functions: first, it ensures the preservation of relevant ESI despite any attempt by an unethical client to destroy or conceal discoverable ESI; second, when a client or a client’s employees do attempt to delete or con-

101. Id. at 433–34.
102. Id. at 433.
103. Id. at 433–34.
104. Id. at 434.
105. Id. (“By taking possession of, or otherwise safeguarding, all potentially relevant backup tapes, counsel eliminates the possibility that such tapes will be inadvertently recycled.”).
108. To control costs and maximize effectiveness, imaging should be limited to key players’ storage devices unless it is apparent that other employees possess a repository of relevant discoverable information on their computers.
110. See, e.g., Covad Commc’ns. Co. v. Revonet, Inc., 258 F.R.D. 5, 10–11 (D.D.C. 2009) (describing any interference of business operations as “insignificant” because imaging can be done at night or on weekends when employees are out of the office).
 getFile discoverable data that is later requested, the forensically imaged drive will save the client from sanctions and the time and expense it would take to restore the deleted e-mails from backup tapes or forensic reconstruction.

B. Zubulake Revisited: Failure to Image Relevant Digital Storage Devices as Potential Negligence Under Pension Committee

Six years after Judge Scheindlin issued the Zubulake opinions, she applied the well-known tort concepts of negligence, gross negligence, and willfulness in a discovery context to determine each litigant’s relative culpability for failing to follow putatively established discovery rules.111 Once a discovery duty is well established, the failure to adhere to that standard can be considered grossly negligent.112 Since it is now abundantly clear that litigating parties have a duty to preserve all responsive, non-privileged information, a failure to preserve evidence resulting in its loss or destruction is surely negligent and may be grossly negligent.113

The simplicity and straightforwardness embodied in the duty to preserve relevant, non-privileged ESI raises the level of acceptable conduct in the discovery phase of litigation. Pension Committee makes explicit that conduct that may have been acceptable or at least pardonable in the past may no longer pass muster.114 It is equally clear that attorneys need to unequivocally inform all key players of their duties to preserve and to turn over potentially relevant documents to counsel. In complex litigation involving dozens of key players and an exponentially larger number of employees, all of whom may be required to produce relevant ESI, it is impossible for even a team of attorneys to ensure that their preservation orders are being dutifully followed. This does not exculpate the client for discovery abuses, however, nor counsel for failing to monitor execution of the hold as closely as possible.

Under Pension Committee, clients will continue to face stiff sanctions for failing to preserve responsive ESI.115 Framed a different way, Pension Committee demands that attorneys find better prophylactic measures to pre-

112. Id. at 470–73.
113. Id. at 464–65.
114. Since its release, Pension Committee and its requirements for competent e-discovery have been widely cited to justify sanctions for discovery abuses. See, e.g., Merck Eprova AG v. Gnosis, S.P.A., No. 07 Civ. 5898(RJS), 2010 WL 1631519, at *4 (S.D.N.Y. Apr. 20, 2010) (stating that the court agrees with the analytical framework set forth in Pension Committee and will rely on it to determine sanctions in the principal case).
Vent their clients from losing or destroying ESI. For the reasons already stated in part A of this section, forensic imaging is one such measure. Secured possession of timely imaged storage devices greatly reduces the risk of spoliation of relevant ESI and subsequent sanctions. Attorneys should think of forensic imaging as the ultimate discovery compliance and insurance measure.

V. When All Else Fails: Imaging an Opponent’s Digital Storage Devices by Order or Agreement

The obstacles and objections to mirror imaging relevant storage devices are potentially well founded, but ultimately surmountable. When an opposing party fails to adequately preserve relevant ESI, knowledge of these possible pitfalls is necessary for any attorney seeking direct access. Recall that the minor thesis of this note is that in certain circumstances, courts should liberally allow direct access to targeted storage devices for the purpose of forensically imaging and searching those devices. This section will explore and explain the circumstances that often necessitate the need for direct access. The goal is to show that direct access is an appropriate remedy. All of these circumstances could be avoided, or, under Pension Committee, are at least negligent and are therefore inexcusable, if the producing party had adequately preserved and produced available ESI at the outset of litigation. Consequently, the receiving party deserves to access evidence that may be critical to its case, while the culpable party has in effect given up its right to control ESI in its possession.

