CONSIDERATIONS REGARDING THE DISCOVERY AND PRODUCTION OF ELECTRONICALLY STORED INFORMATION

Shannan F. Oliver

Electronically stored information ("ESI") is a broad term which escapes the constraints of any one definition. While many equate the term exclusively with e-mail correspondence, ESI includes limitless sources of information including hard drives, magnetic tapes, digital tapes, Web site materials, microfilm, portable drives, voice mail messages, and backup tapes. In a formal legal context, the Uniform Rules Relating to the Discovery of Electronically Stored Information defines ESI as "information stored in an electronic medium and . . . retrievable in perceivable form."[1] In practice, ESI effectively encompasses all recognizable types of computer-based information, along with all future iterations and developments.[2]

Considering this broad scope, practitioners must be cognizant of the rules and pitfalls "uniquely associated with electronic materials when planning and managing litigation."[3] For a basic understanding of these issues, many turn to the seminal case involving ESI, Zubulake v. UBS Warburg LLC, in which Judge Scheindlin divided ESI, for discovery purposes, into two broad categories.[4] The first category of ESI is "data kept in an accessible format," such as that typically found on hard drives, optical disks, and offline storage mechanisms and archives.[5] The second category is electronic data that is are "relatively inaccessible," such as backup tapes and erased, fragmented, or

[1] National Conference of Commissioners on Uniform State Laws, *Uniform Rules Relating to Discovery of Electronically Stored Information* (2007).
[2] Grenig, Stippach, Twigger & Marean, Electronically stored information, Electronic Discovery and Records and Information Management Guide § 1:2 (2015).
[3] Daniel R. Murray, *Taking a Byte Out of Discovery: How the Properties of Electronically Stores Information Have Shaped E-Discovery*, 41 No. 1 UCC L. J. ART 2 (2008).
[4] Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).
[5] Id. at 318.

damaged data.[6] According to the New York court, "the usual rules of discovery apply [to data kept in an accessible format, and] the responding party should pay the costs of producing responsive data."[7] However, for the second category, the court considers a number of factors to determine whether the requesting party should bear the costs of production.[8] Other courts increasingly rely on Zubulake as a guide for determining cost allocation during discovery.

In 2006, not long after Zubulake, the Federal Rules of Civil Procedure were amended.[9] These amendments were drafted in order to address the "myriad issues associated with the discovery and production of [ESI]."[10] While the prior version of Rule 34 extended only to the production and inspection of "documents," it is clear that ESI is now fully encompassed by the Federal Rules of Civil Procedure.[11] Like Zubulake, the Federal Rules divide ESI into two classes based upon the ease of access and burden to produce.[12] "Reasonably accessible" ESI should be produced so long as it is relevant and not privileged.[13] That which is "not reasonably accessible because of undue burden or cost" is not typically produced.[14] However, counsel must still "identify, by category or type, the sources" containing such ESI with "enough detail to enable the requesting party to evaluate the burden and costs of providing the discovery and the likelihood of

---

[6] Id. at 324.
[7] Id.
[8] Zubulake, 217 F.R.D. at 324.
[9] Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 7 (2006).
[10] Id.
[11] FED. R. CIV. P. 34(a).
[12] FED. R. CIV. P. 26(b)(2)(B).
[13] FED. R. CIV. P. 26 advisory committee's note. By way of example, the Committee considered the following as "reasonably accessible" ESI: "electronically stored information form active computer servers, files on regularly accessed shared network drives, computer data saved to the hard drives of individual computers, and e-mails stored in currently accessible folders or mailboxes." Id.
[14] Id. This category of ESI includes "archival materials, backup tapes, or other materials in a system that may retain information on sources that are accessible only by incurring substantial burdens or costs." Id.

finding responsive information on the identified sources."[15] The producing party also bears the usual "statutory and common-law duties" to preserve it.[16] Moreover, the court may order that this material be produced upon a showing of good cause.[17] With these amendments now firmly implanted a decade after their enactment, it is imperative that the prudent practitioner become familiar with the preparation, coordination, and submission of ESI.

A. DUTY TO PRODUCE AND PRESERVE ESI

Not surprisingly, the massive volume of potentially discoverable electronically stored information lends great importance to both the duty to produce discoverable information and, relatedly, the duty to preserve such information prior to its actual production. The duty to produce documents or other evidence results in response to valid discovery requests from opposing counsel.[18] In the context of electronically stored information, Federal Rule of Civil Procedure 34 specifically grants a party the power to inspect, copy, test, or sample "any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, imagines, and other data or data compilations—stored in any medium from which information can be obtained either directly . . . or after translation.[19] However, this power is not absolute; it is limited by the "proportionality" requirement of Federal Rule of Civil Procedure 26(b)(2)(C).[20] Such limitation states that a "party need not provide discovery of electronically stored information from sources that the party

