"MISSION IMPOSSIBLE" -- THE DUTY TO PRESERVE EVIDENCE EVEN WHEN MESSAGES SELF-DESTRUCT IN FIVE SECONDS (ETHICS)

GROUP ONE - FAIRCHILD INN OF COURT[1]

October 9, 2013

Law and Ethics Outline

I. Selected excerpts regarding Maintenance and Preservation of Evidence fromSCR Chapter 20 Rules Of Professional Conduct For Attorneys

SCR 20:1.2 Scope of representation and allocation of authority between lawyer and client

(d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

SCR 20:Rule 1.6 Confidentiality

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in pars. (b) and (c).

(b) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal or fraudulent act that the lawyer reasonably believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interest or property of another.

(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably likely death or substantial bodily harm;

(2) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(3) to secure legal advice about the lawyer's conduct under these rules;

[1] This outline represents the combined efforts of Attorneys David Peterson, Melissa Blair, Joseph Wall and Charles Blumenfield.

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(5) to comply with other law or a court order.

SCR 20:2.1 Advisor

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social, and political factors that may be relevant to the client's situation.

SCR 20:3.3 Candor toward the tribunal

(a) A lawyer shall not knowingly:

(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging, or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in pars. (a) and (b) apply even if compliance requires disclosure of information otherwise protected by SCR 20:1.6.

SCR 20:3.4 Fairness to opposing party and counsel

A lawyer shall not:

(a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;

...

(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party;

ABA COMMENT

[1] The procedure of the adversary system contemplates that the evidence in a case is to be marshalled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.

[2] Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. Paragraph (a) applies to evidentiary material generally, including computerized information. Applicable law may permit a lawyer to take temporary possession of physical evidence of client crimes for the purpose of conducting a limited examination that will not alter or destroy material characteristics of the evidence. In such a case, applicable law may require the lawyer to turn the evidence over to the police or other prosecuting authority, depending on the circumstances.

SCR 20:5.1 Responsibilities of partners, managers, and supervisory lawyers

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

(1)the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2)the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

SCR 20:5.3 Responsibilities regarding nonlawyer assistants

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1)the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
(2)the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

SCR 20: Rule 8.4 Misconduct

It is professional misconduct for a lawyer to:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;

(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

(d) state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law;

(e) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law; or

(f) violate a statute, supreme court rule, supreme court order or supreme court decision regulating the conduct of lawyers;

(g) violate the attorney's oath;

(h) fail to cooperate in the investigation of a grievance filed with the office of lawyer regulation as required by SCR 21.15(4), SCR 22.001(9)(b), SCR 22.03(2), SCR 22.03(6), or SCR 22.04(1); or

(i) harass a person on the basis of sex, race, age, creed, religion, color, national origin, disability, sexual preference or marital status in connection with the lawyer's professional activities. Legitimate advocacy respecting the foregoing factors does not violate par. (i).

II. E-Discovery Statutes in Wisconsin

For an excellent review of the recent changes to the Wisconsin electronic discovery statues see the July 2010 Wisconsin Lawyer article "*What You Need to Know - New Electronic Discovery Rules*" by Richard J. Sankovitz, Jay E. Grenig & William C. Gleisner III.

"The first duty of discovering attorneys is simply to recognize that it may be malpractice not to take careful account of the probability that much of the evidence the client needs access to for litigation may reside on an adversary's computer system."

Wis. Stat. § 802.10(3)(jm): Court management of electronic discovery; appointment of referees with special expertise. New Wis. Stat. section 802.10(3)(jm) adds the following to the list of issues a circuit court may address in issuing a scheduling order: "The need for discovery of electronically stored information."

Under Wis. Stat. § 805.06, the court may also appoint a referee to report on complex and/or expensive discovery issues, including those involving electronically stored information."

Wis. Stat. Section 804.01(4m): New "meet-and-confer" obligation.

Wis. Stat. Section 804.08(3): Producing electronic business records in lieu of an answer to an interrogatory.

Wis. Stat. Section 804.09(1) & (2):

Wis. Stat. § 804.09(1) & (2): Production of documents and things and entry upon land for inspection and other purposes.

(1) SCOPE. A party may serve on any other party a request within the scope of s. 804.01 (2): a) to produce and permit the requesting party or its representative to inspect, copy, test or sample the following items in the responding party's possession, custody, or control: 1. any designated documents or electronically stored information, including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any other medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form;...

(2)(a) ...The request may specify the form or forms in which electronically stored information is to be produced.

> Judicial Council Note, 2010: Sections 804.09 (1) and (2) are modeled on F.R.C.P. 34(a) and (b). Portions of the Committee Note of the federal Advisory Committee on Civil Rules are pertinent to the scope and purpose of s. 804.09 (1) and (2): Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. A Rule 34 request for production of "documents" should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and "documents." (Emphasis supplied)

Preservation Responsibilities. Preservation responsibilities are different from production responsibilities. A party may have legitimate objections to production, based on privilege or trade secrets, but that does not excuse the duty to preserve.

The duty to preserve documents in the face of pending or threatening litigation is not a passive obligation; it must be discharged actively. It rests on the shoulders of both attorneys and senior corporate officers. Attorneys for a business or governmental agency must take steps to learn of a client's file system and document-retention policies as soon as it is reasonably clear that litigation is probable and must be prepared to impose a "litigation hold" on the activities of a computer system so as to prevent the loss of any relevant data. A written preservation plan is crucial to avoid criticism for failing to preserve data. Attorneys must supervise the litigation hold to ensure compliance.

Wis. Stat. Section 804.12(4m): "Safe harbor" for routine deletion of electronically stored information.

The new rules immunize a party from spoliation sanctions if the information that is deleted or otherwise destroyed was done so as the result of the routine operation of the computer system.

III. Selected Federal Case Law

A. *Duty to preserve and maintain evidence and the challenges that this duty can impose.*

1. Fed. R. Civ. P. 37(b)(2)(A) permits sanctions when a party's officer, director or managing agent—or a witness designated under Fed. R. Civ. P. 30(b)(6) or 31(a)(4)—fails to obey an order to provide or permit discovery, including an order under Fed R. Civ. P. 26(f), 35, or 37(a). This Rule provides:

   (2) *Sanctions in the District Where the Action Is Pending.*

(A) *For Not Obeying a Discovery Order.* If a party or a party's officer, director, or managing agent—or a witness designated under Rule 30(b)(6) or 31(a)(4)—fails to obey an order to provide or permit discovery, including an order under Rule 26(f),35, or 37(a), the court where the action is pending may issue further just orders. They may include the following:

(i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;

(ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;

(iii) striking pleadings in whole or in part;

(iv) staying further proceedings until the order is obeyed;

(v) dismissing the action or proceeding in whole or in part;

(vi) rendering a default judgment against the disobedient party; or

(vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

2. If a court determines that a person or organization did not preserve evidence in the face of reasonably foreseeable litigation, the court has considerable discretion to award sanctions on a case-by-case basis. *Fujitsu Ltd. v. Federal Exp. Corp.*, 247 F.3d 423, 436 (2d Cir. 2001).

3. In a diversity case, federal courts generally apply federal rules as opposed to a state's spoliation laws. *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 611 (S.D. Tex. 2010). *But see State Farm Fire & Cas. Co. v. Frigidaire, a Div. of General Motors Corp.*, 146 F.R.D. 160, 161-62 (N.D. Ill. 1992) (spoliation sanctions are substantive rather than procedural and the relevant state's law should be applied).

4. "A party seeking sanctions for spoliation of evidence must establish: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a 'culpable state of mind' and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." *Passlogix, Inc. v. 2FA Technology, LLC*, 708 F. Supp. 2d 378, 409 (S.D.N.Y. 2010) (citations omitted).