A. No Automatic Right to Direct Access

The rules governing the discovery of ESI are on equal footing with traditional discovery rules. This means that without a qualifying reason, parties have no automatic right to image their opponent’s hard drives. Typically, parties will request direct access when they believe that the other party has failed to preserve or produce all relevant documents. A party

116. See Field Day, LLC v. Cnty. of Suffolk, No. 04-2202, 2010 WL 1286622, at *13 (E.D.N.Y. Mar. 25, 2010) (denying plaintiff’s motion for sanctions and explaining that the law with respect to litigation holds and the preservation of electronically stored information developed in Pension Committee was not applicable at the time of the conduct in question).


119. See, e.g., Antioch Co. v. Scrappbook Borders, Inc., 210 F.R.D. 645, 651 (D. Minn. 2002) (where plaintiffs sought direct access to defendant’s computers after making a good faith determination that relevant documents were being deleted); Koosharem Corp. v. Spec Pers., LLC, No.
may also seek direct access to simply learn how the information is stored on a given system. Mere skepticism over whether a party has produced all responsive, non-privileged ESI is not enough to gain direct access. If the courts are going to become more generous in granting direct access, attorneys need to aid judges through clear, informative motions. Parties wishing to compel direct access must satisfactorily prove their case with concrete evidence such as sworn expert affidavits, deposition transcripts, and other documents.

B. Petitioning the Court

In order to gain direct access to an opponent’s digital storage devices, counsel must usually petition the court in a motion to compel. Rule 37(a)(3)(B) allows a requesting party to move for disclosure if a party fails to answer a question asked under Rule 30 or 31, fails to make a designation under Rule 30(b)(6), fails to respond to a discovery request, or fails to permit inspection as requested under Rule 34. The timing of a motion to compel is case specific, but a requesting party should have made all reasonable good faith efforts to obtain the requested documents before filing the motion.

To ensure that a motion to compel is successful, a requesting party must be sure to build an adequate record through carefully crafted interrogatories, requests for production, and depositions. Attorneys managing the discovery phase of a lawsuit should act under the assumption that there will...
be a discovery challenge to every aspect of the process. The “Death Star” deposition is one particularly effective means of building such a record.

A Death Star deposition combines Rules 30(b)(2), 30(b)(6), and 34 and forces a corporate designee to bring all requested documents to an oral deposition. At a minimum, requests for production should specifically inquire about an institution’s managerial structure, including the identification of key players; a detailed map of an organization’s information systems—IT infrastructure, system capabilities, and possible locations or sources of stored information—including individual work computers, home computers, e-mail servers, DMS servers, financial systems, backup servers, corporate firewall, networks, external storage drives, PDA devices, and voicemail; an institution’s document retention policy; and steps an organization has taken to preserve relevant ESI after it reasonably anticipated litigation. By combining an oral deposition with a document request, the deposing attorney is able to determine if all relevant documents were produced and inquire about the precise nature of the requested documents under oath.

If the deposing attorney discovers that the producing party has failed to produce a meaningful number of relevant, producible requested documents, and those documents are not timely produced, she now has a thorough record to use in a Rule 37 motion to compel. This motion should clearly articulate the relationship between a party’s claims and the ESI sought. For example, the motion should articulate that a deponent has explained under oath that a series of relevant requested e-mails were exchanged among key players but were not produced after repeated requests. The motion should also request direct access for the purpose of obtaining a forensic image. Attorneys should explain exactly what forensic imaging is and what it can accomplish. This entails providing the judge with the expert’s qualifications and should include an expert affidavit detailing the

127. Achieving Quality, supra note 47, at 313.
128. Kosieradzki, supra note 123.
129. Id.
132. See Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 313 (S.D.N.Y. 2003) (Zubulake I) (“In fact, Zubulake knew that there were additional responsive e-mails that UBS had failed to produce because she herself had produced approximately 450 pages of e-mail correspondence. Clearly, numerous responsive e-mails had been created and deleted . . . .”).
133. Philipp, supra note 122 (“Lawyers should understand how the computer-forensics technique they want to employ fits into the larger picture and what data are required to investigate that avenue fully, and then structure the order for that data using the rules of best evidence and the Federal Rules of Evidence.”).
same. The motion should also specify in detail the exact imaging and search protocol to be used and include steps to prevent inadvertent disclosure.  