---

[15] Id.
[16] Id.
[17] FED. R. CIV. P. 26(b)(2)(B).
[18] Infinite Energy, Inc. v. Chang, No. 1:07-cv-23, 2008 LEXIS 88084, at *5 (N.D. Fla. Aug. 29, 2008) (stating that the producing party "must respond to each discovery request served in this case and identify each responsive document.").
[19] FED. R. CIV. P. 34.
[20] FED. R. CIV. P. 34(A)(1)(A).

identifies as not reasonably accessible because of undue burden or cost."[21] This protection is not absolute, as the requesting party may seek to compel disclosure of such electronically stored information and, upon a showing of good cause, a court may nonetheless order its production.[22] Of course, a court may limit or otherwise condition the production of electronically stored information,[23] but at least one court has held that courts should apply these limitations in a narrow manner.[24]

Although derived from common law, the duty to preserve evidence which may be discoverable exists in conjunction with the duty to produce.[25] Thus, the competent practitioner must understand and be able to determine the precise moment when such duty to preserve arises—which is "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] From this, practitioners may infer that the duty to preserve documents or other electronically stored information clearly begins once a lawsuit is commenced, but may exist long before the first pleading is filed.[27]

Thankfully, courts have provided guidance as to when the duty to preserve arises. The factors employed by courts to resolve a conflict regarding whether a duty to preserve exists or did exist at a particular time are (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,

---

[21] FED. R. CIV. P. 26(b)(2)(B).
[22] FED. R. CIV. P. 26(b)(2)(B).
[23] FED. R. CIV. P. 26(b)(2)(C).
[24] Mohmeyer v. Wal-Mart Stores East, L.P., No. 09-69-WOB, 2009 WL 4166996, at *3 (E.D. Ky. Nov. 20, 2009) ("A narrow reading . . . is strongly suggested by Rule 37(e).").
[25] FED. R. CIV. P. 37(f) advisory committee's note ("A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case.").
[26] Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001).
[27] Franz. J. Vancura, *Using Computer Forensics to Enhance the Discovery of Electronically Stored Information*, 7 U. ST. THOMAS L.J. 727 (2010).

(4) the closeness of the connection between the 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.[28] In applying these factors, courts appear particularly attentive to the disposition of the litigant(s) and the probability of litigation in order to determine whether the duty to preserve applies.[29]

Following the determination of *when* the duty to produce arises, the next relevant inquiry is ascertaining *what* must be preserved. This second inquest is particularly important in light of the potentially massive scope of electronically stored information in any particular lawsuit. To answer this question, courts turn to the general discovery rules which, in part, entitle parties to discovery of "any non-privileged matter that is relevant to any party's claim or defense."[30] Thus, parties are obligated to preserve all relevant documents in existence at the time the duty to preserve arises and must produce those documents when requested.[31] Parties also have a continuing duty to supplement their document disclosures throughout the discovery process.[32]

B. DEFENSIBLE LEGAL HOLDS

A best practice to engage in when a party reasonably anticipates litigation is to "suspend [any] routine [document] retention policy and implement a litigation hold."[33] The intended effect of such litigation hold is to prohibit the destruction or alteration of documents which may be relevant to pending or anticipated litigation. While a litigation

---

[28] Franz. J. Vancura, *Using Computer Forensics to Enhance the Discovery of Electronically Stored Information*, 7 U. ST. THOMAS L.J. 727 (2010); see also Velasco v. Commercial Bldg. Maint. Co., 169 Cal. App. 3d 874, 877-78 (1985).
[29] Id.
[30] FED. R. CIV. P. 26(b)(1).
[31] Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 433 (S.D.N.Y. 2004)("[T]he notion of a 'duty to preserve' connotes an ongoing obligation.").
[32] Id.
[33] In re Grand Jury Subpoena, 274 F.3d 563, 576 (1st Cir. 2001).

hold may not completely insulate a client from a spoliation finding, many courts consider their issuance as a mitigating factor in such circumstances.[34]

While there is no precise form for a litigation hold letter, it should contain a notice to the client that litigation is underway or reasonably anticipated. In the latter, the letter should generally describe the expected matter and claims as to assist the client in identifying which employees or other custodians may possess relevant information. An adequate litigation hold letter should also identify probable sources of relevant information (e-mails, text messages, etc.) and their potential locations (servers, laptop computers, etc.).[35]

C. METADATA EXPLAINED

Because of the nature of electronic discovery, practitioners must be alert to the additional information that lurks behind the data—metadata.

1. Defining Different Types and Formats

Metadata is often described as "data about data."[36] The term refers to "hidden data that usually can only be seen when a digital document is viewed in its native format using the program that originally produced the document."[37] For example, when a user creates, opens, or saves a document in Microsoft Word, the specific file accessed does not just create the text generated by the user, but actually a spectrum of "metadata" including the user's name, company name, computer name, the name of the network or hard drive where the document is saved, the names of previous authors, document

