Electronic Discovery: Maneuvering the New Federal Rules

By: George Bellas[1]

I. Electronic Discovery → Waving Goodbye to the Days of Paper

In 1997 experts estimated that computer users never convert up to thirty percent of all electronically stored documents into paper form.[2] Recent surveys indicate that 93 percent of all documents produced in 1999 were created in digital form,[3] and an estimated 30 percent of all information is never printed on paper.[4] These numbers are increasing every year and recent estimates are that up to 99% of information is never converted to paper.[5] Every big business uses computers to create information, communicate and store data. Business records routinely available in hard copy in prior decades may now be available only on computer.[6]

Litigants who fail to request electronic data will never find many files through traditional means of paper discovery. Additionally, the electronic version of a document may provide an

---

[1] Mr. Bellas is a principal in his firm of Bellas & Wachowski in suburban Chicago, and is also "of counsel" to the nationally recognized personal injury firm of Clifford Law Offices in Chicago. Mr. Bellas currently serves on the 7th Circuit's E-Discovery Committee and has served as a panelist at a Sedona Conference. He can be reached at *george@bellas-wachowski.com*

[2] See Monte E. Sokol & Philip P. Andriola, *Cyberspace Becomes Ground Zero in Discovery Process and at Trial*, N.Y. L.J., Dec. 1, 1997, at S5 (discussing various legal issues surrounding electronically stored data, such as privacy rights, discovery costs, and client counseling).

[3] John J. Hughes, *One Judge's View of Electronic Information in the Courtroom*, THE FEDERAL LAWYER, August 2002, at 41 (citing Kenneth J. Withers, *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence*, Address at the National Workshop for Magistrate Judges (July 2001)).

[4] Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material*, 64-SUM LAW & CONTEMP. PROBS. 253, 280–81 (2001) (citations omitted).

[5] *See, Law Technology News,* October 2007, Page 1.

[6] *See, e.g.*, Daniel T. DeFeo, *Unlocking the Door to Automaker Databases*, TRIAL, Feb. 2003, at 26 ("computerized databases may contain important information—such as design, simulation, and modeling programs that demonstrate how a vehicle or its components perform in crash situations—that appears neither on hard copies nor on computer printouts").

individual with much more information than its paper counterpart.[7] For example, a paper printout of an e-mail message simply contains the names of the sender and the receiver, the text of the message, and the date and the time that the sender sent the message. An electronic copy of the same e-mail message may reveal not only the above information, but also the date and the time that the recipient received the message, whether the recipient actually "opened" the message, and also to whom, if anyone, the recipient forwarded the message. In addition, computer experts often have the ability to determine the exact terminal within a network from which the sender sent the message. Such information may prove critical in some cases.[8]

II. Federal Rules of Civil Procedure

The federal courts have taken the lead in adapting to the technology revolution. Rule 34 of the Federal Rules of Civil Procedure explicitly authorizes a party to request production of electronically stored data.[9] Rule 34(a) has been revised, and now states that

> "[a]ny party may serve on any other party a request . . . to produce . . . any designated documents or electronically stored information—including writings, . . . and other data compilations stored in any medium from which information can be obtained – translated . . . by the respondent into reasonably usable form."[10]

---

[7] *See* Karen L. Hagberg & A. Max Olson, *Shadow Data, E-Mail Play a Key Role in Discovery, Trial*, N.Y. L.J., June 16, 1997, at S3 (discussing differences between paper and electronic versions of documents); *see also* Charles A. Lovell & Roger W. Holmes, *The Dangers of E-Mail: The Need for Electronic Data Retention Policies*, R.I. B.J., Dec. 1995, at 7 (explaining that computer printouts do not contain complete information that a computer's memory stores).

[8] For a discussion of the importance of emails in discovery, see Samuel A. Thumma & Darrel S. Jackson, The *History of Electronic Mail in Litigation*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (1999). For a popular analysis of the factors that make e-mail both attractive and problematic, *see* David S. Bennehum, *Daemon Seed: Old E-mail Never Dies*, WIRED, May 1999, at 100; http://www.wired.com/s ired/archive/7.05/email.html.

[9] The Federal Rules require the requesting party to present specific information on relevance, privilege, time and costs. Superfilm of America, Inc. v. UCB Films, Inc., 219 F.R.D. 649 (D. Kan. 2004); Playboy Enterprises v. Welles, 60 F.Supp. 2d 105 (S.D. Cal. 1999) (production, copying and inspection of hard drives would be allowed subject to relevance and time and cost considerations with provisions for inspection procedures).

[10] There are several types of data which should be collected, preserved and processed: 1) Active

Although the issue of electronic discovery may seem like a recent concept, courts began ordering production of electronic records beginning in 1978.[11]

The Advisory Committee Notes to Rule 34 make it clear that "electronically stored information stands on equal footing with discovery of paper documents." Also, it is careful to state that "[t]he rule covers – either as documents or electronically stored information—information 'stored in any medium,' to encompass future developments in computer technology." Therefore, it is conceivable that any form of electronic data or medium can potentially be discoverable in litigation.[12]

III. Saying Goodbye to the Days of Hardball.

In the context of document discovery generally, a 1997 empirical study on discovery plainly established that stonewalling, not excessive requests, is the most widespread problem. It found that 84 percent of the attorneys in its sample used document requests in their cases, 28 percent of those complained that a party failed to respond to document requests adequately, and

---

data, which is information immediately accessible to users without un-deletion, modification, or reconstruction; 2) Legacy data, which is information created or stored by outmoded or obsolete software/or hardware; 3) Archived data, which is information not directly accessible to a computer systems user (e.g., back up tapes); 4) Deleted data, which is data that existed on the computer as active data but that has been deleted by the computer system or end user activity. Deleted data remains on storage media in whole or in part until an organization overwrites it due to ongoing usage or "wipes" with a software program specifically designed to remove deleted data.

[11] *Bell v. Automobile Club of Michigan*, 80 F.R.D. 228 (E.D. Mich. 1978).

[12] For example, in *Columbia Pictures Industries v. Bunnel*, Case No. CV 06-1093 (FMC(jCx) (Doc. No. 176), in an order dated May 29, 2007, the court held, for the first time, that the contents of a computer's Random Access Memory ("RAM") are discoverable. This marks the first time that there was a requirement that defendants must create documents (RAM is by definition transitory and unsaved information) that they would not ordinarily maintain for the purpose of satisfying plaintiff's discovery requests. This decision actually broadens the meaning of Rule 34's reference of "stored" to include the temporary holding of information in a volatile memory chip. Ralph Losey, *District Court in LA Decides Computer RAM Memory Must Be Preserved and Produced*, http://ralphlosey.wordpress.com/2007/06/20.

24 percent reported that a party failed to respond in a timely manner.[13] Only 15 percent of respondents complained that an excessive number of documents were requested.[14] In other words, nearly twice as many respondents complained of a failure to respond adequately (one form of stonewalling) than complained of excessive requests. Interestingly, even defense attorneys were more likely to complain about stonewalling than excessive requests, by a margin of 24 percent to 19 percent.[15] Earlier empirical studies show that widespread stonewalling has long been a problem. For example, in a survey conducted in the early 1980's, one-half of 1,500 litigators surveyed believed that unfair and inadequate disclosure of material prior to trial was a "regular or frequent" problem.[16]

With the way the electronic discovery modifications to the Federal Rules of Civil Procedure (effective December 1, 2006) are being applied, parties used to playing hardball with discoverable evidence are likely in for a big surprise in the form of a barrage of sanctions. Although the Committee added Rule 37(f) which contains what some people describe as a "safe harbor" provision that states "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules 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," the Committee (and now the courts) are careful to specify when this provision applies.

---

[13] Thomas E. Willging, Donna Stienstra, John Shapard & Dean Miletich, *An Empirical Study of Discovery and Disclosure Practice under the 1993 Federal Rule Amendments*, 39 B.C. L. REV. 525, 540, 574–75 (1998).

[14] *Id.* at 575.

[15] *Id*.

[16] Deborah Rhode, *Ethical Perspectives on Legal Practice*, 37 STAN. L. REV. 589, 598–99 (1985).

The Committee Note for this section states that it *only* applies when the information is "lost due to the 'routine operation of an electronic information system.'" The information must have been lost in good faith, which may require "a party's intervention to modify or suspend certain features of that routine operation" as a result of a preservation order or "litigation hold." One factor to determine good faith is "whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources."

A. Sanctions Anyone?

While it was originally thought that this rule would make it harder to obtain sanctions and more likely that corporations would hasten their document destruction policies and make it difficult to obtain electronically stored information, this has proven thus far to not always be the case.[17] The courts have, in many cases, taken a hard-nosed approach to dealing with uncooperative and negligent parties as well as their attorneys. A number of requirements/duties for attorneys have developed, that if not complied with, could bring harsh sanctions for the case and even for the attorney personally.

In one early case when counsel gave conflicting statements and inadequate answers to e-discovery requests, the frustrated judge instructed the jury that unless the Defendant could prove otherwise, the jurors should assume they had defrauded the Plaintiff.[18] The Defendants lost substantial compensatory and punitive damages in the case, and in fact, their production of

---

[17] *See* Phillip M. Adams & Assocs., *LLC v. Dell, Inc.*, 2009 WL 910801 (D. Utah Mar. 30, 2009) (the court denied application of the safe harbor provision because an e-discovery expert failed to state that the loss of information was the result of "routine, good-faith operation"),

[18] *See* Charles A. Ragan & Lori Ann Wagner, *Competence and Credibility in E-Discovery*, 43 TRIAL, 40, 42 (Apr. 2007) (citing *Coleman Holdings Inc. v. Morgan Stanley & Co.*, 2005 WL 674885 (Fla. Palm Beach Co. Cir. Mar. 23, 2005).

records in a large number of other securities arbitrations was subsequently investigated. [19] Therefore, not only can the success of the pending matter be affected, but future credibility in other matters can be placed in jeopardy.