C. Third Party Vendors and Costs

The process of forensically examining or searching a digital storage device requires extensive technological expertise and is beyond the ken of all but a handful of attorneys and judges. Attorneys will often need the assistance of a third party vendor to image and search relevant digital storage devices. When selecting a third party vendor, it is best to cooperate with opposing counsel to mutually agree on a specified vendor. If parties cannot agree on a chosen vendor and an adversary challenges the proposed vendor, the selecting party “should expect to support their position with affidavits or other equivalent information from persons with the requisite qualifications and experience, based on sufficient facts or data and using reliable principles or methodology.” Deciding which party will pay for the forensic search is often a point of much contention in any successful motion to gain direct access.

Although it is relatively inexpensive to forensically image a digital storage device, it is very expensive to hire an expert to forensically search or examine the imaged device. Thus, seeking a motion to compel direct access to an opponent’s digital storage devices often triggers proportionality concerns articulated in Zubulake and other cases. Additionally, the 2006 advisory notes to Rule 26 articulate a seven-part test to determine whether cost shifting is appropriate. If the court does not order the producing


135. Equity Analytics, LLC v. Lundin, 248 F.R.D. 331, 333 (D.D.C. 2008); Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 261 n.10 (D. Md. 2008) (explaining that ESI motions often involve complex scientific determinations, which attorneys need to be able to explain through expert affidavits or other means to enable the ruling judge to make a reasonable, informed decision).


137. Here, a “vendor” means a non-party that is hired to provide forensic examination services for the purpose of litigation.

138. Victor Stanley, 250 F.R.D. at 261 n.10 (explaining that ESI motions often involve complex scientific determinations, which attorneys need to be able to explain through expert affidavits or other means to enable the ruling judge to make a reasonable, informed decision).


140. See Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 284 (S.D.N.Y. 2003) (Zubulake III); see also PSEG Power N.Y., Inc. v. Alberici Constructors, Inc., No. 1:05-CV-657 (DNH/RFT), 2007 WL 2687670, at *8 (N.D.N.Y. Sept. 7, 2007) (“In addressing electronic discovery and the rising cost to produce, common law has crafted a cost shifting scheme which is based on Fed. R. Civ. P. 26(c).”).

141. The seven part test articulated in the 2006 advisory notes is as follows: (1) the specificity of the discovery request, (2) the quantity of the information available from other more easily
party to pay for the forensic search, requesting parties should be willing to pay for all or part of the costs associated with hiring a forensic expert to increase their odds of a successful motion to compel. In most instances where the requesting party is ordered to pay all or part of the costs for production, the litigating parties agree that forensic analysis is essential to proper discovery, but the producing party has not intentionally or negligently destroyed any responsive ESI.

Parties who are ordered or agree to produce digital storage devices for forensic imaging often seek protection from the court to avoid waiver of attorney-client privilege, work product doctrine, and the production of trade secrets or non-responsive ESI. Fear of waiver is particularly fierce where producing parties are required to submit their digital storage devices to a non-party forensic examiner. However, in what has been described as a "seminal" case on protecting a producing party from inadvertent waiver and disclosure in the e-discovery context, Hopson v. Mayor & City Council of Baltimore provides a judicially imposed safety mechanism to ensure that the rights and privileges of the producing party are adequately maintained.

accessed sources, (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources, (4) the likelihood of finding relevant, responsive information that cannot be obtained from other more easily accessed sources, (5) predictions as to the importance of and usefulness of further information, (6) the importance of issues at stake in litigation, and (7) the parties' resources.

142. Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524-DJS, 2006 WL 3825291, at *5 (E.D. Mo. Dec. 27, 2006) (“In performing good-cause inquiry, the Court is also permitted to set conditions for discovery, including but not limited to payment by the requesting party of part or all of the reasonable costs . . . .”).

143. See Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 n.6 (D. Minn. 2002) (stating that the court is not required to consider cost-shifting measures where the requesting party offers to pay all costs associated with forensically searching an opponent’s hard drive).