[34] See Chin v. Port Auth. of New York & New Jersey, 685 F.3d 135, 162 (2d Cir. 2012) (holding that lack of litigation hold notice is not gross negligence *per se*, but is considered in imposing spoliation sanctions).
[35] Sonny S. Hayes, *Best Practices: Litigation Holds and Resolving Spoliation Motions*, 57 No. 4 DRI for Def. 30 (2015).
[36] J. Brian Beckham, *Production, Preservation, and Disclosure of Metadata*, 7 COLUM. SCI. & TECH. L. Rev. 1, 7 (2006).
[37] American Law Reports, *Discoverability of Metadata*, 29 A.L.R. 6th 167 (2007).

revisions, document versions, hidden text, and comments, just to name a few.[38] Similarly, the same types of metadata are created when e-mail messages are sent or received, as well as the specific version of a document attached to an e-mail message.[39] Thus, metadata and the information conveyed by it can serve a limitless number of functions in litigation, including determining if and when information was produced, settling billing disputes, and improving the efficiency of document searches.[40]

Metadata is normally categorized into two groups: (1) "system metadata," which is "automatically created by the software program" without any input from the user, and (2) metadata that "is created by the software because the [user] is purposefully using certain features."[41] The first category, system metadata, typically includes the user's name, the "location on the [user's] system where the document is saved, the date and time when the [item] was originally created and the dates and times reflecting when the document was last modified or accessed."[42] System metadata also includes the size of the document and the amount of time a user spent in the document or program, all of which is accessible to the user.[43] The second category of metadata includes ancillary items such as embedded comments created by the author in word processing software or the use of the "track changes" feature to log revisions and other comments.[44]

---

[38] David Hricik, *The Transmission and Receipt of Invisible Confidential Information*, http:// www.hricik.com/eethics/Metadata1103.doc (2003).
[39] Scott Nagel, *Embedded Information in Electronic Documents: Why Metadata Matters* (July, 2004), http:// www.abanet.org/lpm/lpt/articles/ftr07044.html.
[40] Beckham, *supra* n. 36.
[41] Douglas R. Richmond, Metadata, 33. E. MIN. L. FOUND. § 5.03 (2012).
[42] Id.
[43] Id.
[44] Id.

2. Metadata Landmines to Avoid

Metadata is created, stored, and transmitted each time a user implements software, creates a document, or sends an email. Depending on the nature of the metadata and its intended recipient, such metadata may contain or reveal information which the sender did not intend to reveal to the initial recipient or other who may come into possession of the file. With these potential issues in mind, practitioners must educate themselves on both practical and ethical pitfalls which may be encountered.

From a professional responsibility perspective, the most pressing question is whether a lawyer who receives an electronic document may ethically "mine" or review the metadata contained by that document in order to glean whatever information may be available. Perhaps not surprisingly, ethics committees and other writers are divided on the issue. Many authorities, such as the ABA's Standing Committee on Ethics and Professional Responsibility, believe that such mining is ethically permissible because there is currently no explicit prohibition on such actions and further because a lawyer is "ethically required to thoroughly review any documents produced by opposing counsel."[45] To those holding such position, the "primary determination that appears to drive [their] analysis is whether receiving lawyers can routinely treat the transmission of an electronic document with metadata intact as being inadvertent."[46]

On the other hand, entities such as the New York State Bar Association's Committee on Professional Ethics have opined that analyzing metadata is unethical and analogous to a "less technologically sophisticated means of invading the attorney-client relationship."[47] In such jurisdictions, mining metadata has been found to violate

[45] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006).
[46] Douglas R. Richmond, *Metadata*, 33. E. MIN. L. FOUND. § 5.03 (2012).
[47] NY Eth. Op. 749, 2001 WL 1890308, at *2.

existing ethical rules prohibiting conduct involving dishonesty, deceit, fraud, or misrepresentation, and further amounted to conduct prejudicial to the administration of justice.[48]

3. "Scrubbing" Metadata

There is little dispute that metadata is "an ever-present threat to the practice of law and heavily impacts an attorney's ethical obligations."[49] In fact, some observers conclude that given the undeveloped law regarding metadata, the issue of protecting it "is likely to continue to plague unwary practitioners and inflate the cost of transaction and litigation representation."[50] In fact, one of the "top malpractice threats that attorneys are advised to avoid are technological issues applicable to metadata."[51] To that end, many believe that an obligation should be imposed on lawyers "to remove confidential information from electronic data [to] prohibit [others] from mining such [metadata]" rather than engaging in a "high-tech free-for-all."[52] This metadata removal process is popularly known as "scrubbing."

The act of scrubbing is carried out using software classified as "metadata scrubbers." Such software and programs are extremely effective and remove the most important components of metadata.[53] Legal consulting companies claim that their offered software has the "ability to identify and eliminate some of the more harmful

---

[48] Id.
[49] Crystal Thorpe, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata*, 84 N.D.L. REV. 257, 281 (2008).
[50] Shari Claire Lewis, *Reckoning With Metadata*, N.Y. L.J., Dec. 19, 2005, available at http://www.law.com/jsp/law/sfb/lawArticleFriendlySFB.jsp? id=1134727515889.
[51] Crystal Thorpe, *Metadata: The Dangers of Metadata Compel Issuing Ethical Duties to "Scrub" and Prohibit the "Mining" of Metadata*, 84 N.D.L. REV. 257, 284 (2008).
[52] John Levin, *Legal Ethics: What to Do With Metadata*, 21 CBA REC. 68, 68 (June/July 2007).
[53] Adam K. Israel, *To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery*, 60 ALA. L. REV. 469 (2009).