Other sanctions can also be imposed. In *Network Computing Services Corp. v. Cisco Systems, Inc.*, when Cisco tried to insist they did not have a customer list, the judge punished the party by directly informing the jury about the misconduct.

Another potential sanction is the granting of an adverse inference. Some jurisdictions, such as the 10th Circuit, grant an adverse inference instruction only upon a showing of bad faith by the requestor.[20] However, others rely on the three-prong test of *Residential Funding Corp. v. DeGeorge Fin. Corp.*,[21] which states that an adverse inference instruction is satisfied when: 1) party having control over the evidence had an obligation to preserve it; 2) the records were destroyed with a culpable state of mind, and 3) the destroyed evidence was relevant to the party's claim or defense.[22] It is important to consider the standards of your jurisdiction, but regardless, the withholding of information or implementing stall tactics can prove disastrous for your case.

In 2008 and 2009, courts demonstrated a noteworthy unwillingness to tolerate e-discovery mistakes made by counsel, resulting in a greater number of cases in which sanctions were given in order to hold attorneys and parties accountable for their e-discovery shortcomings. A study done in the first 10 months of 2009 by Kroll Ontrack analyzed 108 decisions addressing

---

[19] *See id.* at 42 n.7 (citing Jaime Levy Pessin, *Morgan Stanley Used 9/11 As Escuse, NASD Says*, WALL ST. J., Dec. 20, 2006, at A3.

[20] *See, e.g.*, Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 2007 U.S. Dist. Lexis 15277 (D. Colo. Mar. 2, 2007).

[21] *See* World Courier v. Barone, 2007 U.S. Dist. LEXIS 31714 (N.D. Cal., Apr. 16, 2007).

[22] 306 F.3d 99, 105 (2d Cir. 2002).

e-discovery. Thirty-nine percent of these cases addressed sanctions. 66.67% of the cases addressing sanctions involved preservation and spoliation issues, 16.67% involved production disputes, and the last 16.67% involved other discovery abuses.[23] Of the forty-two cases dealing with sanctions, 69% of those awarded sanctions in full or in part.[24] Obviously, the topic of sanctions remains a hot-button issue in the realm of e-discovery, as fewer courts are willing to tolerate misbehaviors or substandard e-discovery practice by counsel and parties.

B. Avoiding Sanctions: New Duties of Counsel.

As outlined by relevant case law, there seems to be three duties that counsel must adhere to in order to avoid these types of sanctions in litigation with electronic discovery:

1 Take appropriate measures to ensure that the client has provided all available information and documents which are responsive to discovery requests.[25]

> One of the most critical issues facing the attorney seeking discovery of electronic data is determining whether all of the requested materials have been produced for inspection and/or copying. The only means by which a proper determination of whether a document production has been satisfied is to retain a data forensics specialist to make a mirror image[26] of the targeted party's computer hard drive and to analyze it in order to determine when and if any deletions and/or modifications of a document has occurred and, if so, recreate the original document and indicate the date of the deletion or modification.[27]

This duty includes validating employee production of documents, and not merely relying

---

[23] *Practice Points: 2009 Year in Review—Courts Continue Imposing Sanctions for E-Discovery Shortcomings*, KROLLONTRACK.COM NEWSLETTER, Jan. 2010, *available at* http://www.krollontrack.com/newsletters/clu_0110.html.

[24] *Id.*

[25] *Cache La Poudre Feeds*, 2007 U.S. Dist. LEXIS 15277, at *56–57.

[26] A "mirror image" 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. United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 48 (2002).

[27] Stephen M. Cohen, *Electronic Data and Discovery: Nightmare or Opportunity*, 76-FEB FLA.B.J. 30, 32–33 (2002).

on employees to locate and identify relevant documents.[28] By inadequately relying on employees or other parties to validate information, the attorney could be the subject of sanctions, perhaps similar to those imposed on Land O'Lakes in March 2007, where they were sanctioned $5,000 for inappropriately relying on employees who failed to halt an email destruction program, and to identify 400 applicable backup tapes.[29] In *Phoenix Four Inc. V. Strategic Resources Corp.*, the court sanctioned counsel and found that it was their duty to search for sources of information, and that they could not blindly accept the client's representations as to whether there were computers to search. Counsel was required to conduct a methodical search and ask all relevant questions in order to ensure that all relevant information was produced.[30] The key to this duty is communication between the client, the attorney, and identified Information Technology personnel within the company, or hired from without. The attorney, after receiving information, must confirm it from personnel authorized and knowledgeable enough to validate it.[31]

2. Counsel must instruct their client not only of the existence of a "legal hold" to ensure preservation, but must also oversee its compliance.[32] "Counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical)

---

[28] *Id.* at 45–46.

[29] *Id.*

[30] 2006 WL 1409413 (S.D.N.Y. May 23, 2006).

[31] *See Linnen v. A.H. Robins Co.*, 1999 WL 462015 (Mass. Super. June 16, 1999) (counsel sanctioned after he obtained information from a manager about the existence of email backup tapes rather than interviews with knowledgeable IT personnel).

[32] *Zubulake v. UBS Warburg, LLC.*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004).

implementation of the firm's recycling policy."[33] This duty is similar in some respects to the duty to ensure the release of documents. The attorney is required to implement many of the same techniques as ensuring production of documents, however, they are simply ensuring that relevant information is not destroyed, rather than produced. If an attorney fails in this duty, the client could potentially be responsible for expensive restoration of data that could have easily been preserved.

In *Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority*,[34] when the producer did nothing to stop the process of automatically deleting emails, counsel's argument that restoring the emails would cause undue burden and expense was fruitless as the Magistrate compared it to Leo Kosten's definition of chutzpah, "that quality enshrined in a man who, having killed his mother and his father, throws himself on the mercy of the court because he is an orphan." Therefore, the client was forced to incur the full burden of restoring emails from backup tapes as a result of the previous failure to implement the litigation hold.[35]

In *Housing Rights Center v. Sterling*, shortly before trial, the Plaintiffs were able to secure an order for monetary sanctions and an adverse jury instruction because counsel failed to instruct their clients to preserve relevant documents.[36] Intentional destruction is clearly not required for sanctions to be imposed, but mere negligence can cause sanctions.[37]

---

[33] *Id.*

[34] 2007 U.S. Dist. LEXIS 39606 (D.D.C., June 1, 2007).

[35] *Id*.

[36] 2005 WL 3320739 (C.D. Cal. Mar. 2, 2005).

[37] *See MOSAID Tech., Inc. v. Samsung Electronics Co., Ltd.*, 348 F. Supp. 2d 332 (D.NJ. 2004); *see also Applied Telematics* (1994), a patent infringement suit, ATI's request for documents had been thwarted. Sprint's policy of rotating backup tapes (which included deleted information) eliminated prior week data and, therefore, Sprint could not produce all of the requested data.

To avoid these types of hopeless situations, and the disfavor of the judge, it is imperative that the attorney ensure that litigation holds are properly implemented. Attorneys should regularly consult with clients about the techniques and policies in place, and how they are being monitored to ensure that relevant data is not destroyed.

3. Counsel must proceed at a "reasonable pace." When tactics are employed that indicate indifference to discovery obligations and deliberate sluggishness, an array of sanctions can result. As such was the case in *Lava Trading, Inc. v. Hartford Fire Insurance Co*,[38] where the court recognized a pattern of large-scale production on the eve of court conferences and key depositions, as well as a failure of the attorney to ensure relevant documents were located. The Plaintiffs in this case were heavily sanctioned.

A reasonable pace also comes into play in the number of parties organized to fulfill discovery responses. In *Williams v. Taser International, Inc.*, the court rejected Taser's continued representations that it had limited IT and legal resources.[39] The court elaborated by saying, "Taser implies that because it has elected to hire and train only a single technology employee, and because it has chosen to retain only a handful of attorneys to conduct document review, it is somehow relieved from its obligations to timely respond to Plaintiff's discovery requests. That is not the case. Rather, the Court expects that Taser will make all reasonable efforts to comply with its discovery orders including, if necessary, retaining additional IT professionals to search electronic databases and adding additional attorneys to perform document review." [40] This comment can potentially have staggering implications for smaller firms who are

---

The court ruled against Sprint, even though the destruction of the data was not deemed willful.

[38] 2005 WL 459267 (S.D.N.Y. Feb. 24, 2005).

[39] 2007 U.S. Dist. LEXIS 40280, *20 (N.D. Ga. June 4, 2007).

[40] *Id*.

considering taking on a larger litigation with a lot of electronic discovery. When taking any case, attorneys have to account for their available resources and keep in mind that the court is not going to excuse a party simply because they only have a couple of attorneys dedicated to the case or a shortage of IT personnel. Discovery obligations must be complied with in a timely manner regardless of staffing. Short-staffed parties can appear (to the court) to be evading discovery obligations and can be sanctioned accordingly.