5. Courts generally have identified three key factors as to whether and to what extent to award sanctions: (1) the degree of fault of the party who destroyed the evidence; (2) the degree of prejudice to the opposing party; and (3) whether a lesser sanction will avoid substantial unfairness to the opposing party, and whether a sanction will deter future conduct. *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S.D. Tex. 2010); *Philip M. Adams & Associates, LLC v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1192 (D. Utah 2009).

6. "The question of prejudice 'turns largely' on whether a spoliating party destroyed evidence in bad faith." *Micron Technology, Inc. v. Rambus Inc.*, 917 F. Supp. 2d 300, 319 (D. Del. 2013).

7. Generally, "[a] litigant has a duty to preserve evidence that he knows or should know is relevant to imminent or ongoing litigation." *Jordan F. Miller Corp. v. Mid-Continent Aircraft Service, Inc.*, 1998 WL 68879, *5 (10th Cir. 1998).

8. "The broad contours of the duty to preserve are relatively clear. That duty should certainly extend to any documents or tangible things (as defined by Rule 34(a)) made by individuals 'likely to have discoverable information that the disclosing party may use to support its claims or defenses.' The duty also includes documents prepared *for* those individuals, to the extent those documents can be readily identified (*e.g.*, from the 'to' field in e-mails). The duty also extends to information that is relevant to the claims or defenses of *any* party, or which is 'relevant to the subject matter involved in the action.' Thus, the duty to preserve extends to those employees likely to have relevant information-the 'key players' in the case." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) (citations omitted)

9. Although a litigant is "under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request," a litigant is not required to keep every piece of paper, every electronic document, and every back-up tape. *Concord Boat Corp. v. Brunswick Corp.*, 1997 WL 33352759, *4 (E.D. Ark. 1997).

10. In *Phillip M. Adams & Associates, L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1180 (D. Utah 2009), the defendant's email preservation system that consisted of instructing employees to preserve email on their computers, coupled with "very little evidence compared to what would be expected," led the court to conclude that the "safe harbor" of Federal Rule of Civil Procedure 37(e) did not apply, and that the defendant should be sanctioned for spoliation. Defendant's practice of having employees archive email was not "good faith" evidence of defendant's data management practices.

11. In *Brigham Young University v. Pfizer, Inc.*, 282 F.R.D. 566, 572 (D. Utah 2012), the court rejected reliance on the *Adams* case and clarified that organizations do not need to preserve information until litigation is "reasonably anticipated." This case is significant for the following findings: (1) organizations are not required to keep electronically stored information until the duty to preserve is reasonably anticipated; (2) organizations can and should use document retention protocols to rid themselves of data stockpiles; (3) the holding of the *Adams* case is narrowed to its particular facts; and (4) organizations will be protected from sanctions to the extent they destroy electronically stored information in good faith pursuant to a reasonable retention policy.

B. *The challenges of finding, preserving, and litigating production of relevant evidence in the face of:*

1. Corporate records retention policies and today's technologies, including:

    a. Self-destructing "snapchat.com" photos and
    b. Evanescent Instagram and text messages and
    c. Social media postings.

    A. Social media content is subject to the standard rules of discovery governing all electronically stored information, notwithstanding whether such media is "locked" or "private." *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).

    B. See also http://technology.findlaw.com/modern-law-practice/ediscovery-rules-applied-to-social-media-what-this-means-in.html

2. Client legal duties to retain records

    a. Lawyer suspended for 5 years for advising client to clean up Facebook photos http://www.vsb.org/docs/Murray-092513.pdf

    b. Cincinnati defense attorney indicted for advising clients to "destroy the SIM" 8/22/13. Her attorney claims lawyers are exempt from obstruction of justice statutes when advising clients:

        "*We believe she was doing her job as an attorney and when we do that we are exempt from obstruction of justice charges*," said attorney Peter Rosenwald.
        http://www.wlwt.com/news/local-news/cincinnati/wife-of-sheriff-candidate-indicted-in-cell-phone-obstruction-scheme/-/13549970/21576872/-/lssany/-/index.html

c. Lawyer destroys church music director's laptop; charged with Sarbanes-Oxley violation; convicted of misprision of a felony and sentenced to 6 months house arrest, $25,000 fine, and community service. Laptop contained child pornography; lost, then regained law license following suspension. http://usatoday30.usatoday.com/news/nation/2007-12-17-1170752970_x.htm

[See also ABA Journal article appended at end of outline, also available here: http://www.abajournal.com/news/article/ct_case_sarbanes_v_attorney_et..]

C. *Legal and ethical duties of attorneys to advise clients to preserve evidence.*

1. In *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. 2008), the court ordered Qualcomm to pay $8.6 million in sanctions, finding that Qualcomm deliberately withheld 50,000 documents from discovery in a patent dispute. The court also sanctioned six of its attorneys and asked the California state bar to investigate them for failing to conduct a reasonable inquiry into the adequacy of Qualcomm's document production. Although the sanctions award ultimately was reversed, the reversing court admonished the attorneys for a breakdown in communication with their client during the discovery process, failing to meet with the appropriate employees involved in the lawsuit, and the failure to determine where the data was stored.

2. If an attorney is using keyword searches for retrieval of electronically stored information, it is the attorney's duty to ask key custodians of documents for their input regarding search terms used to identify relevant documents to appropriately discuss document collection. As one court stated: "It is time that the Bar - even those lawyers who did not come of age in the computer era - understand this." *William A. Gross Const. Associates, Inc. v. American Mfrs. Mut. Ins. Co.*, 256 F.R.D. 134, 136 (S.D.N.Y. 2009).

IV. Selected Wisconsin Spoliation Cases

A. *Jagmin v. Simonds Abrasive Co.*, 61 Wis. 2d 60, 211 N.W.2d 810 (1973).

Products liability case where defendant could not produce allegedly defective wheel. "The court believes it must reiterate that the mere fact that evidence in this case may or may not have been lost, does not create an inference of impropriety on the part of the defendant." Trial court was correct in finding that the plaintiff had not proven to a reasonable certainty by evidence which was clear, satisfactory and convincing that the defendant intentionally destroyed or fabricated evidence by substituting a second wheel. The spoliation instruction is "reserved for deliberate, intentional actions and not mere negligence even though the result may be the same as regards the person who desires the evidence."

B. *Milwaukee Constructors II v. Milwaukee Metro. Sewerage Dist.,* 177 Wis. 2d 523, 502 N.W.2d 881 (Ct. App. 1997).

During discovery, plaintiff revealed that boxes of documents were destroyed as the company reduced the inventory of old or obsolete files in storage. At the time of the purging, the company was aware that it would bring a lawsuit against the defendant. Citing to *Struthers Patent Corp v. Nestle Co.*, a D.N.J. case, the trial court laid out a five-step process for evaluating an allegation concerning document destruction:

1. Identification of documents destroyed
2. Relationship of the documents to the issues in the action
3. Extent to which such documents can be obtained from other sources
4. Whether the party responsible for the destruction knew, or should have known, that at the time of the destruction litigation was a distinct possibility, and
5. Whether, in light of the circumstances disclosed by the factual inquiry, sanctions should be imposed and if so, what the sanctions should be.

The trial court imposed dismissal as a sanction for the destruction. The appellate court reversed, stating that there was no evidence that the plaintiff purposefully sought to impair the defendant's ability to discover information. The plaintiff's conduct was volitional and negligent, but this did not rise to the level of egregiousness that warrants dismissal. Court of Appeals stated dismissal is a sanction that should rarely be granted and is appropriate only in cases of egregious conduct.