forms of metadata from documents."[54] Such software functions by prompting the user to "scrub" or remove "all or part of the metadata contained within a document before it is transmitted electronically, minimizing the problem of overlooking the existence of metadata." Thankfully, particularly to the practitioner, metadata scrubbers are relatively inexpensive and can cost less than $100 per year, depending on the number of users and subscriptions necessary.[55] While metadata scrubbers may be flawed in some instances, when used in conjunction with the functions provided by modern word processing programs, they are generally a wise investment in order to "minimize the potential consequences posed by inadvertent disclosure of metadata containing confidential client information."[56]

D. USING APPLICATIONS AND SOFTWARE TO OBTAIN ESI

With so much information available from sources such as cell phones, computers, flash drives and other mediums, how should a party collect it? There are two primary methods. A logical acquisition is a simple process which literally results in a copy of the file.[57] Although it "preserves the integrity of the files, it "does not copy the attributes of the physical device."[58] On the other extreme, a physical collection results in a true "forensic copy of the physical state of the storage memory of [a] device."[59] This method captures not just a copy of the file, but it also extracts individual data from it. This

---

[54] Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 COLO. LAW., Oct. 2004, at 53.
[55] Israel, *supra* n. 53.
[56] Id.
[57] Michael Arnold, *Collecting Data from Mobile Devices*, American Bar Association Litigation News (2012).
[58] Id.
[59] Id.

second, more complicated method is typically required to capture emails and most application data.[60]

E. PREDICTIVE CODING DO'S AND DON'TS

Given the volume of potential sources of electronic information, searching through it for responsiveness and relevance can be overwhelming. In that regard, "predictive coding" is a method of computer assisted document review which some have designated as the most significant development in e-discovery in recent years. Predictive coding is a "machine learning process" which involves processes performed by both humans and computer systems in order to identify potentially responsive documents.[61] This process, which is far more advanced than a simple keyword search, is generally described as follows.[62] First, an attorney manually reviews a small sample of documents from a pre-production document set to create a "seed set" encompassing documents designated relevant, not relevant, privileged, or not privileged.[63] Next, software implements the seed set to create an algorithm which ranks and codes the remaining documents based upon the attorney's initial manual review.[64] This process is repeated until the software is capable of designating documents with a certain degree of accuracy.[65]

Predictive coding is viewed with great excitement considering its potential for altering the discovery landscape and reducing costs. It is no secret that in-house counsel and law firms alike are under pressure from their clients to curtail e-discovery

[60] Id.
[61] Charles Vaccaro, *Look Before You Leap into Predictive Coding: An Argument for A Cautious Approach to Utilizing Predictive Coding*, 41 RUTGERS COMPUTER & TECH. L.J. 298, 335 (2015).
[62] Nicholas Barry, *Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and A Computer-Utilizing Predictive-Coding Technology*, 15 VAND. J. ENT. & TECH. L. 343, 354 (2013).
[63] Matthew Nelson, *Shining a Light into the Black Box of E-discovery Predictive Coding*, Corporate Counsel (May 29, 2012), http:// www.corpcounsel.com/id=1202556081861.
[64] Id.
[65] Id.

costs. In many cases, law firms are "held accountable for some of these cost pressures so they [feel] the need to analyze discovery early on to identify issues, project costs, and determine appropriate strategies before they undertake a costly review cycle."[66] Many believe that the utilization of predictive coding could alleviate these cost pressures, and even reduce the cost of e-discovery, by significantly streamlining the document review and production process.[67] Even further, the speed and accuracy at which predictive coding operates may provide litigants with an increased awareness of the documents supporting their own case and a more accurate assessment of the claims asserted therein.[68] Some observers opine that the potential benefits of predictive coding may lead to the adoption of technology-driven processes like predictive coding as the "gold standard" of discovery review in favor of manual document review.[69] Others go as far as predicting that courts will accept predictive coding as a "reasonable" under the Federal Rules of Civil Procedure.[70]

However, in its current form, predictive coding brings with it a number of risks. For example, the complexity of the software used by predictive coding "increases the risk of missing important relevant documents or inadvertently producing privileged documents."[71] The occurrence of human error at the "top level" data sampling and attorney review could lead to "a trickle-down effect that compounds downstream

---

[66] Rich Turner & Cathy Story, *Controlling Discovery Costs: Early Case Assessment Manages Litigation Costs*, Content Analyst 1 (2009), available at http://www.contentanalyst.com/images/images/whitepaper_early_case_assessment_controls_eDiscovery_costs.pdf.
[67] Jason R. Baron, *Law in the Age of Exabytes: Some Further Thoughts on "Information Inflation" and Current Issues in E-Discovery Search*, 17 RICH. J.L. & TECH. 9, P 33 (2011).
[68] Id.
[69] Nicholas Barry, Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and A Computer-Utilizing Predictive-Coding Technology, 15 VAND. J. ENT. & TECH. L. 343, 364 (2013).
[70] Id.
[71] Nelson, *supra* n.63.