With the barrage of sanctions being handed out, it can be confusing and almost impossible to outline the exact duty of the attorney, and to what degree of prodding of their client's company the attorney is required to institute. Unfortunately there is no definitive answer, except that it seems to be appropriate to rely on knowledgeable Information Technology Personnel to whom you have informed that it is to the utmost degree of importance for all relevant information to be produced and preserved, and to ensure that nothing is hidden. They must also be informed that deceitful behavior (as in engaging in intentional destruction of evidence) is often detected by the court, as forensics will often recover data thought to have been destroyed or uncover other devious behavior.[41] This is important because a lawyer's reputation can be permanently damaged if they are associated with the destruction or concealing of evidence.[42] Attorneys should ask clients (and their employees), even repeatedly, if they are sure that everything is produced and preserved with regard to both current and archived data. They need to fully understand that any negligence in these matters could cost the company a

[41] *See* Ragan, *supra* note 16, at 50. This last point regarding "deleted data" is significant. Many, including judges, believe that once a data is deleted, it cannot be recovered. This is not true. There are companies that specialize in restoring deleted data or data that has been found on computers that have been damaged. Once such company, Kroll Ontrack, can retrieve data even in part by using special restorative equipment and software that searches through the recovered data; *see also* Antioch Co. V. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (Deleted computer files, whether they be emails or otherwise, are discoverable).

[42] *See id.*

significant amount of money not only in monetary sanctions, but from the potential cost of losing the litigation as the result of the granting of an adverse inference or, if done by plaintiffs, a dismissal of the case completely.[43] Attorneys must also ensure that the fulfillment of discovery obligations is moving along at a reasonable pace, and if not, they must immediately consult with their clients about hiring additional personnel.

IV. The Advent of the Meet and Confer: Not just your average Pre-trial Conference.

These duties of counsel in litigation begin with the Meet and Confer conference. Rule 26(f) of the Federal Rules of Civil Procedure is amended to direct the parties to discuss discovery of electronically stored information during their discovery-planning conference. It states that "the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses . . . to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning: . . . (3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."

This rule is important as these early discussion requirements can have a tremendous effect on the direction and progress of modern electronically loaded litigation. This rule forces the parties to develop a discovery plan very early in the litigation and agree on certain terms of discovery, potentially alleviating the likelihood of later expensive discovery disputes. It can be important to make it clear to the opposing party, even prior to this meet and confer, what you expect from the conference and that you are not treating it as a perfunctory "drive-by"

[43] *See, e.g.*, Leon v. IDX Systems Corp., 464 F.3d 951 (9th Cir. 2006).

exchange.[44] It is better to discuss these issues at the outset and set the tone for the litigation.

The Judge in *Hopson v.Mayor of Baltimore*,[45] described the obligations under new Rule 26(f) with particularity:

> [C]ounsel have a duty to take the initiative in meeting and conferring to plan for appropriate discovery of electronically stored information at the commencement of any case in which electronic records will be sought . . . At a minimum, they should discuss: the type of information technology systems in use and the persons most knowledgeable in their operation; preservation of electronically stored information that may be relevant to the litigation; the scope of the electronic records sought (i.e. e-mail, voice mail, archived data, back-up or disaster recovery data, laptops, personal computers, PDA's, deleted data); the format in which production will occur (will records be produced in "native" or searchable format, or image only, is metadata sought); whether the requesting party seeks to conduct any testing or sampling of the producing party's IT system; the burdens and expenses that the producing party will face based on the Rule 26B2 factors, and how they may be reduced (i.e. limiting the time period for which discovery is sought, limiting the amount of hours the producing party must spend searching, compiling and reviewing electronic records, using sampling to search, rather than searching all records, shifting to the producing party some of the production costs); the amount of pre-production privilege review that is reasonable for the producing party undertake, and measures to preserve post-production assertion of privilege within a reasonable time; and any protective orders or confidentiality orders that should be in place regarding who may have access to information that is produced."[46]

Since this early conference requires that parties discuss information systems, preservation, and format exchange, it is impossible to have a productive conference if the attorneys are not at least familiar with their client's IT systems and data locations. Keep in mind the unwillingness of the party to invest too much into finding out about their IT system especially, but make it clear regardless that they have an obligation to put forth this information

---

[44] Jeffrey J. Greenbaum, *Report Regarding Changes to Discovery Rules Regarding Electronic Discovery*, https://www.abanet.org/litigation/standards/docs/ediscovery_report.pdf.

[45] 232 F.R.D. 228 (D. Md. 2006).

[46] *Id.* at 245.

and find out in spite of the cost. Judge Shira Scheindlin, the originator of the Zubulake Duty (requiring attorneys to make certain that all relevant electronic information is put on hold) was quoted as saying that if attorneys' come to conferences unprepared to discuss all aspects of e-discovery, "that's just not accepted by the rules."[47] She goes on to say that "[y]ou don't have to know everything at the first conference. But you at least have to start to assess the situation." This infers a small amount of leeway, but probably for only a very short period of time in the litigation.

This also does nothing to dispel the growing concerns about the vast resources potentially necessary to become familiar with IT systems early in the litigation and satisfy these requirements. This is an even greater concern for attorneys representing mid to large size corporations with extremely complex IT structures that few of the company's own IT personnel even understand. On the other hand, however, the more that an attorney understands early on in the litigation, the more aspects of their client's system they are able to rule out of discoverable information, and discovery requests can therefore be narrowed (substantially lowering the cost of discovery) at the 26(f) conference. The more accurately you can narrow the system to include only the most relevant information, the more the opposing party may be willing to limit their scope of discovery in an agreement.

Therefore, by reminding the other party of their obligations and fulfilling yours to learn about your own client's IT systems, many disputes can potentially be diffused early-on in the litigation by revealing a much more accurate cost assessment for both sides, thereby promoting settlement discussions to avoid these said costs.

Even after insisting to your opposing party their obligations, if you are still met with a

[47] Jason Krause, *E-discovery Gets Real,* ABA J., Feb. 2007.

contentious opposing party who continues to be ignorant of their client's IT systems, another recourse is taking a Rule 30(b)(6) deposition of the IT personnel of the company.[48] This will allow you to find out the way in which documents have been stored and maintained, and what is available.[49] Then following, some type of agreement can potentially be made.

However, in failing to come to some type of agreement on these issues in the Rule 26(f) conference(s), you run the risk that the court will establish its own discovery protocol for your case. In *Williams v. Taser International, Inc.*, as a result of the parties' inability to work together reasonably in an effort to resolve discovery disputes, the court imputed its own discovery plan on the parties.[50] There again, contentious behavior amongst the parties will probably not net anyone what they want or could have bargained for originally.

V. Preservation: Steps to Success.

There are several issues with respect to preservation. The first pertains to discussions prior to commencement of litigation. Whether you are a plaintiff's or a defendant's attorney, you should discuss generally where and how relevant information is kept. Magistrate Judge Ronald Hedges feels that lawyers should be asking clients "Where are your documents?"[51] They should know "for no other reason than to comply with Federal Rule 11 obligations before litigation commences."[52] He also finds that "the fact that a person consults a lawyer" does not "ipso facto creat[e] a preservation obligation."[53] The Judge goes on to state that a failure to

---

[48] Ken Withers, *Judges, Lawyers, and the New Rules*, 43 TRIAL 20, 21 (Apr. 2007).

[49] *Id*.

[50] 2007 U.S. Dist. LEXIS 40280, *15–16 (N.D. Ga. June 4, 2007).

[51] *See* Withers, *supra* note 47, at 24.

[52] *Id*.

[53] *Id*.

discuss these issues prior to litigation could potentially result in some type of malpractice.[54]

The next issue with respect to preservation is the Preservation Letter. It is a Preservation Letter when sent to your adversary and a "litigation hold notice" when sent to your client.[55] Trial Magazine describes it perfectly as "a tool to educate your opponent about the sources of relevant electronic evidence and the importance of quickly taking steps to ensure that they remain intact and accessible."[56] The importance of the letter is to force the opposing party to recognize their duty to preserve data and discredits any future frivolous claims under the "safe harbor" provision of Rule 37(f).[57] The duty to preserve arises when a party "knows or has reason to know that evidence may be relevant to future litigation."[58]

According to Craig Ball, an expert in electronic discovery, the perfect preservation letter should encompass the following:

1. Tell the party what the letter and litigation is about with sufficient information that a reasonable person reading the letter would know what is relevant; as many times, the letter is the recipient's first notice of a dispute.
2. Be very specific about what you want and do NOT demand ALL electronic communications because it is likely that your opponent may be less accountable for the destruction of information than if you were very specific about what should be preserved.
3. Emphasize the importance of clearly communicating retention obligations to

---

[54] *See id.*

[55] Craig Ball, *The Perfect Preservation Letter*, 43 TRIAL 28, 28 (Apr. 2007).

[56] *Id*.

[57] *Id.* at 28, 30.

[58] *Id.*

employees and third parties; (as a preservation letter is effectively useless if it never reaches the appropriate hands so several letters may be appropriate if you are serving a large company).

4. Do a thorough search of the structure of backup systems within the company and be specific about whether you want the company to preserve all current data or just newly created data.
5. If Metadata is required for a case, articulate why it is relevant and specifically require it to be preserved.
6. If computer forensics is necessary for a case—such as when deletion, alteration or fabrication is an issue in the case—the preservation letter should specify that systems that contain deleted data must be immediately preserved in a "forensically sound way" and even suggest suitable methods. (This will probably require consulting an expert).[59]

Articulation and communication is the most important goal of the preservation letter. You want to succinctly, and expertly craft a document that allows your adversary to know that you are serious about the litigation, that you are well prepared, fully aware of their preservation obligations, and intend to enforce them.