C. *Garfoot v. Fireman's Fund Ins. Co.*, 228 Wis. 2d 707, 599 N.W.2d 411 (Ct. App. 1999)

Plaintiff injured when propane tank exploded. When plaintiff's attorney conducted an inspection of the explosion site, technician disconnected and then reconnected joints leading to the gas pipes and in doing so prevented further testing to see if these joints had leaked and caused the explosion. Defendant moved for sanctions against plaintiff for spoliation of evidence and trial court granted, dismissing the case based on a finding of negligence on the part of plaintiff's attorney/agents.

Court of appeals reversed, holding that dismissal was not proper sanction where party's conduct in destroying evidence was not egregious but merely negligent. Court of Appeals held that: "[D]ismissal as a sanction for destruction/[spoliation] of evidence requires a finding of egregious conduct, which, in this context, consists of a conspicuous attempt to affect the outcome of the litigation or a flagrant knowing disregard for the judicial process.

D. *Estate of Neumann v. Neumann*, 2001 WI App 61, 626 N.W.2d 821.

Defendant destroyed evidence, a gun used in the homicide of defendant's wife. Trial court issued a destruction of evidence jury instruction. Defendant argued that the instruction was inappropriate because defendant was not a party at the time of the

destruction. In this case, unlike *Jagmin*, the plaintiff presented clear, satisfactory and convincing evidence that the defendant destroyed the relevant evidence. The court rejected the argument that the destruction was not committed in the court of litigation, because in some circumstances the remedies for spoliation of evidence are available even when litigation has not yet commenced.

A spoliation inference is appropriate if the party fails to preserve property for another's use as evidence in pending or reasonable foreseeable litigation. Where the "spoliation inference" is applied the trier of fact is allowed to infer that the evidence that was destroyed was unfavorable to the party who destroyed it. Defendant knew or should have known he was interfering with potential civil and criminal litigation. It is further undisputed that the destruction of evidence interfered with law enforcement's investigation, the estate's case, and the defendant's own defense. *Neumann* summarized that Wisconsin Courts have recognized the following three remedies for spoliation:

> 1. pre-trial discovery sanctions (citing *Sentry Ins. v. Royal Ins. Co.*, 196 Wis. 2d 907, 918-19, 539 N.W.2d 911 (Wis. Ct. App. 1995) (upholding exclusion of evidence as a sanction);
> 2. the spoliation inference (citing *Jagmin v. Simonds Abrasive Co.*, 61 Wis. 2d 60, 80-81, 211 N.W.2d 810 (1973) (recognizing that the spoliation inference may be appropriate where evidence was intentionally destroyed, but not where negligently destroyed); and
> 3. dismissal (citing *Garfoot*, 228 Wis. 2d at 724 (dismissal requires a finding of egregious conduct).

E. *Ins. Co. of N. Amer. v. Cease Elec. Inc.*, 2004 WI App 15, 674 N.W.2d 886.

Cold Spring's ventilation system failed, resulting in the death of chickens. Cold Spring rewired the barn to save the remaining birds and did not find out until a week later that the backup thermostat was improperly wired. Cold Spring misplaced the backup thermostat and had the barn rewired without documenting the mis-wiring. Not all destruction, alteration or loss of evidence qualifies as spoliation. At the time of destruction, Cold Spring had no reason to foresee litigation or believe that the evidence would be relevant to such litigation. Trial court should consider whether the party knew, or should have known, at the time of destruction that litigation was a distinct possibility and whether the party knew, or should have known, that the evidence would be relevant to such litigation.

F. *Harris v. Menard, Inc.*, 2005 WI App 214, 704 N.W.2d 423.

Woman tripped over a pallet at a Menards. A written incident report was made but lost. Trial court issued a spoliation instruction. Trial court has wide discretion in fashioning jury instructions and they will be upheld so long as they are not erroneous and adequately inform the jury of the law to be applied. Parties disputed what showing must be made before the jury can be instructed on spoliation. The appellate court held that plaintiff must show clear and convincing evidence of intentional destruction. The plaintiff

satisfied the standard. Menard's did not claim to have lost the report, but stated it was never written. However, an affidavit included direct quotations of statements attributed to the report. This was determined to be clear and convincing evidence that Menard's had the report at some point during discovery and intentionally failed to turn it over.

G. *Morrison v. Rankin*, 2007 WI App 186, 305 Wis. 2d 240, 738 N.W.2d 588.

In order to determine whether a party has engaged in spoliation, Wisconsin courts must find:

> (1) that the party responsible for the destruction of evidence knew or should have known at the time it destroyed the evidence that litigation was a "distinct possibility"; and
> (2) that the party destroyed evidence which it knew or should have known would constitute relevant evidence in the pending or potential litigation.

Dismissal is available as a sanction for spoliation but only where the party responsible for the destruction has acted egregiously or in bad faith. When the destroying party has acted egregiously or in bad faith, the court may impose the sanction of dismissal, even if the destruction of evidence did not impair the opposing party's ability to present a claim or defense.

H. *Amer. Family Mut. Ins. Co. v. Golke,* 2009 WI 81, 768 N.W.2d 729.

Trial court dismissed the action for spoliation of evidence – house which was allegedly negligently repaired by roofers, after catching fire was razed and rebuilt. Pictures were taken, but physical evidence from the fire was not preserved. Supreme Court addressed the following issues:

> (1) When does a party or potential litigant discharge its duty to preserve evidence relevant to a potential legal claim;
> (2) Can sufficient notice be effectuated by the mailing of a letter via first-class mail; and
> (3) When is dismissal an appropriate sanction for spoliation of evidence?

The Court held that the duty to preserve relevant evidence is discharged when a party or potential litigant with a legitimate reason to destroy evidence provides reasonable notice of a possible claim, the basis for that claim, the existence of evidence relevant to the claim, and a reasonable opportunity to inspect that evidence. The Court further held that such notice can be properly effectuated by mailing a letter via first-class mail. The Court also affirmed that dismissal is an appropriate sanction for spoliation of evidence only if a party acts egregiously—that is, in a conscious effort to affect the outcome of litigation or in flagrant, knowing disregard of the judicial process.

I. *Maciolek v. Ross*, 2010 WI App 1, 778 N.W.2d 171.

Trial court refused to give a spoliation instruction regarding notes taken summarizing conversations with the defendant. After the lawsuit began, an employee of plaintiff compiled a summary of the notes into one document prepared on her computer and disposed of the actual notes. Trial court's denial of the requested spoliation instruction was upheld because the defendant failed to provide clear, satisfactory and convincing evidence that plaintiff intentionally destroyed or fabricated evidence. In any event, any error was harmless because defendant was still permitted to argue that the missing notes damaged the plaintiff's case.

J. *S.C. Johnson & Son, Inc. v. Morris*, 2010 WI App 6, 779 N.W.2d 19.

Issue for appeal: whether trial court gave a "draconian spoliation instruction." Trial court decided that there was clear and convincing evidence, almost overwhelming inference to be drawn that the original bank ledgers were intentionally destroyed at some point when their importance and significance to contemplated or pending litigation would have been known. Appellate court noted that the party that destroyed the documents did not know why they were missing and made inconsistent statements as to why documentation was missing. Appellate court held that defendant did not meet its burden of proving why the trial court's inference was unreasonable.

K. *Cody v. Target Corp.*, 2013 WI App 94, 2011AP2831 (June 27, 2013).

Target destroyed evidence consisting of an air mattress box that personal injury plaintiff had returned to the store. Plaintiff contended the box had been sold by Target with noxious ant and roach poison in it instead of the Eddie Bauer air mattress it was supposed to have in it. Plaintiff alleged that a day or two after returning the box members of her family became ill. She called the store to complain and a customer service person made notes about the call and her complaints, noting she was very upset. Some days after that call, the store loss prevention manager placed the box in a return goods chargeback area, and afterwards Target disposed of the box and its contents.