document productions."[72] Another risk entails establishing a seed set with erroneous or otherwise flawed documents, which will further multiply predictive errors. Despite these risks, studies claim that predictive coding is more accurate than manual attorney review.[73]

F. SPOLIATION PITFALLS

One of the risks associated with electronic information is its destruction, even in the normal course of business, which brings with it the dreaded accusation of spoliation. Spoliation is the "concealment, destruction or significant alteration of evidence, or the failure to preserve property for another's use . . . in pending or reasonably foreseeable litigation."[74] This concept is the counterpart to the "fundamental duty to preserve relevant evidence over which [an] entity [has] control and reasonably knew or could reasonably foresee was material to a potential legal action."[75] Spoliation and related considerations are of utmost importance in modern litigation due to the vast volume of electronically stored information created in modern computer systems and the nature of the electronic storage systems in which such information is maintained. This apparent paradox poses challenges in civil discovery and requires practitioners to obtain, at a minimum, a general understanding of how ESI is created, managed, and stored. Complicating such understanding, however, are inherent characteristics of ESI—such as automatic deletion or modification due to storage constraints— and the ever-evolving nature of modern computer technology. Although safeguards are sometimes

[72] Id.
[73] Joseph H. Looby, E-Discovery - Taking Predictive Coding Out of the Black Box, FTI JOURNAL (Nov. 2012), available at http:// ftijournal.com/article/taking-predictive-coding-out-of-the-black-box-deleted.
[74] West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999).
[75] China Ocean Shipping Co. v. Simone Metals, Inc., No. 97 C2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999).

implemented to alleviate these issues, the prudent practitioner must nonetheless take great lengths to ensure compliance with their discovery obligations regarding ESI.

Federal Rule of Procedure 37(e) is of the utmost importance when analyzing potential spoliation issues. In relevant part, this rule provides that "[a]bsent exceptional circumstances, a court may not impose sanctions . . . on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[76] Therefore, under this rule, "spoliation sanctions are precluded so long as the [party] acted in good faith and the information was lost a result of the routine operation of a storage system."[77] With "good faith generally understood to be the absence of bad faith," it is important to examine conduct which has proved problematic in the spoliation context in order to determine which mistakes to avoid.

Perhaps the most egregious example of sanctionable conduct was outlined in Kucala Enterprises v. Auto Wax Co..[78] In that case, the defendant received a letter from the plaintiff discussing pending litigation between the parties.[79] Thereafter, the defendant obtained a program called "Evidence Eliminator," which was a form of "data destruction technology" functioning to "delete . . . deadly evidence . . . embedded in the computer's memory."[80] In response to implementing this software, the court sanctioned the defendant for "willfully and with the purpose of destroying discovery by purchasing and then using Evidence Eliminator on his computer."[81] Similarly, in Pennar Software

[76] FED. R. CIV. P. 37(e).
[77] FED. R. CIV. P. 37(e). See also Andrew Hebl, *Spoliation of Electronically Stored Information, Good Faith, and Rule 37(e)*, 29 N. ILL. U.L. REV. 79, 96 (2008).
[78] Kucala Enterprises v. Auto Wax Co., 56 Fed. R. Serv. 3d 487 (N.D. Ill. 2003).
[79] Id. at 487.
[80] Id. at 489.
[81] Id.

Corp. v. Fortune 500 Systems, Ltd., the Northern District of California sanctioned a defendant for its bad faith conduct in "manufacturing the [web page], delet[ing] the page from its web server, delet[ing] another relevant page two days later, and finally alter[ing] the server's log files in an attempt to cover its tracks."[82] Thus, not only should a party avoid software which intentionally deletes data in light of pending or foreseeable litigation, it should take action to avoid even the appearance of bad faith.

G. SANCTIONS AND PROPORTIONALITY

By now, it is well-established that parties in litigation have a duty to preserve evidence "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."[83] Spoliation occurs when a party breaches this duty to preserve relevant evidence.[84] Where spoliation occurs, courts are vested with the authority to impose a wide array of sanctions in order to punish the offending party.[85] Such sanctions range from the dismissal of the action, an adverse inference jury instruction, monetary fines, or an award of attorneys' fees.[86] In practice, however, the application of the sanctioning power of trial courts is regulated by proportionality considerations. In other words, "an award of sanctions must be proportionate to the circumstances surrounding the failure to comply with discovery."[87] These sanctions can be divided into two basic categories—evidentiary and punitive.

---

[82] Pennar Software Corp. v. Fortune 500 Sys., Ltd., 51 Fed. R. Serv. 3d 279, 286 (N.D. Cal. 2001).
[83] Kronisch v. United States, 150 F. 3d 112, 126 (2d Cir. 1998).
[84] Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 4656 (S.D.N.Y. 2010) ("Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.")
[85] Daimler Chrysler Motors v. Bill Davis Racine, Inc., No. 03-72265, 2005 WL 3502172, at *3 (E.D. Mich. Dec. 22, 2005) (sanctioning spoliating party with adverse instruction based on negligent destruction of emails following filing of complaint.).
[86] Id.
[87] Landley v. Union Elec. Co., 107 F.3d 510, 515 (7th Cir. 1997).