In addition, once the litigation has commenced, under the Meet and Confer requirements of Rule 26(f), the parties should discuss issues with respect to preservation. This can prove to be an easier way to resolve discovery disputes early and avoid applications for preservation orders from the court, as these discussions about disclosure or discovery of electronically stored information can, as a result of the modification to Rule 16(b), be included in the court's

[59] *Id*. at 30–33.

scheduling order. If these issues are not adequately discussed before the Rule 16(b) scheduling conference, the conference may accomplish little or nothing with regard to the progress of the case. In many instances, more than one Rule 26(f) conference is necessary for proper scheduling of all of the time tables for electronic discovery.[60] In that case, the court may require the parties to confer at a 16(b) conference after each session in order to resolve any disputes.[61] However, if the case is neither complicated, nor wrought with electronic discovery, this can be a waste of time and resources for the parties and the court's patience will likely grow thin very quickly, as attorney's have a duty to learn about the IT systems of their clients early in litigation or face sanctions.[62]

Counsel should not defer to the option of motioning for a preservation order from the court. The Advisory Committee states in its Comments under Rule 26(f) that "A blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations." In addition they further warn that [a] preservation order entered over objections should be narrowly tailored" and that [e]xparte preservation orders should issue only in exceptional circumstances." Consequently, an application for a preservation order may not net the party what it needs or wants, or anything that a proper negotiation could not have netted with the proper techniques and cooperation. The court is loath to get involved in discovery disputes, especially with contentious parties who continually bring them before the court.

Therefore, a well-crafted strategy for preservation is to first, prior to litigation, speak to

---

[60] *See* Lee H. Rosenthal, *A Few Thoughts on E-discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167 (2006), http://thepocketpart.org/2006/11/30/rosenthal.html.

[61] *Id.*

[62] *See supra* Section III.

your client about preservation issues and the location of information. Then once litigation is certain, craft a narrowly tailored preservation letter to ensure that the opposing party is satisfying their own discovery obligations. Finally, once the litigation has commenced, enter the Meet and Confer session fully prepared to discuss all issues with respect to the preservation of electronic discovery so that you are able to negotiate. This strategy is in the best interest of your client as litigation is a two-way street. If you are consistently unprepared with a contentious attitude, insisting that the opposing party release absolutely everything they have immediately, that behavior will likely be mirrored in their responses, effectively dragging out litigation and causing more expense for your own client.

VI. Importance of the Forms of Electronic Information: Preservation and Production.

When communicating with the opposing party with respect to Preservation and Production, it is important to confer with the opposition about the forms in which documents are being preserved and produced.

With respect to preservation, the rules merely state that preservation should be one of the issues discussed at the Meet and Confer conference under Rule 26(f). However, it is important to keep in mind what the courts have outlined with respect to preservation. One court, in *Quinby v. Westle AG*, recognized that the defendant could choose how to meet its preservation obligation and should not be sanctioned for selecting one format over another, not even for selecting an inaccessible format over an accessible format.[63] The consequences of this decision mean that early in the litigation, it is necessary to specify the form or forms in which discoverable information is being preserved. The courts are not necessarily going to require the party to preserve information in ways that are easily accessible.

[63] 2006 WL 2597900 (S.D.N.Y. Sept. 5, 2006).

However, on the other hand, this issue is extremely unpredictable as a different judge in the same jurisdiction found that storing information in a less accessible format does not meet the party's preservation obligation and may be sanctionable.[64] Therefore, if your client is the producing party in a litigation, it is wise to discuss a plan for preserving information. If certain information is readily accessible at the beginning of the litigation, but is deemed relevant to discovery later, it may be difficult to claim undue burden in producing it if it was your client who made the information inaccessible after the preservation obligation arose.[65]

Another issue for discussion should be the form or forms in which information is produced when discovery actually commences. The Federal Rules of Civil Procedure provide under Rule 34(b) that a request for production of electronically stored information "*may* specify the form or forms in which electronically stored information is to be produced." If no form is specified, the opposing party can produce the information either "in the form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." If you are the requesting party, it is a good idea to put a specific form into the production request (if possible).[66] Almost anything is "reasonably usable" including non-searchable TIF images. In fact, nothing in the rule prevents a responder from printing out paper copies and providing these

---

[64] *See* Trexel v. Biovail Corp., 233 F.R.D. 363, 372 n.4 (S.D.N.Y. 2006).

[65] These approaches to Rule 26B create a situation for the producer where he has a duty to preserve electronically stored information that he knows or reasonably should know is *relevant* to anticipated or filed litigation. It may choose to secure this information in formats that are not reasonably accessible. But to recover costs, it must secure electronically stored information that it should reasonably foresee would be *discoverable* only on accessible sources. A producer may have to make this distinction early in the litigation between "reasonably-foreseeable-as-relevant-to-the-litigation" and "reasonably-foreseeable-as-discoverable" early in the process. Rosenthal, *supra* note 59.

[66] This is yet another reason why it is important to emphasize the importance to the opposing party of being prepared for the 26(f) conference, as it is impossible to specify the form or forms of production if you have no idea the type or location of electronic information prior to this Meet and Confer conference.

are reasonably usable. If documents are requested in "native format," or the format ordinarily maintained, even though there is a general presumption against the production of metadata, the courts have held that this creates the opposite presumption that the metadata should be produced intact and attached to the electronic documents.[67]

The easiest way to avoid conflicts regarding the form or forms of production is to discuss, pursuant to Rule 26(f)(3), this matter in the Rule 26(f) Meet and Confer conference in a detailed manner. If you are producing party in the litigation, inform your opponent that you are stripping out most of the metadata, and leave the requesting party to show the judge why they really need it.[68] If you are the requesting party, closely evaluate whether the metadata is even necessary to your case, and avoid arbitrarily asking for it just because you can, as it can run up the review costs of discovery without much benefit.[69] As is evident from a Legal Tech Conference in January, 2007, judges are not thrilled with controversies over metadata, and U.S. Magistrate Ronald Hedges even described it as "the disease of the week," causing court proceedings to be unnecessarily dragged out.[70]

It is important for both sides to be clear from the beginning about issues relating to forms of production, especially when it comes to metadata. The more clearly both sides discuss these issues, the less needless litigation and motion practice will result.

---

[67] *See* Williams v. Spring/United Management Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (holding that when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, . . . the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata).

[68] Jo Maitland, *Judges Speak Candidly on New E-Discovery Rules*, SEARCHSTORAGE.COM, Jan 31, 2007, http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1241499,00.html (outlining the recommendations of Thomas Allman, senior counsel at Mayer, Brown, Rowe & Maw, LLP , at a Legal Tech conference in New York in January, 2007).

[69] *Id*.

[70] *Id*.

VII. Privilege and Work Product Waivers: Ensure your client's privacy.

The potential waiver of privileged materials or those protected by attorney work product is a concern in litigation involving a vast amount of electronic information that is difficult, time-consuming and expensive to adequately monitor. The Federal Rules of Civil Procedure in Rule 26(b)(5)(A) state in essence that a party who withholds information on claim of privilege must specifically describe the documents in a way that enables an identification on whether they are privileged or not. This provision only seems to create problems with respect to the cost of reviewing the information for privilege.[71] Even the Advisory Committee notes the time and effort required to review documents for privilege.[72]

However, bigger problems occur with Rule 26(b)(5)(B) which states that:

> If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

The Advisory Committee notes that the courts have protocol for determining whether waiver results from inadvertent disclosure and seems to defer to their judgment. However, this can be avoided by the parties agreeing to a privilege/work product protocol before any actual exchange of documents occurs, during the meet and confer conference under Rule 26(f). In addition, Rule 16(b) allows the court to include "any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production," into the

[71] Refer to Advisory Committee Notes for Fed. R. Civ. P. 26(b)(5) that notes the time and effort required to avoid waiver by reviewing all materials produced.

[72] *Id.*

scheduling order. If you are the party producing a lot of electronic data, it is a good idea to outline a detailed protocol for when privileged or work-product information is accidentally produced. This can become even more important in considering the next issue.

When documents are inadvertently produced, while Rule 26(b)(5) provides the protocol for inadvertently produced documents in federal court by way of the "clawback provision," the rules fail to mention whether or not this inadvertent production is a waiver in a state court case.[73] This could potentially create a serious problem for litigants mass-producing electronic data for production. As previously noted, reviewing documents for privilege and work-product can cause great expense and delay in the case, but the cost of the potential waiver of a document in other litigation could be staggering. And while the parties could have an agreement that concerns the ultimate non-waiver of documents in future litigation, this does not preclude non-parties, (who obviously came to no agreement), from taking advantage of this inadvertent production in future federal or state cases. Parties need to be cautious, while as they are protected from inadvertent waiver in the current litigation, it is not as airtight of a protection as it seems.

In addition to this danger, counsel should be wary that the courts are likely to import a reasonableness requirement into the Rule 26(b)(5)(B) "clawback provision." According to *Trial Magazine*, a party's careless work is not excused just because it was inadvertently produced. The producing party needs to show that it used reasonable procedures to ensure that privileged or otherwise protected material was not disclosed.[74] In addition, the Advisory Committee on Evidence Rules of the Judicial Conference approved the addition of a new Rule 502.[75] When an inadvertent disclosure is made, this rule would govern whether or not there was a waiver of

---

[73] *See* Withers, *supra* note 47, at 25, 27.