The trial court determined that the box was destroyed at a time when Target should have been aware that litigation was a distinct possibility and that the box was relevant to that potential litigation. Because of the spoliation, the trial court imposed a discovery sanction of taking away any defense causation argument. The trial court also dismissed all co-defendants, leaving Target as the only defendant. The Court of Appeals affirmed, and held that a finding of egregious conduct was not a prerequisite for entering this form of statutory discovery sanction, and that the sanction was appropriate given the circumstances. A petition for review has been filed.

V. Additional Wisconsin Statutes of Significance

A. *Wisconsin Statute Regarding Electronically Stored Information:*

Wis. Stat. § 804.12(4m) - Failure to provide electronically stored information.

> Absent 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. *See also* Fed. R. Civ. P. 37(e).
>
> **Advisory Committee Note**
>
> The published rule barred sanctions only if the party who lost electronically stored information took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action. . . . The present proposal establishes an intermediate standard, protecting against sanctions if the information was lost in the "good faith" operation of an electronic information system. The present proposal carries forward a related element that was a central part of the published proposal—the information must have been lost in the system's "routine operation." ...
>
> The change to a good-faith standard is accompanied by addition of a provision that permits sanctions for loss of information in good- faith routine operation in "exceptional circumstances." This provision recognizes that in some circumstances a court should provide remedies to protect an entirely innocent party requesting discovery against serious prejudice arising from the loss of potentially important information.

B. *Wisconsin Statutes Regarding Obstruction of Justice and Computer Crimes:*

Wis. Stat. § 946.60 Destruction of documents subject to subpoena.

> (1) Whoever intentionally destroys, alters, mutilates, conceals, removes, withholds or transfers possession of a document, knowing that the document has been subpoenaed by a court or by or at the request of a district attorney or the attorney general, is guilty of a Class I felony.
>
> (2) Whoever uses force, threat, intimidation or deception, with intent to cause or induce another person to destroy, alter, mutilate, conceal, remove, withhold or transfer possession of a subpoenaed document, knowing that the document has been subpoenaed by a court or by or at the request of a district attorney or the attorney general, is guilty of a Class I felony.

(3) It is not a defense to a prosecution under this section that:

(a) The document would have been legally privileged or inadmissible in evidence.
(b) The subpoena was directed to a person other than the defendant.

Wis. Stat. § 946.65 Obstructing justice.

(1) Whoever for a consideration knowingly gives false information to any officer of any court with intent to influence the officer in the performance of official functions is guilty of a Class I felony.

(2) "Officer of any court" includes the judge, reporter, bailiff and district attorney.

Only conduct that involves a 3rd-party contracting with another to give false information to a court officer in an attempt to influence the performance of the officer's official function is proscribed by this section. State v. Howell, 141 Wis. 2d 58, 414 N.W.2d 54 (Ct. App. 1987).

Wis. Stat. § 943.70 Computer Crimes

(2) Offenses against computer data and programs.

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in pars. (b) and (c):

1. Modifies data, computer programs or supporting documentation.
2. Destroys data, computer programs or supporting documentation.
3. Accesses computer programs or supporting documentation.
4. Takes possession of data, computer programs or supporting documentation.
5. Copies data, computer programs or supporting documentation.
6. Discloses restricted access codes or other restricted access information to unauthorized persons.

Note: Violations of this statute can involve penalties ranging from misdemeanors to felonies, and include injunctive relief.

V. Sarbanes-Oxley and the Federal Criminal Statutes – Document Retention and Obstruction of Justice.

A. The 2002 passage of the Sarbanes-Oxley Act strengthened and broadened the reach of the federal obstruction of justice statutes, especially those applicable to document retention and destruction. Sarbanes-Oxley was enacted in the wake of the Enron bankruptcy, at that time the largest bankruptcy in the country's history, and in reaction to the abuses uncovered in the subsequent investigation of the company.

a. The Act "tightened regulation of the accounting industry and instituted new penalties for fraud and obstruction of justice following a 'series of celebrated accounting debacles.'" *United States v. Yielding*, 657 F.3d 688, 710 (7th Cir. 2011) (citation omitted).

b. The purpose of the Act was to "prevent and punish corporate and criminal fraud, protect the victims of such fraud, preserve evidence of such fraud, and hold wrongdoers accountable for their actions." S. Rep. No. 107-146, at 5-6 (2002) at 2.

B. The longest-serving, but also the most narrow and limited, obstruction of justice statute is 18 U.S. C. § 1503, which provides in relevant part: "Whoever corruptly . . . influences, obstructs, or impedes, or endeavors to influence, obstruct, or impede the due administration of justice, shall be punished."

a. To prove obstruction of justice under this statute, the government must prove "that there was a pending judicial proceeding, that the defendant was aware of the proceeding, and that the defendant corruptly intended to impede the administration of that judicial proceeding." *United States v. Fassnacht*, 332 F.3d 440, 447 (7th Cir. 2003).

b. Courts have read into the statute a "nexus" requirement, that is, "that the act must have a relationship in time, causation, or logic with the judicial proceedings." *United States v. Aguilar*, 515 U.S. 593, 599 (1995). "In other words, the endeavor must have the natural and probable effect of interfering with the due administration of justice." *Id.* (quotations omitted).

c. "However, a government agency's investigation – such as the FBI's – that is separate and apart from the court's or the grand jury's authority does not constitute a 'judicial proceeding.'" *United States .v MaCari*, 453 F.3d 926, 937 (7th Cir. 2006).

C. Prior to the passage of Sarbanes-Oxley, the most specific, and farthest reaching, federal obstruction statute applicable to documents and records was 18 U.S.C. § 1512(b)(2)(A)&(B) which provides (and provided) in relevant part: "Whoever knowingly . . . corruptly persuades another person . . . with intent to cause or induce any person to . . . withhold a record, document, or other object, from an official proceeding; alter, destroy, mutilate, or conceal an object with intent to impair the object's integrity or availability for use in an official proceeding (shall be punished)." Creating its chief distinction from section 1503, section 1512(f)(1) states that "an official proceeding need not be pending or about to be instituted at the time of the offense . . . ."

a. Citing to Black's Dictionary, the United States Supreme Court stated that "'[c]orrupt' and 'corruptly' are normally associated with wrongful, immoral, depraved, or evil." *Arthur Anderson v. United States*, 544 U.S. 696, 705

(2005). *See also* Pattern Criminal Jury Instructions of the Seventh Circuit (2012) at page 453: "A person acts 'corruptly' if he or she acts with the purpose of wrongfully impeding the due administration of justice." (According to the Committee Comment, this definition applies to sections 1512 and 1503.)

b. This statute can reach obstructive conduct that occurred during the course of a law enforcement investigation. However, there must be direct evidence that the defendant expected a proceeding "in the foreseeable future, and that his intent was to make the items unavailable . . . in such proceeding or proceedings." *United States v. Frankhauser*, 80 F.3d 641, 652 (1st Cir. 1996). "Foreseeability" is the key consideration. *See Anderson*, 544 U.S. at 708.

c. A civil suit qualifies as an "official proceeding" such to trigger the criminal penalty provisions of the statute. *See United States v. Burge*, 711 F.3d 803, 808 (7th Cir. 2013).

D. Sarbanes-Oxley expressly enacted what is now subsection (c) of 18 U.S.C. § 1512. Section 1512(c)(1) provides in relevant part: "Whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object . . . with the intent to impair the object's integrity or availability for use in an official proceeding (shall be punished)."

a. This subsection filled the hole left by subsection (b)(2) of the statute, which focused on the conduct of an individual who corruptly "persuades" another to destroy or withhold documents or records. Subsection (c) focuses on the conduct of the active participant.

b. The statute does not require proof of materiality. "All that need be proved is that the document was concealed in order to make it unavailable in an official proceeding." *United States v. Black* 530 F.3d 596, 603-604 (7th Cir. 2008).