Evidentiary sanctions are "predominantly compensatory and allow[] courts to 'level the playing field' when one party destroys evidence that circumstances suggest would aid the non-spoliating party's case."[88] Evidentiary sanctions include certain jury instructions or an inference that allows a jury to form conclusions it might have made had the spoliating party preserved and produced the evidence at issue. On the other hand, punitive sanctions are intended to punish past conduct and deter future occurrences. These punitive sanctions range in form from a default judgment, dismissal with prejudice, to other monetary penalties.[89] In the event that a court finds that sanctions are warranted, whether evidentiary or punitive, due process considerations typically require a hearing on the merits of the spoliation issue.[90]

The availability of these sanctions, perhaps to the chagrin of requesting parties, is nonetheless limited by proportionality considerations in electronic discovery. Proportionality, in the context of electronic discovery, is set forth in Federal Rule of Procedure Rule 26(b)(2)(B), which states that 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."[91] This so-called "proportionality test" contained within Rule 26 has been applied to "limit discovery if it [is] determined the burden of the discovery outweigh[s] its benefit."[92] In interpreting the limitations imposed by it, the Sedona Conference on Electronic Discovery opined that Rule 26(b)(2)(C) provides a court with "flexibility and discretion to ensure that the scope and duration of discovery is reasonably proportional to the value of the requested

---

[88] Daniel Renwick Hodgman, *A Port in the Storm?: The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U.L. REV. 259 (2007).
[89] Id.
[90] Hodgman, *supra* n. 88.
[91] FED. R. CIV. P. 26(b)(2)(B).
[92] Tamburo v. Dworkin, No. 04-C-3317, 2010 WL 4867346, at *3 (N.D. Ill. Nov. 17, 2010).

information, the needs of the case, and the parties' resources."[93] While the Sedona Conference recognized that courts have not always correctly applied this proportionality rule, it emphasized that "in the electronic era, it has become increasing important for courts *and* parties to apply the proportionality doctrine to manage the large volume of ESI and associated expenses now typical in litigation."[94] Other observers, in supporting this principle, have asserted that "the greatest value of proportionality is that it creates a mindset in the court and litigants that discovery needs to be focused on the real issues in the case and that cost is a consideration."[95] Thus, the prudent practitioner should become well-versed in the concept of proportionality in order to protect clients from considerable effort and expense.

H. RULE 502 and CLAWBACK PROVISIONS

With so much information to review, the costs of a thorough review can become unmanageable. Absent a thorough review, however, an inadvertent disclosure of privileged or confidential information becomes more likely. Fortunately, some procedures and practices can alleviate this concern.

The Federal Rules of Civil Procedure grant strong privilege protection and waiver avoidance to parties who are able to follow their guidance and also agree upon a sufficiently drafted protective order. To this end, Federal Rule of Evidence 502 provides, in relevant part, that a federal court "may order that the [attorney-client privilege and work product protection] is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in

[93] The Sedona Conference Commentary of Proportionality in Electronic Discovery, 11 SEDONA CONF. J. 289 (2010).
[94] Id.
[95] John L. Carrol, *Proportionality in Discovery: A Cautionary Tale*, 32 CAMPBELL. L. REV. 455, 460 (2010).

any other federal or state proceeding."[96] Such an order, known as a "Rule 502(d) order," confers a number of benefits upon litigants and establishes a bright line for those parties who invoke its protections.[97]

Rule 502 promotes cost savings "by dictating that a protective order can eliminate disclosure-based privilege waiver, thereby making feasible lower-cost privilege review."[98] Further, a court may provide "for the return of privileged documents irrespective of the care taken by the disclosing party."[99] Because Rule 502 orders "confer these protections *within* the proceeding . . . as well as beyond the given proceeding," the parties enjoy the benefit of reduced cost and time necessary to complete discovery by allowing them to reduce or forego privilege review.[100] Therefore, a Rule 502 order will minimize the damage created by the inadvertent disclosure of privileged information. A Rule 502 order will also eliminate the possibility of many worst-case scenarios, such as the opposing party gaining leverage in settlement negotiations upon learning information through accidental disclosure of a privileged document.[101]

Practitioners can further protect their clients by negotiating a clawback agreement. Such agreements are part of an increasing trend for parties to "forgo privilege review altogether in favor of an agreement to return inadvertently produced privileged documents."[102] This trend is the function of cost-saving efforts and a growing