[74] Alan Blakley, *Sharpen your discovery from nonparties*, 43 TRIAL 34, 35 (Apr. 2007).

[75] *Id.* at 35–36.

privilege or work product. Section B of the proposed rule explicitly outlines that the "disclosure was made in spite of 'reasonable precautions to prevent disclosure.'"[76] Since many state and civil courts tend to adopt the federal rules, it is likely that they will also adopt this reasonableness requirement.

Accordingly, it is imperative in litigation that adequate procedures are in place to prevent, whenever possible, any inadvertent disclosures of any items subject to attorney-client privilege or attorney work-product. While the clawback provision prevents them from being used in the current litigation, there is no guarantee that it could be excluded in later federal litigation or outside of federal court. In addition, having these procedures properly in place may also prevent these items from being used as evidence in a subsequent state proceeding depending on the jurisdiction. An attorney should discuss with his or her client the cost/benefit analysis of the potential future effects of any disclosures, and weigh it against the current costs and delays in a meticulous review of everything released to the opposing party.

VIII. Automatic Disclosure, Withholding and Cost-Shifting: Considerations for Success.

Under Rule 26(a), parties have an initial obligation to automatically disclose certain information. While this combines with the potential duties of knowing about your client's IT systems described above, and concerns about the waiver of privilege, there are certain circumstances where automatic disclosure can be withheld, that is, if the information poses an unreasonable burden on the parties to produce it.

At this point, federal courts apply a balancing test to determine whether to shift some or all of the costs of producing "inaccessible" electronically-stored information. This balancing test is derived from two cases arising out of New York's Southern District, *Rowe Entertainment Inc.*

[76] *Id.*

v. William Morris Agency, Inc. and *Zubulake v. UBS Warburg LLC*. In *Rowe*, decided in 2002, the defendants were asked to produce e-mails relating to the selection of concert producers. The defendants refused on the basis that much of this information was kept on legacy back-up tapes, making it prohibitively expensive to produce.[77] Judge Francis ruled that the high cost of recovery alone was not a basis for precluding discovery, and proceeded to outline an eight-factor balancing test to determine who should pay for the cost of retrieving the data,[78] ultimately deciding that the plaintiffs should bear the cost of production.[79]

The *Zubulake* cases[80] are arguably two of the most important in terms of e-discovery cases, and are certainly important in terms of setting the standard for cost-shifting. It was in this case that Judge Shira Scheindlin noted that whether the production of electronically stored information is unduly burdensome is dependent upon whether that information is in an accessible or inaccessible form, which is further dependent upon the type of media on which this ESI is stored. Judge Scheindlin further found that the *Rowe* eight-factor balancing test "tend[ed] to favor the responding party, and frequently result[ed] in shifting the costs of electronic discovery

---

[77] Rowe Entertainment Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 424–26 (S.D.N.Y. 2002).

[78] The factors to be taken into consideration were: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party.

[79] *Rowe*, 205 F.R.D. at 432.

[80] The relevant *Zubulake* cases are *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. May 13, 2003) ("*Zubulake I*") and its follow up case *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. July 24, 2003) ("*Zubulake III*"). *Zubulake II* (Zubulake v. UBS Warburg LLC, 2003 U.S Dist. LEXIS 7940 (S.D.N.Y. May 13, 2003) addressed Zubulake's request to report the contents of certain depositions to outside agencies.

to the requesting party."[81] The court then modified the *Rowe* balancing test to a seven-factor balancing test.[82] It was that seven-factor test first outlined by the *Zubulake* court that heavily influenced the 2006 amendments to the Federal Rules of Civil Procedure Rule 26.

Advisory Committee notes require that the parties confer on these issues before a motion to compel discovery or protective order is sought. If the parties are still unable to agree, the court will move into the two part judicial inquiry in Rule 26(b)(2)(B). First the party opposing the discovery must establish that the sources are unreasonably accessible due to undue burden or cost. When deciding whether or not under Rule 25(b)(2)(C), a proportionality rule or "cost-benefit analysis" is described where the evidence can be excluded if the "burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues."

If undue burden is found, the party seeking the discovery still has a chance to compel discovery under the second part of the judicial inquiry in Rule 26(b)(2)(B) if they can establish good cause for production. The Advisory Committee has suggested seven factors for the court to consider in making this analysis:

1. the specificity of the discovery request;
2. the quantity of the information available from other and more easily 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;

---

[81] *Zubulake I*, 217 F.R.D. at 323.

[82] *See* Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 284 (S.D.N.Y. 2003) ("*Zubulake I*") (citing the seven factor test for determining whether cost-shifting is appropriate for inaccessible data: 1) The extent to which the request is specifically tailored to discover relevant information; 2) The availability of such information from other sources; 3) The total cost of production, compared to the amount in controversy; 4) The total cost of production, compared to the resources available to each party; 5) The relative ability of each party to control costs and its incentive to do so; 6) The importance of the issues at stake in the litigation; and 7) The relative benefits to the parties of obtaining the information.)

4. the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
5. predictions as to the importance and usefulness of the further information;
6. the importance o the issues at stake in the litigation; and
7. the parties' resources.[83]

There is a concern under this rule that it acts as another safe-harbor, rewarding outmoded IT systems and acting as a disincentive to upgrades that would improve accessibility to stored information.[84] This rule makes hard-to access computer data unavailable absent a showing of good cause, where the seeking party will likely have to overcome the Seven Factor Test. Data with difficult access may, then, never have to be searched or produced. And while the attorney has a duty to proceed at a reasonable pace and know his or her client's IT system in order to be able to adequately meet and confer under Rule 26(f), the attorney may be able to adequately describe these inaccessible sources of data, without knowing what they contain, and run to a judge claiming inaccessibility, thereby triggering a showing of good cause on the seeking party. Also in considering that one of the factors is "the parties' resources," if the party is a small computer-outdated corporation, it may be impossible to gain the information if you are unable to solidly show that the information will be important and crucial to the litigation. And while it may be a risk to companies not updating their systems in possibly losing to a showing of good cause,[85] the provision considering the parties' resources may make it impossible for a party to

[83] The Court applied these seven factors in *In re Veeco Instruments, Inc. v. Securities Litigation*, 2007 U.S. Dist. LEXIS 23926 (S.D.N.Y., April 2, 2007), finding that, "Emails sent or received by Defendants relating to the issues herein could constitute important relevant evidence and are reasonably calculated to lead to admissible evidence. It has not been demonstrated that said information is reasonably available from any other easily accessed source. The discovery requests are specific. The resources of the parties are not an issue." *Id.* at *5.

[84] Ralph Losey, *Do the New Rules Discourage IT Improvements?*, http://ralphlosey.wordpress.com/.

[85] *See* Kentucky Speedway, LLC v. NASCAR, 2006 U.S. Dist. LEXIS 92928 (E.D. Ky. Dec. 18, 2006) (illustrating that costs of 3 million dollars in five months are not that unusual).

access information in a case expected to be worth less than the projected millions accessing the data might cost.

One way to possibly counteract this effect is to insist that the responding party fulfill their duty under the Advisory Committee note for Rule 26(b)(2) and "identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and likelihood of finding responsive information the identified sources." Remind the party that they have a duty to preserve these sources.[86] However, a requesting party must be sure to consider how much it will cost to review the information if it is actually obtained.[87]

Yet another consideration arises under the Advisory Committee note to Rule 26(b)(2)(B). The general assumption for discovery is that the party from whom discovery is sought bears the cost of producing the documents. However, Rule 26(b)(2)(B) allows for a court to shift the costs of production of sources deemed not reasonably accessible.[88] This provision should also be a concern, as excessively broad discovery requests that include reasonably inaccessible

---

[86] Advisory Committee Note for Fed. R. Civ. P. 26(b)(2), and advice of Judge Ronald Hedges who states that even after a court decides that a source is not subject to discovery, the party is still not "safe discarding anything until they get some type of agreement from the other side." *See* Withers, *supra* note 47, 25.

[87] Consider using word-searching, sorting, and other forms of computer manipulation that can possibly reduce the time involved in reviewing and organizing evidence. Mark D. Robins, *Computers and the Discovery of Evidence: A New Dimension to Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 419 (1999). The cost of using a litigation support system is reduced dramatically if the documents are in electronic form from the start and do not need to be scanned. J. Roger Tamer, *Preparing for Electronic Discovery*, N.Y.L.J., Jan. 25, 1999, at S5.

[88] Note that cost-shifting is inappropriate for information that is already in electronic format, assuming that the material is not inaccessible. Keith Altman, *Putting the Brakes on Cost-Shifting*, 43 TRIAL 38, 39 (Apr. 2007).

information may allow for the opposing party to shift a substantial amount of the cost of production to the requesting party.[89] The court uses many of the same factors in this determination as in determining good cause,[90] and a determination can certainly go either way.[91] When requesting large amounts of information, it is imperative to keep in mind that you may end up having to pay for the cost of producing it. It is better to try to adequately access what is needed for the litigation and limit the discovery, possibly in an agreement under the Rule 26(f) Meet and Confer.[92]

Another consideration with respect to cost-shifting is the documents requested from non-parties to the litigation. It is important to be cautious in the amount of information requested

---

[89] *See e.g.*, Anti-Monopoly v. Hasbro, 1996 WL 22976 (S.D.N.Y. Jan. 23, 1996). The Plaintiff moved to compel production of electronic data at Hasbro's expense. The court ruled that the cost of the special programming needed to retrieve discoverable data should be borne by the plaintiff, as the "data did not exist in such a form as to exclude irrelevant and non-producible data."