E. More significantly, Sarbanes-Oxley also resulted in the enactment of 18 U.S.C. § 1519, which greatly expanded the grounds of criminal liability for document destruction. The statute provides in relevant part that: "Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation . . . of any matter within the jurisdiction of any department or agency of the United States . . . or in relation to or contemplation of any such matter . . . (shall be punished)."

a. The statute adopts a "knowing" standard rather than a "corrupt" standard.

b. The statute eliminates the "nexus" requirement written into the other obstruction statutes. *See United States v. Yielding*, 657 F.3d 688, 712-13 (8th Cir. 2011). "[K]nowingly falsifying a document, in contemplation of a federal

matter, with intent to impede, obstruct, interfere with that matter my result in criminal liability, whether or not the obstruction was likely to succeed." *Id.* at 713.

c. There is no requirement that the government prove that the defendant knew that the "matter" in issue was within the jurisdiction of a department of agency of the United States. *Yielding*, 657 F.3d at 713-14. "The fact that a matter is within the jurisdiction of a federal agency is intended to be a jurisdictional matter, and not in any way linked to the intent of the defendant." 148 Cong. Rec. S7419 (daily ed. July 26, 2002) (statement of Sen. Leahy).

d. There is no need to prove that a matter was pending at the time of the destructive act. *Yielding*, 657 F.3d at 715. *See also United States v. Gray*, 642 F.3d 371, 377-78 (2nd Cir. 2011).

e. The statute does not require the government "to prove that [the defendant] intended to obstruct a federal investigation. Rather, the plain language of the statute only requires the government to prove that [the defendant] intended to obstruct the investigation of *any* matter that happens to be within the federal government's jurisdiction." *United States v. Gray*, 692 F.3d 514, 519 (6th Cir. 2012).

f. In summary then, the intent of the statute is plain: "people should not be destroying, altering, or falsifying documents to obstruct *any* government function." *United States v. Kun Yun Jho*, 465 F.Supp.2d 618, 635-36 (E.D.Tex. 2006) (emphasis added).

VI. Wisconsin Lawyer Articles on Electronic Evidence and Related Topics

What You Need to Know - New Electronic Discovery Rules
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?Volume=83&Issue=7&ArticleID=2043

Proposed Rules for Electronic Discovery
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?volume=82&issue=12&articleid=1871

Panning for Gold : Social Networking's Impact on E-Discovery
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?Volume=84&Issue=2&ArticleID=2260

Ethics: Drawing the Line on Discovery Abuse
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?volume=75&issue=11&articleid=254

Avoiding E-discovery Traps
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?Volume=84&Issue=6&ArticleID=2057

E-Discovery: Who Pays
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?volume=85&issue=10&articleid=10335

Technology: Engage the Jury: Presenting Electronic and Computer Evidence at Trial
http://www.wisbar.org/newspublications/wisconsinlawyer/pages/article.aspx?volume=83&issue=2&articleid=2029

CT Case: Sarbanes v. Attorney Ethics
Posted Aug 13, 2007 12:30 PM CDT
By Martha Neil

Fellow practitioners are watching with increasing concern the case of Philip Russell, a Connecticut lawyer who has been charged with violating the Sarbanes-Oxley Act because he allegedly obstructed justice by destroying a client's computer.

"For a lawyer, especially a criminal lawyer, this is the most important case in a long, long time," says George D. Royster of Halloran & Sage in Hartford, Conn. But business lawyers also should be concerned about what this federal prosecution could portend concerning inadvertent destruction of important corporate documents, according to New York Lawyer). This aggressive application of corporate compliance law by federal prosecutors in Russell's case conflicts with a lawyer's ethical duty to zealously represent his or her client and keep client information confidential, says the Connecticut Criminal Defense Lawyers Association. It has filed an amicus curiae brief on behalf of Russell, who is seeking a dismissal.

"Regardless of whether there are ethics issues here, it's not a crime and certainly not a crime under Sarbanes-Oxley," says Jon Schoenhorn, CCDLA's president. "This has a chilling effect on any advice you give to a client."

Robert M. Casale, of Branford, Conn., is defending Russell, who says he didn't know, when he destroyed the computer, that Robert Tate, who worked for Russell's client, Christ Church of Greenwich, Conn., was being investigated in a child pornography case. As discussed in an earlier ABAJournal.com post, Russell himself says he has a clear conscience in the matter: "The law does not require a gym coach to keep a beer can he finds on a school bus," he told Greenwich Time.

Sarbanes-Oxley Ethical Issues

www.chubb.com/businesses/csi/chubb4629.pdf (Article title: "A Lawyer's Guide to Records Management Issues")

http://www.morganlewis.com/pubs/LEPG05_Ethical_Issues_PPT.pdf

http://www.bu.edu/law/faculty/scholarship/workingpapers/documents/Koniak-et-al-Sarbanes-Oxley-04-20.pdf

http://www.kaufmanandcanoles.com/documents/misc/Ethical%20Issues%20for%20Business%20Lawyers.pdf

http://www.zuckerman.com/media/site_files/129_NYBLJ_Ethical%20Issues%20for%20Business%20Lawyers%20Lawyer-Directors%20Just%20a%20Bad%20Idea_Stewart_.pdf

http://scholar.valpo.edu/cgi/viewcontent.cgi?article=1343&context=vulr (Article title from 2004: "What Do I Do Now? A Lawyer's Duty Post-Sarbanes-Oxley)

http://www.sec.gov/news/press/2003-13.htm

See also the attached articles about Attorney Phillip Russell who was prosecuted for a Sarbanes-Oxley related violation and sent to prison. He later commented:

> "The sad fact is that we (lawyers) are considered a prized bounty by federal prosecutors," Russell said. "It's sad, and it's sick and we still go out there every day for our clients."

Here is Russell's ethics decision (a reprimand): http://www.jud.ct.gov/sgc/decisions/070832.pdf

And an article about his return to work after serving his sentence: http://www.bishop-accountability.org/news2008/11_12/2008_12_21_Friedman_LawyerReturns.htm

And finally for now, avoiding non-profit scandals: http://philanthropy.com/article/Antidote-to-Nonprofit/133269/

Litigation Holds: Ten Tips in Ten Minutes

Stephanie F. Stacy
Baylor, Evnen, Curtiss, Grimit & Witt, LLP
1248 "O" Street, Suite 600
Lincoln, Nebraska 68508
sstacy@baylorevnen.com

Introduction

A **litigation hold** is a written directive advising custodians of certain documents and electronically-stored information ("ESI") to preserve potentially relevant evidence in anticipation of future litigation. Also called "preservation letters" or "stop destruction requests," these communications basically advise of the possibility of future litigation and identify relevant documents and ESI which should be preserved. The terms "Litigation Hold Letter" and "Litigation Hold Notice" are used interchangeably to describe written requests from adversaries designed to trigger the duty to preserve relevant evidence, and the same terms are used to describe the written notice lawyers send their own clients advising them to suspend routine document retention/destruction policies and implement a legal hold on all evidence which may be relevant to future litigation.