---

[96] FED. R. EVID. 502(d).
[97] Edwin M. Buffmire, *The (Unappreciated) Multidimensional Benefits of Rule 502(d): Why and How Litigants Should Better Utilize the New Federal Rule of Evidence*, 79 TENN. L. REV. 141 (2011).
[98] Buffmire, *supra* n. 97.
[99] Id.
[100] Radian Asset Assurance, Inc. v. Coll. of the Christian Bros. of N.M., No. 09-0885, 2010 WL 4928866 (D.N.M. Oct. 22, 2010) (ordering production of documents without review because party was protected by Rule 502(d)).
[101] Buffmire *supra* n. 97.
[102] Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003).

recognition that inadvertent disclosure of privileged documents and its resultant consequences had been transformed into a "specter that haunts every document intensive case."[103] A typical clawback agreement contains language to the effect that the "production of any of the documents presently in dispute shall not constitute a waiver of any privilege."[104] Clawback agreements are construed pursuant to general contract law and as such, parties are able to mold their basic terms to specify details such as which type of privilege is covered, how much time a party has to claim a privilege, and the procedures employed when a party does so.[105]

I. WORKING WITH AND SUBPOENAING SOCIAL MEDIA COMPANIES

Among the many sources of electronic discovery is the world of social media. In recent years, social media has provided a playground for litigators. Unsuspecting litigants and witnesses share private details of their lives on various social media platforms, from Facebook to Twitter to Snapchat. There are evidentiary and ethical considerations for a practitioner who hopes to tap into this source of information.

1. Subpoena Power

It may not surprise the reader to learn that social media companies resist third-party subpoenas aimed at obtaining user account contents. The reasons for such opposition vary, but conceivably include precluding the investment of substantial resources in responding to potentially endless discovery requests and the potential for privacy concerns or other questions arising from the user base. Some social media companies appear to have adopted an unofficial policy of noncooperation regarding third-party subpoenas. Others, like Facebook, publicly assert that federal law does not

[103] FDIC v. Marine Midland Realty Credit Corp., 138 F.R.D. 479, 479-80 (E.D. Va. 1991).
[104] Navajo Nation v. Peabody Holding CO., 209 F. Supp. 2d 269, 281 (D.D.C. 2002).
[105] Jessica Wang, *Nonwaiver Agreements After Federal Rule of Evidence 502: A Glance at Quick-Peek and Clawback Agreements*, 56 UCLA L. Rev. 1835, 1842–43 (2009).

allow private parties to use subpoenas in order to acquire user account contents. These companies rely upon the Stored Communication Act (the "SCA") for support of their position.[106]

The SCA, passed by Congress in 1986, prohibits a person or entity providing an "electronic communication service" to the public from, among other things, knowingly divulging "to any person or entity the contents of a communication while in electronic storage by that service."[107] The SCA further prohibits a provider of a "remote computing service or electronic communication service" from knowingly divulging "a record or other information pertaining to a subscriber to or customer of such service."[108] Thus, the SCA "creates a set of Fourth Amendment-like privacy protections by statute, regulating . . . service providers in possession of users' private information."[109] Despite the fact that it was enacted long before the advent of social media, the SCA now finds itself squarely at the center of the battlefield between social media companies and litigants who seek to obtain information from them. The ongoing battle is demonstrated by the following case.

In Crispin v. Christian Audigier, Inc., *et al.*, plaintiff filed suit against various licensees and sublicensees for breach of contract, copyright infringement, and other claims related to their use of his artistic works.[110] During discovery, defendants served subpoenas upon Facebook and MySpace aimed at obtaining plaintiff's subscriber information and communications conducted through those social media services.[111]

---

[106] See 18 U.S.C. § 2701.
[107] 18 U.S.C. § 2702(a)(1).
[108] 18 U.S.C. § 2702(a)(3).
[109] 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, at 1213.
[110] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).
[111] Id. at 968-969.

Plaintiff moved *ex parte* to quash defendants' subpoenas on the ground that they were prohibited under the SCA.[112] After finding that plaintiff could properly challenge the subpoenas based on his interest in the communications sought, the district court held that Facebook and MySpace were each considered a "remote computing service" and a "electronic communications service" based upon the nature of the messaging services offered by Facebook and MySpace, both private and public.[113] Therefore, Facebook and MySpace were subject to the entire scope of the protections and prohibitions of the SCA. As such, the subpoenas were quashed, and the social media sites were relieved from the obligation of producing the information requested.[114]

As in Crispin, social media companies now use the SCA to fend off a potential tidal wave of third-party subpoenas aimed towards user information.[115] It is yet to be determined how such protection may exist in the future because, as the Crispin court recognized, there is a "difficulty in interpreting the [SCA, which] is compounded by the fact that [it] was written prior to the advent of the Internet and the World Wide Web."[116] That court also pointed to the Ninth Circuit's observation that "until Congress brings the laws in line with modern technology, protection of the Internet and [social media websites] will remain a confusing and uncertain area of the law."[117] Despite this guidance, the SCA remains in effect as of the date of this paper and litigants must remain mindful of the roadblocks it imposes upon them in seeking user information and communications.