[90] While the two possible tests used to be the *Rowe* eight-factor test and the *Zubulake* seven-factor test, the *Zubulake* balancing test became the standard later enshrined in FRCP Rule 26.

The two possible tests that courts have chosen to use under these circumstances. *See* In re Veeco Instruments, Inc. Securities Litigation, 2007 U.S. Dist. LEXIS 23926 (S.D.N.Y. April 2, 2007). Even though the court required the producer to bear the cost initially, the court gave the producer the opportunity to file an affidavit utilizing the seven *Zubulake* factors, after which the court would consider whether any costs should be shifted.

[91] *See* In re Brand Prescription Drugs Antitrust Litigation, 1995 WL 360525 (N.D. Ill. 1995). The court ordered Ciba-Geigy to produce all computer-stored email relevant to the case. Ciba had 30 million pages of email data stored on backup tapes, and had to develop a special program to extract the responsive data. The court ruled that the cost of this program was not the plaintiff's responsibility, but rather Ciba's as an ordinary and foreseeable risk of its business.

[92] Indeed, recent cases reveal that courts are emphasizing early planning strategies and agreement between parties involved in e-discovery. *See, e.g.*, Aguilar v. Immigration and Customs Enforcement Division, 255 F.R.D. 350, 355 (S.D.N.Y. 2008) (court stated that early agreement on ESI by the parties to that dispute might have avoided "court involvement or additional expense"); Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (plaintiff "miss[ed an] opportunity" in refusing to stipulate to a "search methodology" for the defendant's document searches because "plaintiff might have convinced [defendant] to broaden its search in ways that would uncover more responsive documents and avoid subsequent disputes").

from third parties. If the information is not reasonably accessible, even though the evidence might be crucial to the lawsuit, the court could very easily order cost-shifting, and the requesting party may have to incur the full cost of production if they cannot establish that the costs are *de minimis*.[93] The Court emphasizes that the encouragement of cooperation by non-parties in the future is important and should not be placed in jeopardy.[94] Consequently, the utmost cooperation should be promoted with any non-parties with whom discovery will be sought in order to lower the potential costs of production and reduce the risk that they will seek cost-shifting.

After the *Zubulake* decisions, a number of organizations began to propose guidelines addressing various issues of e-discovery, including those of cost-shifting and cost-allocation. Indeed, because of the complexity of the balancing tests used to determine cost-shifting and cost-allocation as well as the long-standing presumption against requiring a party to bear the costs of its own discovery requests, it has been argued that discussions of cost-shifting have proven more popular for discussion among scholars than among federal district court judges.[95] One proposed set of scholarly guidelines emerged from the Sedona Conference, which added an additional factor to the seven-factor *Zubulake* test and also arguably opens the way to cost-allocation for

---

[93] *See e.g.*, Guy Chemical Co., Inc., v. Romaco AG, 2007 U.S. Dist. LEXIS 37636, *7–8 (N.D. Ind. May 22, 2007) (ordering requesting party to pay for the costs associated with third party discovery).

[94] *Id.* at *7; *see also* William A. Gross Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co., 2009 WL 724954 (S.D.N.Y. Mar. 19, 2009) (where a non-party agreed to produce electronic documents but objected to search terms both parties proposed, the court issued a "wake-up call" to attorneys about the need to effectively design search terms used in e-discovery efforts and endorsed the 2008 "Cooperation Proclamation" from the Sedona Conference).

[95] *See* Martin H. Redish, *Back to the Future: Discovery Cost Allocation and Modern Procedural Theory*, Finding the Balance Between Benefit and Cost: A Public Policy Roundtable on the Federal Rules of Civil Procedure 14 (2010) (as-yet unpublished manuscript), *available at* http://www.law.northwestern.edu/searlecenter/uploads/Redish_McNamara_Discovery_Final.pdf.

accessible ESI.[96] Principle Thirteen (of the Sedona Conference's fourteen principles for e-discovery) "incorporates the seven *Zubulake* factors and states that the responding party should generally bear the costs of discovery except when the ESI demanded is not "reasonably available in the ordinary course of business."[97] The Sedona principles do not limit cost-shifting to inaccessible ESI, but rather endorse cost-shifting measures where the information might be accessible but the *volume* of information could be deemed disproportionate to the need.[98] Additionally, the Sedona Principles expand the meaning of "costs" to include privilege review costs and costs related to the disruption of business caused by production of electronically stored information.[99] Ultimately, the Sedona Principles take the approach that "whatever rule of cost-allocation a court adopts . . . it should not become an excuse to bypass the requirement, that discovery is only warranted when its usefulness to the litigation outweighs the burden it will cause to the responding party."[100]

IX. Getting Started

A. Issue a preservation letter

Electronic discovery should always begin with the issuance of a demand letter requesting the preservation of all relevant computer evidence. Sending a preservation letter when a lawsuit is imminent or has been served is critical to minimizing the loss of documents and data. This

---

[96] JOINT E-DISCOVERY SUBCOMMITTEE OF THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK, MANUAL FOR STATE TRIAL COURTS REGARDING ELECTRONIC DISCOVERY COST-ALLOCATION 36 (2009), *available at* http://www.nycbar.org/Publications/pdf/Manual_State_Trial_Courts_Condensed.pdf.

[97] *Id.* (citing *The Sedona Principles (Second Edition): Best Practices Recommendations & Principles for Addressing Electronic Document Production* ("*Sedona Principles*")).

[98] *Id.*

[99] *See id.*

[100] *Id.* at 36–37.

letter should suspend the defendant's document retention and destruction policy and put the defendant on notice that any destruction of documents from that point forward could result in spoliation claim.

An example of a preservation is attached hereto as "Attachment 1". If possible, the preservation letter should be specific and list the names of pertinent individuals, document formats such as e-mails, e-mail attachments, and native file formats. Document categories should be identified that include any specific reports and time periods. Most importantly, the preservation letter should request suspension of any corporate document destruction policies and preservation of the existing electronic data. The preservation letter should be sent even if intentional spoliation is unlikely.

B. Create a discovery plan.

Once a plan has been established, send out interrogatories and production requests to ascertain the types of relevant information and the form of the relevant information. You should also ascertain the computer network configuration, the software used, document retention policies, data backup and storage locations and who has control of the information. From this information a specific request for electronic information can be crafted.

Sample Interrogatories are attached to be used in discovery of electronic evidence.

Amongst the information which should be requested in your production requests are:

> – Electronic devices and equipment where relevant information may be stored such as servers, workstations, desktops, PCs, laptops, and mainframe computers.
> – Common servers may include databases, files, e-mail, network Internet/Web, print, fax proxy and application servers.
> – PDAs, pagers, telephones, voice mail, caller ID, and answering machine records, digital cameras, camcorders, GPS devices, CD duplicators, security systems, and vehicle computer devices (Black Boxes).
> – Devices and equipment used at businesses, homes, remote offices, portable or personal computers.

– Storage media such as fixed, removable, and external hard drives.
– Policies and systems such as document retention, deletions, archiving, back-up, disaster recovery, and legacy. Operating systems including software application programs for word processing, accounting, spreadsheets, reporting, communication files for voice based communications.
– Information from software program files, system history files, web site files including text, graphics, photos, audio databases, b logs, forums, and web site log files, cache files, and cookies.

Much of this information can be gathered from a productive and detailed Rule 26(f) Conference. Other topics for discussion should include the form of production of these documents and electronic information and procedures for the inadvertent disclosure of attorney work product and privileged materials.

C. Ascertain the Defendant Corporation document retention policies

Every corporation has a document retention (destruction) policy. This outlines a schedule for the destruction of corporate records. Some records must be preserved longer for tax purposes or requirements under Federal regulations. Other documents utility is minimized as time moves on. The concept of preserving documents for litigation actually runs contrary to the corporation's document destruction policies. Try to learn as much as possible about document retention policies either through the initial meet and confer under Rule 26(f) or at a Rule 30(b)(6) deposition of IT personnel.

D. Identify a consultant

Since we all know from our experience that all kinds of relevant information exists in electronic form, we should have an arrangement with specialists who can assist with organization of the information and forensics examination of the information.

Computer forensics deals with the collection, preservation, analysis and the presentation of computer related evidence. These consultants can conduct a search of the electronic data to

find those gems that will help prove our cases. The cost of most forensic evaluations should be borne by the requesting party, but keep in mind this cost can be shifted back to the producing party if it is shown that files were deleted.

The IT consultant should also be used to glean information about your own client's IT system. The attorney now has an obligation to ensure that everything is produced and preserved from their client, despite lack of computer knowledge.[101]

X. New Directions: The Seventh Circuit Electronic Discovery Pilot Program

A. Introduction

As technology continues to evolve, thus creating new areas of ambiguity in the area of e-discovery, various efforts have been underway to make sense of the issues surrounding the discoverability of electronically-stored information. One such effort was spearheaded by the Seventh Circuit Electronic Discovery Pilot Program Committee, who presented their findings in a 425-page report to the Seventh Circuit Bar Association on May 13, 2010. Judge James Holderman, who originally instituted the Seventh Circuit Electronic Discovery Committee, stated that the Committee is attempting to "develop[] procedures that enable the purposes of the Federal Rules of Civil Procedure to be achieved in the 21st century and make them work for the types of discovery that are necessary in litigation today."[102] This pilot program "was designed to develop and test principles aimed at decreasing the expense, burden, and time of e-discovery in modern litigation,"[103] and "signals the judiciary's interest in finding practical ways to change the

---

[101] Note that "computer illiteracy" is *not* a defense. *See* Martin v. Northwestern Mutual Life Insurance Company, 2006 WL 148991 (M.D. Fla. Jan. 19, 2006). The Magistrate rejected the attorney's excuse of "computer illiteracy" as "frankly ludicrous."