In the past several years spoliation of relevant evidence—and particularly of ESI spoliation—has assumed a level of importance in civil litigation which warrants very careful attention. Claims of spoliation and motions seeking discovery sanctions for failure to preserve relevant ESI cause litigants and courts to take costly and time-consuming detours from the litigation, and are occurring with greater regularity in all sorts of cases. As Magistrate Judge Piester observed in 2007:

> "When the prospect of litigation is present, parties are required to preserve documents that may be relevant to the issues to be raised, and their failure to do so may result in a finding of spoliation of evidence. The obligation to preserve evidence begins when a party knows or should have known that the evidence is relevant to future or current litigation. *See Stevenson v. Union Pac. R.R. Co.,* 354 F.3d 739, 746 (8th Cir. 1993)(Sanctions not abuse of discretion in pre-litigation destruction of evidence without showing of bad faith); *see also Zubulake v. UBS Warbrg LLC*, 220 F.R.D. 212, 216-18 (S.D.N.Y 2003)("Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure preservation of relevant documents." *Id.* at 218)(citing *Fujitsu Ltd. v. Federal Express Corp.,* 247 F.3d 423, 436 (2d Cir. 2001); *Kronish v. United States,* 150 F.3d 112, 126 (2d Cir. 1998)). At a minimum, that means counsel must direct the client to ensure that documents are preserved, not deleted from an electronically stored information system or otherwise destroyed or made unavailable. Failure to do so has been found to be 'grossly negligent.' *Zubulake*, 220 F.R.D. at 221."

Board of Regents of the Univ. of Nebraska v. BASF Corp., Case No. 4:04CV3356, 2007 WL 3342423 at 4-5 (D. Neb., Nov. 5, 2007).

Discovery sanctions for failing to preserve relevant evidence can be game-changers for lawyers and litigants, and include orders which direct that certain facts be taken as established; prohibit the

disobedient party from supporting or opposing certain claims or from introducing certain matters into evidence; strike pleadings in whole or in part; dismiss the action in whole or in part; render a default judgment against the disobedient party; impose monetary fines on the lawyers and/or clients; give adverse jury instructions; or exclude evidence if the court later concludes relevant evidence was destroyed in bad faith. *See, e.g., Meccatech, Inc. v. Kiser et al.,* Case No. 8:05CV570, 2008 WL 6010937 (D. Neb. April 2, 2008)(Recommending sanctions including striking the disobedient party's answer and entering default judgment against it; holding admissible ESI which eventually was recovered from a hard drive; finding certain facts contained in deleted documents were established for purposes of the action; and precluding disobedient parties from defending against certain of the plaintiff's claims); *Board of Regents of the University of Nebraska v. BASF Corp.*, Case No. 4:04CV3356, 2007 WL 3342423 (D. Neb., Nov. 5, 2007)(Recommending Plaintiff's counsel be required to produce affidavits showing efforts to preserve electronic information going forward; pay defendant's attorney fees regarding sanctions motion; immediately impose a litigation hold on all electronic information of clients to prevent further destruction of evidence; and halt further progress in the case until these sanctions had been met, among other sanctions).

Ten Tips for Responding to Litigation Hold Letters

1. **Watch for Triggers:** Sometimes the event which triggers an organization's duty to preserve relevant documents and ESI is obvious—a letter threatening litigation and demanding that certain evidence be preserved leaves little doubt the duty has been triggered. Other times the triggering event may be more subtle, like a group of supervisors talking about reported harassment, *see, e.g., Doe v. Norwalk Community College*, 248 F.R.D. 372 (D. Conn. 2007), or an SEC investigation into a client's financial irregularities, *see, e.g., Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005). Be aware that events which provide notice of pending, potential or threatened litigation can take many forms, and even when the threat of future litigation is clumsy or obscure, it may trigger the duty to preserve.

2. **Don't Procrastinate:** Responding to and managing preservation issues can be daunting for busy lawyers, but delaying action for even a few days can result in the destruction of relevant evidence which exposes the lawyer and the client to costly discovery sanctions. Place a high priority on responding to preservation issues—this is one area where a day really can make a difference.

3. **Reply to All:** If you receive a Litigation Hold Letter from an adversary, respond in writing stating the measures you and your client are taking to identify and preserve relevant evidence. If you disagree with the parameters or scope of the preservation request as articulated by the adverse party, say so, and offer to consider taking additional measures if the adverse party can show the measures are legitimately warranted under the circumstances. A response letter provides you the opportunity to establish the parameters of what you consider relevant to the issues involved in the future litigation, and places the burden on your adversary to articulate why those parameters should be broader. *See Maddex, Stephen J., "Responding To A Litigation Hold Letter," www.lexology.com (Feb. 19, 2009).*

4. Identify What is Relevant: The scope of a litigation hold will be driven by the documents and ESI which are relevant to the facts and circumstances likely to be at issue in the future litigation. The type of evidence which will be deemed relevant will, of course, depend on the specific facts. Rule 401 of the Federal Rules of Evidence defines relevance as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." The touchstone of discovery in civil cases is whether the information sought is "reasonably calculated to lead to the discovery of admissible evidence" and, in considering the reasonable scope of a litigation hold, one should be guided by the same legal principles. Fortunately, the courts have recognized the duty to preserve is not unlimited and does not require litigants to "preserve every shred of paper, every e-mail or electronic document, and every backup tape," *see Zubulake IV*, 220 F.R.D. at 217, yet determining what information may be relevant is not always easy. Despite the difficulty of determining what sort of information is likely to be relevant to future litigation, lawyers should avoid the temptation of issuing a Litigation Hold Notice which simply asks members of an organization to preserve "relevant" evidence without providing any practical guidance on what that means in the context of the particular claim. *See Samsung Electronics Co., Ltd. v. Rambus, Inc.*, 439 F. Supp.#2d 524, 565 (E.D.Va. 2006)(instructing employees to "look for things to keep" and telling them not to destroy "relevant documents" were insufficient for implementing a legal hold and were found to be the sort of token effort which will "hardly ever suffice.")

5. Put Your Client's Hold Notice in Writing, and Be Specific: A good Litigation Hold Notice should clearly identify the reason for the hold, should prohibit the destruction of relevant documents, and should identify what sort of information is considered relevant. Don't leave a voice-mail or send an e-mail communicating the litigation hold, and don't walk down the hallway and instruct the custodian to "save everything." Put the Litigation Hold Notice in writing, with clear instructions to suspend automatic deletion and clear instructions on what should be preserved. Make sure the Litigation Hold Notice is disseminated to all key players in the organization, and not merely to the official record custodian. Remind your client of the consequences of disregarding the litigation hold, and advise the client that if questions arise about whether something may be relevant, they should check with you before deleting it. Open communication with the client will help ensure all relevant data sources are discovered and relevant information is retained on a continuing basis.

6. Think Outside the E-Mail Box: Talk with your client about what sort of ESI they have, where and how it is stored, and who has access. Consider all your client's sources of data, and look beyond just e-mail, calendar entries, contacts and task lists. What about employee cell phones and Blackberrys®? What about text messages? Voice-mail messages? Backup tapes? Hard drives? Thumb drives? Office lap tops? Social networking sites? Home computers that access the office network? Work closely with your client's IT Manager (or hire a consultant or vendor if appropriate) to get an accurate data map of all your client's ESI so you consider all data sources and can clearly articulate and monitor the preservation obligation.

7. **Follow Up to Ensure Compliance:** Litigation holds, when done correctly, involve more than sending an initial hold notice to your client. It is critical that counsel follow up on the litigation hold to ensure it was implemented properly and is being followed. Counsel should docket and send periodic written reminders about the litigation hold to keep it top-of-mind among the key players, and counsel should refine the scope of the hold if the legal issues evolve or change. *See, e.g., Eng, Michael J., "Counsel Must Not Only Implement Litigation Hold But Must Also Oversee Its Compliance. Electronic Discovery Navigator," www.ediscoverynavigator.com (Mar. 7, 2007).*

8. **Don't be Afraid to Bring In Help:** There may be times when the sheer amount of ESI, the complexity of the data sources, or the level of sophistication required to implement a litigation hold or identify discoverable documents are too much for you and your client to manage effectively or efficiently. In those situations, hiring a qualified ESI consultant may be wise. Particularly when the litigation involves sensitive issues such as alleged fraud, certain employment-related matters, or internal investigations, an impartial third party consultant can assist in implementing and monitoring the litigation hold, as well as do the heavy lifting of sifting through ESI when the time comes to respond to discovery requests, as well as offering independently defensible testimony concerning the reasonableness of the steps taken to preserve and collect evidence.