---

[112] Id. at 969.
[113] Id. at 989-990.
[114] Id. at 991.
[115] The SCA provides government agencies with an exclusive subpoena procedure. See 18 U.S.C. § 2703(b).
[116] Crispin, 717 F. Supp. at 988
[117] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

2. Issues Related to Facebook Evidence

As one of the most popular social media platforms, Facebook is full of fodder for a prudent litigator. Although Facebook may challenge a Subpoena, an artful discovery request can lead to the same information. That said, litigators must tread carefully through these uncharted waters.

a. The Archive Feature

Facebook created an "archive" feature which allows users to easily download their Facebook "data" into one central file.[118] The data included in this archive includes nearly every action a user can take while using Facebook and the services it offers, from photos and videos to advertisements and "likes." This information may be easily downloaded and accessed in either the user's "downloaded info" or "activity log." While there is no method to individually select which data the user wishes to download (e.g., photos posted), distinct data may be viewed upon access of the entire downloaded file. Facebook's archive feature thus may be used to easily consolidate information due for production from one's client. It may also be leveraged against an uncooperative opposing counsel who claims that compiling their client's Facebook information is an impossible or otherwise overly burdensome task.

b. Friending or Following to Obtain Information

Considering the fact that there are an estimated 901 *million* monthly active users of Facebook, practitioners are keenly aware of the relevance and importance of the information Facebook users voluntarily provide for the world to see. Thus, one of the first reactive measures one may seek to take is to "check Facebook" for relevant

[118] *Accessing Your Facebook Data*, https://www.facebook.com/help/405183566203254?helpref=faq_content (last visited Sept. 14, 2016).

information about an opposing party, attorney, or witness. While such steps may seem harmless and permissible considering the voluntary disclosure of such information by users, ethical considerations are in play, and practitioners should familiarize themselves with any applicable rules before engaging in this type of "detective work."

For example, American Bar Association Model Rule 4.2 states in relevant part that "[i]n representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer."[119] Some ethical authorities, including local and state bar ethics committees, have found that a Facebook "friend" request, even if nominally generated by Facebook and not the attorney, is at least an indirect ex parte communication with a represented party.[120] In this particular decision, the ethical authority equated such a "friend" request, when considering the context in which such request is made, to a request that "X wants to have access to the information you are sharing on your Facebook page."[121] In the event that such "friend" request is found to be motivated by the quest for information about the subject of the representation, additional ethical violations have been found to have occurred. In a similar vein, ethical rules prohibiting attorneys from causing others to encourage an opposing party or counsel from communicating about the subject of the representation have been found to prevent an attorney, or anyone on their behalf, from making a "friend" request in an attempt to obtain information which may only be viewed by accepted "friends."[122] Thus, such an action is comparable to requesting (in the real world) that the opposing party provide access to their private files to (hopefully) provide

[119] MODEL RULES OF PROF'L CONDUCT 4.2.
[120] San Diego County Bar Legal Ethics Committee, SDCBA Legal Ethics Opinion 2011-2, May 24, 2011.
[121] Id.
[122] Id.

helpful information about the case. At a minimum, practitioners must be mindful of potential ethical pitfalls when attempting to obtain information from opposing parties through Facebook "friend" requests or other similar means. The ethical rules in place for traditional modes of communication are still applicable and may lead to a number of unintended negative consequences.

c. Closed Accounts

Facebook provides two options for its users in terms of "closing" an account: deactivation and permanent deletion. An account deactivation removes a user's profile from view of others and search parameters.[123] Such deactivation does not affect the user's Facebook data (which is retained) and thus the account may be "reactivated" at any time through a simple request process.[124] On the other hand, the permanent deletion of a Facebook account precludes any future reactivation. In order to accomplish this permanent deletion a user must make a written request to Facebook.[125] Facebook will delete the account upon such request, but the actual purge of all photos and other data from Facebook servers may take up to ninety (90) days. However, this data is inaccessible to others during the deletion process.[126] Upon permanent deletion, the user's data is erased but some information, such as messages sent to another user, may still remain. Therefore, there is little data which may be recovered in the event of permanent deletion aside from messages or other information which may have been provided from one user to another.

---

[123] *How do I deactivate my account?*, https://www.facebook.com/help/214376678584711?helpref=search.
[124] Id.
[125] *How do I permanently delete my account?*, https://www.facebook.com/help/224562897555674?helpref=search.
[126] Id.

d. Deleted Accounts

Facebook contends that all information or other data (photos, videos, etc.) which is deleted by the user is permanently deleted from Facebook servers.[127] However, Facebook recognizes that deleted data may remain on Facebook servers for a "short time" before its systems eventually complete the deletion.[128] Further, deleted information remains on Facebook backup archives for a longer period of time in order to meet the company's backup needs in the event of a data loss event or other relevant occurrence.[129] Facebook has not publicized if or how access may be made to deleted data which exists in archives or backups.

[127] *Accessing Your Facebook Data*, https://www.facebook.com/help/405183566203254?helpref=faq_content (last visited Sept. 14, 2016).
[128] *Facebook Help Community*, https://www.facebook.com/help/community/question/?id=10154310920251632 (last visited Sept. 14, 2016).
[129] Id.