[102] Marc Gottridge, Frank T. Spano, Allison C. Stanton & Claudia Morgan, *Practical Principles for E-Discovery in the 21st Century: Phase One Results of the Seventh Circuit's Electronic Discovery Pilot Program*, DIGITAL DISCOVERY & E-EVIDENCE, May 13, 2010, at 2.

[103] *Id.*

adversarial assumptions litigators bring to the discovery program."[104]

B. The Principles

The Committee drafted the Pilot Program's Principles Relating to the Discovery of Electronically-Stored Information (ESI) in the summer of 2009, adopted them in September 2009, and put them into practice in October 2009. The Committee-defined purpose of the eleven Principles is to "incentivize early and informal information exchange on commonly encountered issues relating to evidence preservation and discovery, paper and electronic, as required by Rule 26(f)(2)"[105] with the hope of helping courts secure the "just, speedy, and inexpensive determination of every civil case, and to promote, whenever possible, the early resolution of disputes regarding the discovery of electronically stored information without court intervention."[106]

The Principles are based on two foundational standards: (1) cooperation[107] and (2) proportionality. The cooperative exchange of information between attorneys regarding evidence preservation and e-discovery is not simply encouraged in the Principles; this cooperation is enshrined as a rule in Principle 1.02 Cooperation. This principle states:

> An attorney's zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests

[104] Laura D. Cullison, *The Seventh Circuit's E-Discovery Pilot Program*, ABA COMMITTEE ON PRETRIAL PRAC. & DISCOVERY, Spring 2010, at 1.

[105] Gottridge, Spano, Stanton & Morgan, *supra* note 101, at 2.

[106] *Id.*; *see also* Principle 1.01 [Purpose]. The Principles, in total, cover Purpose (1.01), Cooperation (1.02), Discovery Proportionality (1.03), Duty to Meet and Confer on Discovery and to Identify Disputes for Early Resolution (2.01), E-Discovery Liaisons (2.02), Preservation Requests and Orders (2.03), Scope of Preservation (2.04), Identification of ESI (2.05), Production Format (2.06), and Education Principles (3.01 and 3.02). *See* Cullison, *supra* note 103, at 21–23.

[107] This call for cooperation was also proclaimed and strongly advocated in the Sedona Conference Corporation Proclamation. *See* Cullison, *supra* note 103, at 20.

and responses raises litigation costs and contributes to the risk of sanctions.[108]

While in the past it may have been assumed that zealous representation includes drafting a discovery request to ask for everything the other party may possess that may potentially lead to unearthing of relevant information, this principle makes it clear that that is no longer the case, nor is it the expectation. This principle clearly states that it is an expectation that counsel present "reasonably limited" discovery requests in order to better represent their clients by avoiding potential sanctions, raising costs, and delaying the progress of the litigation.

Principle 1.03 emphasizes the role of proportionality in discovery efforts—a theme that has long been present in the Federal Rules,[109] but somewhat difficult to define in the realm of electronic discovery. Principle 1.03 states

> The proportionality standard set forth in Fed. R. Civ. P. 26(b)(2)(C) should be applied in each case when formulating a discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as practicable.[110]

Thus, the standard of proportionality to be used in electronic discovery efforts has been defined as narrowing one's requests to be "targeted, clear, and specific."

C. Effects of Implementing the Principles

From October 2009 to May 2010, the aforementioned Principles were tested in ninety-three real cases in the Seventh Circuit by thirteen judges of the U.S. District Court for the Northern District of Illinois.[111] When a survey was administered in May 2010 to all thirteen

---

[108] Cullison, *supra* note 103, at 21.

[109] *See id.* at 20.

[110] *Id.* at 21.

[111] Gottridge, Spano, Stanton & Morgan, *supra* note 101, at 3.

judges and the 285 attorneys whose cases had been part of Phase One,[112] most respondents reported that they felt it was too early to gauge the effectiveness of the Principles, since at that point they had only been tested for five or six months.[113]

Additionally, there was considerable variation among judges and attorneys concerning their perceptions on the usefulness and effectiveness of some of the Principles. For example, while 84% of judges believed the Principles "increased of greatly increased the level of cooperation by counsel," only 34% of attorneys agreed. And while 92% of judges reported feeling that the Principles had a "positive effect on counsels' meaningfully attempting to resolve discovery disputes before requesting court involvement," only 39% of attorneys agreed.[114]

While there was considerable variation in survey responses, there were also some things upon which the judge and attorney respondents generally agreed. Both groups of respondents found the use of a discovery liaison to be useful and beneficial; both reported that they thought litigation costs were decreased or unaffected; and the majority also felt that the Principles had not in any way hindered the attorneys' abilities to zealously represent clients.[115]

D. Moving Forward: Phase Two

Phase Two of the Pilot Program is currently scheduled to run from July 1, 2010 to May 1, 2010, and will expand both the number of participating judges and cases and the geographic area within the Pilot Program.[116] As is evident from the responses in the surveys administered after Phase One of the Pilot Program, there is a great deal of variation among attorneys and judges

[112] Phase One took place between October 2009 and May 2010 and involved creating and testing the principles; Phase Two will begin in July 2010.

[113] Gottridge, Spano, Stanton & Morgan, *supra* note 101, at 3.

[114] *See* Gottridge, Spano, Stanton & Morgan, *supra* note 101, at 3.

[115] *Id.*

[116] *Id.*

about the perceived effectiveness of the Principles, and thus, room for improvement as testing moves into Phase Two. For example, the Committee has recommended that perhaps Principle 2.01 Duty to Meet and Confer, and Principle 2.05 Identification of ESI be revised and strengthened for Phase Two. While it is obviously unclear what the exact outcome of Phase Two of this Pilot Program will be, these Principles "ha[ve] implications for all civil matters in federal court," and represent an important step made by the Seventh Circuit towards outlining more practicable litigation and discovery strategies to accommodate for constantly-evolving technologies.

XI. Social Media & E-Discovery

Social media websites are growing in popularity and worldwide use by the day. Currently, there are 500 million active Facebook accounts and 145 million Twitter accounts.[117] This number is only predicted to grow. As more people using various forms of social media share more information on these sites, it will become even more crucial to understand the kinds of information that is being shared, who owns this information, and the various privacy issues that will arise with this new unprecedented growth in usage.

A. What Is Social Media and Why Social Media Tools Are Important

Social media has been defined as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."[118] These websites include such common names as Facebook, Twitter, MySpace, LinkedIn, and FourSquare, as well as the vast number of blogs that are now

---

[117] Posting of Natalie Sisson to Work In Progress, http://blogs.forbes.com/work-in-progress/2010/09/14/are-you-a-social-media-snob-or-a-non-believer/?boxes=Homepagechannels (Sept. 14, 2010, 11:33 EST).

[118] Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 2010 BUSINESS HORIZONS 53, 59.

available for public consumption. All of these sites share the common ground that they are built primarily on user-generated content that is shared publicly or with specifically chosen groups of individuals. Not only are there more types of social media outlets available by the day, but the amount of time the average consumer spends on these sites is also growing. For example, in August 2010—for the first time in history—internet users in the United States spent more time on Facebook than they spent on any other site on the internet.[119] Additionally, it is not just the age thirty-five and younger crowd that is using these social media outlets anymore. In fact, the demographic logging the most Facebook use behind the 26–34-year olds are 55-year-old women.[120] Additionally, as of September 2010, fifty-four percent of small and midsize businesses are using social media to promote their business or products, with thirty-five percent of those updating daily.[121] This figure has doubled since December 2009, marking a dramatic increase in the use of social media for business reasons.[122]

Why is this important? Because it means that more than likely your family members, your clients, your business partners, your golfing partner, your spouse, and your administrative staff are users of some form of social media. It also means that simply by virtue of more people being users of social media, that more information will be shared, and some of that information will be vital to litigation.

---

[119] Business Insider, Charts of the Week: Facebook Passes Google in Time Spent on Site for First Time Ever, http://www.businessinsider.com/charts-of-the-week-facebook-passes-google-in-time-spent-on-site-for-first-time-ever-2010-9#facebook-passes-google-in-time-spent-on-site-for-first-time-ever-3 (last visited Sept. 14, 2010).

[120] Posting of Natalie Sisson, *supra* note 116.

[121] Alison Diana, *Social Media Has Scorching Impact On Small Biz*, http://www.forbes.com/2010/09/14/social-media-facebook-linkedin-twitter-entrepreneurs-technology-informationweeksmb-growth-lessons-10.html?boxes=entrepreneurschannelinentre (last visited Sept. 14, 2010).