9. **Plan Ahead:** Work with your clients now to develop a litigation readiness plan so that, if necessary in the future, a litigation hold can be effectively enacted, including the sequestering of back-up tapes, suspension of data destruction policies, and implementation of ESI collection procedures. Identify in advance where data is stored in active systems, backups, archival systems, and other locations so the client's data map is well-developed. Put in place methods to identify those who should be contacted for timely preservation of data. Develop exit checklists for when employees leave the client's company to ensure their documents are easy to locate and properly deleted or stored. *See, e.g., Graham, Jeffrey R., "Litigation Holds: Best Practices for Protecting Your Company's Email Data From Inadvertent Loss and Spoliation," www.abatoday.com (Aug. 2007); Beard, Jeffrey J., "White Paper: Best Practices for Legal Hold Processes," www.legalholds.typepad.com (June 23, 2009).*

10. **Stay Current in this Rapidly-Evolving Area of Law, and Attend the Fall CLE on E-Discovery.** The law concerning litigation holds is evolving rapidly, with important opinions coming out every month that impact the way in which litigation holds are managed. To be sure you comply with the discovery rules, avoid sanctions, and protect yourself and your clients from allegations of spoliation, you should closely monitor changes in this area of law, and consider attending the seminar on E-discovery which the Federal Practice Committee is planning for later this fall.

ADDITIONAL RESOURCES

For informative blogs and additional information on managing litigation holds consider:

- ✓ *www.bowtielaw.wordpress.com* – "The Knotty Issues of e-Discovery"
- ✓ *www.ediscoverynavigator.com* – "Electronic Discovery Navigator: Predictability and Consistency in eDiscovery"
- ✓ *www.lexology.com* – "Practical Know-How and Market Intelligence for Business Lawyers"
- ✓ *Maddex, Stephen J., "Responding To A Litigation Hold Letter," www.lexology.com (Feb. 19, 2009)*
- ✓ *www.legalholds.typepad.com* – "Legal Holds and Trigger Events: A blog dedicated to cases, insights, developments and best practices relating to the development and implementation of legal holds"
- ✓ *www.abanet.org* – "ABA Law Practice Today"
- ✓ *www.businessmanagementdaily.com* – "Business Management Daily"
- ✓ *www.ediscoveryjournal.com* – "Unique Perspective. Independent Insight. Pragmatic Advice."

Special thanks to Joshua Gilliland of D4 LLC for his contributions to the "Ten Tips in Ten Minutes." Joshua Gilliland is a nationally-recognized expert on E-discovery matters and can be reached at:

D4 LLC
303 Twin Dolphin Drive
Suite 600
Redwood City, California 94065
(650) 576-3298
jgilliland@d4discovery.com
www.bowtie.com

FARELLA BRAUN + MARTEL LLP

Advising the Corporate Client on the Duty to Preserve Electronic Evidence

by Douglas R. Young
Farella Braun + Martel LLP
San Francisco, California
dyoung@fbm.com

www.fbm.com

Table of Contents

Advising the Corporate Clienton the Duty to Preserve Electronic Evidence

by Douglas R. Young*

I. Introduction

Electronic evidence is often critical in criminal cases. For example, David Copenhefer tried to delete ransom notes from his computer, but experts recovered them and they helped convict him of murder.[1] In the first reported conviction for an online hate crime, a federal jury found Richard Machado guilty of sending racist death threats via e-mail to Asian students at a California college.[2] The e-mails themselves were the prime evidence against him.[3] As this article goes to press, federal prosecutors are planning to use computer records as evidence of a multinational conspiracy in the bombings of the American embassies in Kenya and Tanzania.[4] Although these cases involved individual defendants, corporate defendants have just as much reason to be concerned that electronic evidence may be used against them.

Much of the information generated in American businesses today, such as e-mail and draft versions of documents, is never reduced to paper form. Some observers estimate that 20-30% of electronic data never appears on paper.[5] With most businesses now storing information in electronic form, a lawyer advising a corporate client must understand not only the law, but also (at least at a basic level) the technology of electronic data storage.

Because of the high risks associated with retaining electronic documents, some corporations have instituted document retention programs that periodically delete electronic documents. In-house counsel typically advise clients to be aggressive and thorough in this regard, as such a system can purge potentially embarrassing documents before a controversy arises in which they could be relevant. Once a corporate client is on notice, however, of a possible criminal investigation (whether by grand jury or otherwise) or even a civil investigation or dispute, continuing to use such a system could conflict with the duty to preserve evidence. In this situation, electronic data (and sometimes even associated hardware) must be preserved like any other potential evidence. Purging electronic documents at that point is no different from shredding paper documents, and can subject the corporation to a range of consequences, including trial sanctions, sentencing enhancement, and independent criminal prosecution. Even the attorney herself may suffer sanctions.

This article explores the issues involved in preserving or destroying potential electronic evidence. We begin in Section II with the fundamentals of electronic evidence. Section III discusses document retention programs and the need to adapt them to manage electronic documents. Section IV summarizes the law regarding the duty to preserve evidence after notice of a government investigation or proceeding. Section V outlines potential consequences of the failure to preserve electronic evidence. Finally, Section VI provides some guidelines on advising the corporate client regarding the duty to preserve electronic evidence.

II. Fundamentals of Electronic Evidence

In a superficial sense, electronic documents are simply documents that exist in electronic, rather than paper, form. They possess many characteristics not shared by paper documents or other tangible evidence, however.

First, electronic "data can be analyzed more efficiently, and more effectively, than hard-copy documents."[6] A computer expert may search for relevant evidence by file, by sub-directory, or by designing keyword searches that ferret out particular names, words, places, or any combination of them. In an antitrust prosecution for price-fixing, for example, an expert can search for words or names associated with the targeted product and narrow the search dramatically from the start. If the keyword search is well-defined, it can be the most efficient way to find the needle in the haystack. Thus, "the more digital data that can be obtained, the better."[7]

Electronic evidence can provide a wealth of information about the inner workings of a corporation. "Computers, and the various media in which computer-generated information is stored, provide a unique window into a company's memoranda, correspondence, strategies, business plans, product designs, analyses, projections, economic forecasts, statistics, and data."[8] Not only can computers quickly reveal information about, for example, the composition of a company's labor force, but unguarded e-mails may yield telling glimpses into the subjective motives of a corporation's employees and officers.[9] Electronic documents also typically include precise dates and times when documents were sent, received, or edited; these can illuminate a chronology that would be obscure if the documents were on paper.

Computer records also allow access to a range of information not available in paper form, either because the information has never been reduced to printed form or because the paper version no longer exists. These records may include superseded drafts, corporate documentation of interbank transfers, inventory and sales data, and internal e-mail.[10] Because users typically do not expect these electronically stored documents, such as drafts and e-mail, to be printed, they often compose and circulate such documents with a casual and candid attitude. As a result, investigators are likely to find more revealing, and often damaging, information included in these electronic documents than they would in their paper counterparts.