144. See, e.g., Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (granting plaintiff’s request for direct access, but ordering that the plaintiff is required to pay for the forensic analysis due to Rule 26(b)(2)(B)’s undue burden/cost limitation); Equity Analytics, LLC v. Lundin, 248 F.R.D. 331, 334 (D.D.C. 2008) (where, in the interest of prompt resolution to a discovery dispute involving plaintiff’s request to forensically image defendant’s hard drive, the ruling judge stated, “My order will also provide that the cost of the examination will be borne by [plaintiff] and that it may not seek to recover that cost from [defendant] at any time or for any purpose.”).

145. See supra notes 16–19 and accompanying text.

146. Equity Analytics, 248 F.R.D. at 334.

147. 232 F.R.D. 228, 239–40 (D. Md. 2005). Given the importance of the Hopson’s judicially imposed safety valve, it is necessary to quote part of the opinion in length: “Despite the uncertainty regarding which approach to inadvertent disclosure of attorney-client privileged material would be adopted by the Fourth Circuit, there is a viable method of dealing with the practical challenges to privilege review of electronically stored information without running an unacceptable risk of subject-matter waiver. It lies with the courts issuing scheduling orders under Fed.R.Civ.P. 16, protective orders under Fed.R.Civ.P. 26(c), or discovery management orders under Fed.R.Civ.P. 26(b)(2) that incorporate procedures under which electronic records will be produced without waiving privilege or work product that the courts have determined to be reason-
Further, judges are able to appoint third party vendors as officers of the court, which obliges the forensic experts to abide by the same rules and procedures as an attorney. This exposes the forensic examiner to the possibility of tremendous sanctions or liability should she violate any court rules or provisions of the court order.

VI. Conclusion

Discovery failures involving ESI are on the rise, and the redundancy of cases in which a party or a party’s employees have failed to preserve or produce relevant ESI reveals that an unacceptable number of civil litigants and litigators still suffer from a poor appreciation of their court-mandated duties. Cost-conscious clients and overworked judges are demanding that attorneys develop novel approaches to solve litigation problems. Competent and ethical representation now requires that attorneys adapt to the significant challenges brought about by the inexorable growth of ESI. Forensic imaging at or prior to the onset of litigation can solve many of the discovery related abuses that unnecessarily waste the court’s time, prevent the merit-based adjudication of issues, and wantonly increase a client’s costs. Further, judges should liberally allow forensic imaging where a party fails to live up to its discovery duties. These proposals serve to protect client and attorney alike, while acknowledging that the status quo is no longer tenable.

able given the nature of the case, and that have been agreed to by the parties. This practice, already commonly followed in cases where discovery of electronic records is anticipated, is specifically encouraged by the proposed rule changes to the discovery rules now under review by the Supreme Court.”

In 2006, the Supreme Court adopted the proposed amendments to the Federal Rules. Among the new changes was Fed. R. Civ. P. 26(b)(3)(B), which states: “If the court orders discovery of those materials, it must protect against the disclosure of the mental impressions, conclusions, opinions, or legal theories of a party’s attorney or other representative concerning litigation.” See also Sharon Nelson & John Simek, New Federal Rules of Evidence: An ESI Primer, 32 LAW PRAC. 23, 23 (2006).

148. “A person who is charged with upholding the law and administering the judicial system. Typically, officer of the court refers to a judge, clerk, bailiff, sheriff, or the like, but the term also applies to a lawyer, who is obliged to obey court rules and who owes a duty of candor to the court.” BLACK’S LAW DICTIONARY (9th ed. 2009).

149. See, e.g., Ferron v. Search Cactus, L.L.C., No. 2:06-CV-327, 2008 WL 1902499, at *4 (S.D. Ohio Apr. 28, 2008) (“[T]he two identified computer forensic experts shall serve as officers of this court.”); Playboy Enters., Inc., 60 F. Supp. 2d at 1054 (“Any outside expert retained to produce the ‘mirror image’ will sign a protective order and will be acting as an Officer of the Court pursuant to this Order.”).

150. Achieving Quality, supra note 47, at 302.