[122] *Id.*

B. The Information on Social Media, and Why It Might Be the Focus of Discovery

Indeed, as social media grows in popularity, "attorneys are utilizing these services in both criminal and civil litigation."[123] What information are attorneys finding on these sites that has become so useful in litigation? Well, for example, on sites like Facebook, users create a personal page, often times listing their names, location, schools attended, place of employment, and other friends. Users can also update their locations and share those locations with friends, and can also post status updates detailing what they're doing and who they're with. Thus, "more and more attorneys use these rich archives of personal information to investigate the backgrounds of parties, witnesses, opposing counsel, jurors, and even judges."[124] It has been shown that a great number of social media users are "shockingly candid"[125] when posting personal information on social media sites, including information about their drinking, drug use, and sex lives. This information, in turn, can be used to gauge how a judge or jury might respond to a witness or an expert in a jury. Additionally, attorneys can use information on social media websites to corroborate or undermine a plaintiff's case.[126] For example, a teenager in a forcible rape case in Oregon claimed that she would never willingly have sex, only to have the defense attorney discover information on her MySpace page detailing the parties she attended, her drinking habits, and her discussions about "getting some." These self-proclamations obviously had an impact on her credibility as a witness, and the grand jury ultimately dismissed the charge.[127]

---

[123] Sean P. O'Donnell, *The Use of Information Posted on Facebook and MySpace in Litigation*, Subrogation and Recovery Alert, Oct. 19, 2009, *available at* http://www.cozen.com/cozendocs/outgoing/alerts/2009/subro101409.pdf.

[124] Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B.J. 366, 366 (2010).

[125] *Id.* at 367.

[126] O'Donnell, *supra* note 122.

[127] Boggs & Edwards, *supra* note 123, at 367.

Because this information is proving to be useful in so many different (and sometimes unexpected) ways, attorneys are more frequently filing discovery motions to obtain information found on social media sites. While there does not appear to be entirely consistent case law or opinion regarding the extent to which this information is discoverable, ultimately "most courts have allowed discovery of relevant information posted to Facebook and other sites."[128] Still, it is difficult to establish consensus regarding the rules of social media and discoverability because the format of social media is always changing, and rules have simply not evolved quickly enough to govern the new information.

In the case of *Mackelprang v. Fidelity National Title Agency*, the district court of Nevada denied the defendant's motion to compel e-mail communications that may have contained evidence of whether the plaintiff had engaged in consensual sexual activities from the plaintiff's MySpace because the defendant could only speculate about the persons with whom the plaintiff could have exchanged messages or the content of those hypothetical messages.[129] Thus, in that case, the court required something more concrete than what it seemed to be mere speculation about the possibility of incriminating e-mails sent on social media and the potential nature of those e-mails, but that court did allow "discovery of any e-mail communications relevant to assessing the credibility of [the plaintiff's] emotional distress claims."[130]

In comparison, in the case of *Crispin v. Christian Audigier, Inc. et al.*, a federal court in California did not allow any discovery of any private e-mail messages from social media sites regarding an alleged breach of contract.[131] The result turned out differently in the case of *Beye v.*

---

[128] *Id.*

[129] 2007 WL 119149, at *2 (D. Nev. 2007).

[130] Boggs & Edwards, *supra* note 123, at 368.

[131] Order Granting Plaintiff's Motion for Review of Magistrate Judge's Decision Re Plaintiff's

Horizon Blue Cross Blue Shield of New Jersey.[132] In that case, the plaintiffs contended that Blue Cross Blue Shield wrongfully denied coverage of their children's eating disorders, and the court ordered the plaintiffs to turn over their children's MySpace and Facebook pages because there was a "lower expectation of privacy where the person asserting the privacy right might make the information public in the first place."[133] Ultimately, the decision of the court to allow discovery of social media information appears to turn on whether the requested information is particularized and relevant.[134]

C. The Effect of *Quon*: Who Owns and Controls Social Media Information

While the case law on the discoverability of information on social media remains unsettled as these technologies continue to evolve, a recent Supreme Court decision helps to shed light on who may be deemed to own and control social media information. In *Ontario v. Quon*, the Supreme Court held that a public employer's search of an employee's employer-issued pager for sexually explicit text messages did not constitute an illegal invasion of privacy.[135] The city of Ontario, California acquired twenty alphanumeric pagers that were capable of sending and receiving limited text messages, intended to be used by SWAT members when mobilizing and

---

Motion to Quash Subpoena, No. 09-09509 (C.D. Cal. 2010), *available at* http://lawyersusaonline.com/wp-files/pdfs-2/crispin-v-christian-audigier-inc.pdf.

[132] 568 F. Supp. 2d 556 (D.N.J. 2008).

[133] Boggs & Edwards, *supra* note 123, at 368.

[134] *Compare* Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018, at *2) (court allowed discovery of information from Facebook and MySpace where the plaintiffs put relevant and confidential facts in issue and the request was "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case") *with* TV v. Union Township Board of Education, UNN-L-4479-04 (N.J. Super. Ct. App. Div. Dec. 22, 2004) (court denied access to a plaintiff's Facebook and MySpace pages because the student's privacy interests prevailed absent a particularized showing of relevance).

[135] 560 U.S. ____ (2010), *available at* http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf.

responding to emergencies. Before these pagers were issued to employees, the City announced a "Computer Usage, Internet and E-Mail Policy," specifying that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." Even though this policy did not apply, on its face, to text messages, the City made it clear that it would be treating e-mails and text messages the same way. After Quon exceeded the allowed character limit on his pager multiple times, transcripts were requested of his text messages, and the lieutenant responsible for facilitating contact with the technology company hosting the pager communications discovered that many of Quon's text messages were sexual in nature.[136] The Court assumed arguendo that:

> First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the Fourth Amendment; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.[137]

The Court concluded that a government employer's warrantless search is reasonable if it is "justified at its inception" and if "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" the circumstances giving rise to the search if done for a "non-investigatory, work-related purpose" or for the "investigation of work-related misconduct."[138] However, even while this holding sheds light on the expectation of privacy government employees might have while using government employer-issued technology for personal communications, the opinion goes out of its way to decide the case on very narrow

---

[136] *See id.* at *2–*4.

[137] *Id.* at *12.

[138] *Id.*

grounds, stating that "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[139] Thus, the Court appeared hesitant to arrive at a holding that could definitively be used by future courts when these cases arise in the future, even going so far as declining to decide which of two competing standards would apply in this case because a review of Quon's text messages would be reasonable under either.[140]

While this case obviously does not deal directly with social media sites like Facebook or MySpace, its implications have consequences for the discoverability of that information as well. For example, it is not difficult to imagine that the Court might also hold that information posted to Facebook by a government employee while using government-owned computers would be accessible to employer searches, provided that a technology policy like the one in *Quon* was in place. At the least, the case appears to imply that while at work and using government-owned equipment, government employees should expect that any information they post on social media sites might be accessible by their government employer. However, would the situation be different if the government employee was using a personal cell phone? What if they were using the government-owned computer on their lunch break, or at another time during which they were "off the clock"? What if part of the employee's job is to publicize information about their employer on a site like Facebook in order to promote certain employer agendas—would that employee's personal information on the site also be accessible? These questions remain unanswered, and will surely be the subject of future cases concerning information shared on social media.

---

[139] *Id.* at *10.

[140] *See id.* at *16.

D. Policies Companies Should Follow Regarding Social Media

While the Supreme Court may not have arrived at the broadest or most widely applicable holding in *Quon*, it did very significantly provide some considerations that might factor into future determinations of reasonable expectations of privacy in the workplace. These include:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. *And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.*[141]

That the Supreme Court would specifically state that employer policies will shape the reasonable expectations of privacy enjoyed by employees is very significant; it signals that in the future, the Court will most assuredly be looking at the specifics of employer's policies regarding employee use of technology, and the extent to which those policies have been articulated and enforced with uniformity and consistency. This, then, underscores the importance of employers having policies dealing with social media.

After the *Quon* decision, it is clear that in order to maximize the chances that an employer's monitoring of employee communications will be determined reasonable and will not result in liability, the employer should enact a written technology policy that covers as many forms of technology as the employer finds relevant to monitor without appearing too invasive. In particular, the policy should specifically state that the employees should have no expectation of privacy when they are using employer-owned technology or property. This policy, once enacted, should then be clearly conveyed to all employees who use or have access to that

[141] *Id.* at *11 (emphasis added).

particular technology. Also like in *Quon*, this policy should then be conveyed and reviewed with employees in a meeting at which the policy can be fully explained, any ambiguities might be cleared up, and the employees could then sign an acknowledgment that they have read and understand the technology policy as it applies to them and their work for the employer. It will then be important for all supervisors to enforce the technology policy with consistency, fairness, and uniformity, in order to avoid undermining the policy or creating any impression amongst the employees that it might not be enforced. And lastly, any monitoring or searching of employer-owned equipment or technology should be limited in scope and tied to an articulable and legitimate "work-related" purpose.

XII. Conclusion

As the technological world keeps evolving, the courts have struggled to keep up the pace. While the new rules have attempted to simplify the discovery process with new procedures and standards, complications are nevertheless inevitable. However, many of them can be avoided simply through knowledge and cooperation. The more that an attorney knows about his own client's IT systems, the more powerful he can be to push the opposing party to do the same. In this modern age, the court is no longer accepting computer ignorance as an excuse for discovery failures or delays. In addition, when it comes to electronic discovery, contention between parties seldom can result in a benefit. In fact, if a party institutes stall tactics and an unwillingness to cooperate, harsh sanctions can result. In this new age of electronic discovery, it is most advantageous to be prepared with an expert IT consultant and a cooperative attitude, thereby ensuring the best result for your client.