E-mail is particularly problematic. It is becoming universal in today's corporate environment -- according to recent statistics, 90% of organizations with over 1,000 employees use e-mail, as well as most smaller corporations.[11] The informal nature of e-mail correspondence provides a false sense of security. It is thus a well-observed phenomenon that "thoughts and opinions that would never be placed in a formal memorandum or letter often end up in e-mail."[12] People assume, wrongly, that such messages are private, and that they maintain control over who will be privy to message content. In reality, a single e-mail may be forwarded many times over. E-mails, therefore, are a "likely repository of 'smoking guns.'"[13] Moreover, e-mail may be particularly convincing evidence because juries tend to believe that e-mail reflects an author's "true, ad-hoc feelings."[14]

Even when hard-copy versions of electronic documents are available, they may be incomplete. Electronic communications are rarely identical to their paper counterparts - they are records unique and distinct from printed versions of the same records.[15] Earlier drafts of documents will often provide additional context and information about the final version. Draft versions may also provide useful snapshots into the author's thought processes. With the right software applications, even marginally sophisticated users may now record hidden text or comments that are not apparent when a document is viewed on screen or printed. Annotations by many people may be embedded in a single document, though invisible on printouts.[16] System history

records can also reveal a wide range of information that would not be apparent from the face of a document. Electronic records can show when people deleted or created files, or when they changed passwords.[17] "Key words, remarks, headers and footers, even file names, can reveal a mother lode of material for cross-examination."[18]

As important from an investigatory point of view, computers continue to store electronic records long after all paper versions have been lost or destroyed. Thus, the fact that no hard copy version of a document can be found rarely means that the document is unattainable:

> Back-up copies of files may be available as a result of formal or informal preservation of information. Formally, companies often make timed back-ups of all the information stored on a computer network at given points. These archival tapes may be preserved for short periods of time as a source of memory in the event of an emergency such as accidental deletion or loss of important data. Subsequently, such tapes may be recycled for further archiving or other use. Archival tapes may also be preserved for longer periods of time either because of government-mandated recordkeeping requirements or simply for purposes of historical preservation. Informally, employees may make their own random back-up copies of files to guard against accidental deletion or system failure. These back-ups may employ different file names. Indeed, different versions of an evolving document may be saved under different file names.[19]

Moreover, electronic documents may exist, in varying forms, in several locations on a computer network. Digital data is stored as an employee works, and then is often copied or forwarded many times. This process has been greatly facilitated by e-mail systems that allow users to attach files easily, as most now do.[20] The presence of digital data in multiple locations promotes later recovery of documents thought to have been deleted, and complicates a corporation's ability to manage document storage and deletion. Forensic computer specialists are well aware of the increasingly transitory nature of electronic data. As John Jessen, managing director of Electronic Evidence Discovery, Inc. ("EED"), notes: "Even if we can't find the deleted file on the hard disk, there's almost always copies of it lying around somewhere else, on backup tapes, in a file folder, on the network. It's rarely really gone."[21]

The persistence of electronic data, often to the surprise of authors who believe they have effectively deleted data from a computer system, is one of the most important ways electronic evidence differs from traditional forms of evidence. "If there's any golden rule about electronic evidence, it's this: It's hard to get rid of."[22] Many users have belatedly learned what David Copenhefer learned about his ransom notes: information stored on a computer is not deleted simply by pressing the delete button.[23] Rather than erasing the information from the system, this function merely removes the file name from view. The computer then marks the file on the hard disk as space to be overwritten by new information. The deleted file is still recoverable at this point and will continue to exist until it actually is overwritten, which may take months (or longer).[24] Even when a file is eventually overwritten, it may be only partially so, leaving remnants of the original file undisturbed.[25]

The informal tone of many electronically stored documents, coupled with the persistence of electronic records, means that such documents are often "even more

dangerous than written records and memos" to a corporation.[26] "An unfiled note gets deleted in the next day's trash," but "in a typical office network almost all e-mail is recorded on the system server. Messages sent years ago may live on in taped storage, far beyond the reach of a delete key, although not of a subpoena."[27] And because saving an electronic document is so easy, and appears to take no physical space at all, users may be reluctant to delete anything with any potential use, enriching the hunting ground for future investigators.

Although corporations are beginning to implement destruction policies to decrease the risk associated with indiscriminately maintaining electronic documents, "[a] destruction policy, even if followed, may turn out to be illusory. For as a software engineer must know, merely deleting a message from one's personal computer is usually not enough to purge it from the system."[28] Thus, in addition to a regular deletion policy, a corporation must also employ special software if it wishes to ensure that unnecessary files are regularly eliminated from the computer network. Such software is now available -- for example, EED offers a software called "TruErase,"[29] said to "delete the deleted."[30] Such software operates as a modern version of the paper shredder by pre-programming computer systems to actually eliminate deleted files.

Even this may not be enough. In addition to company-wide systems, local area networks, individual desktop PCs, online services, disks and laptops may all contain potentially relevant evidence. People today often work from home, connected to their offices by modem, so evidence may also lurk on home computers and laptops, beyond the reach of a corporation's document management regime.

Although lawyers are not expected to be computer experts, some familiarity with basic electronic data concepts can help in advising clients. Corporate information systems departments can also help to educate the lawyer (especially in-house counsel). Basic electronic evidence concepts include the following:

- **Computer systems**, at the most basic level, act as tools to process and store information.

- **Files** are simply aggregates of information placed under a common name and stored on a computer.[31]

- **Active data** includes such information as word processing documents, spreadsheets, databases, e-mail messages, electronic calendars, and contact managers. This is the information most readily available and accessible to users.

- **Replicant data** are "clones" of active data that are created in order to help recover lost data in the event of a computer malfunction, power loss or a system crash. Most software programs now include an automatic backup feature that makes and periodically saves copies of active files as users create them. Typically, however, the clones are not stored in the same directory as the active file. On networked systems, they are generally saved directly to the user's hard drive rather than to the centralized network file server. The effect is that documents purged from the central file server (for example, under a corporate document retention program) may still exist as clones on a user's hard drive. In addition, users may not be aware of the automatic backup feature and will not think to delete the copies from their hard drives.

- A corporation may also deliberately back up its network on a regular basis, thereby creating **backup data**. Backup data is information that is copied as a user protection measure in the event of system failure. Backups normally copy only data saved on the file server, but not data stored on individual users' hard drives. Most networks are backed up routinely -- for example, a corporation may back up data fully once a week, perform spot backups throughout the week, and save the last weekly backup of every month. Monthly backups may be saved for months or even years.

- **Residual data** are data that seem not to exist, but can nevertheless be retrieved. Examples include "deleted" files that continue to reside on disk surfaces, and information in non-system hardware, such as in the buffer memories of printers, copiers, and fax machines. As noted, with most software, simply "deleting" a file does not erase that file from the computer system, but only frees up the space to be overwritten. Computer forensic specialists also have tools that allow them to examine drives for residual data that may be located in harder-to-find places on disks and drives.

- In addition to data files, which include e-mail, **background information** can also be potential evidence. For example, computer logs and audit trails create an electronic map of network usage, recording information such as the identities of network users, time length of network access, and places a user visited on the computer system. These trails can also reveal who printed, copied, accessed or purged particular files, and the locations to which the files were downloaded. Special software can monitor which programs employees use, e-mail they send and receive, and internet sites they visit. Many corporations also use access control lists to control user's rights to view and edit information. Access control lists can quickly help to identify individuals who had access to particular files and the type of access allowed.[32]

III. The Need to Adapt Corporate Document Retention Programs to Manage Electronic Documents

A corporation's approach to preserving its documents can make a profound difference in litigation and in criminal prosecutions. The Microsoft antitrust case provides a sobering example.[33] There, the government was able to discover an estimated 3.3 million Microsoft documents, including "mega-bytes of e-mail messages" dating back many years.[34] As widely reported, the complaint quotes e-mail messages sent by top executives at Microsoft that seem to indicate anti-competitive behavior.[35] These e-mails proved very damaging to the credibility of Microsoft's corporate witnesses, including Bill Gates himself. How did this happen?

Ironically for a software giant, as late as 1998, Microsoft had no e-mail retention policy.[36] Chairman Gates quipped that the company would not be changing its business practices at all as a result of the trial – except that it might be revising its policy of keeping records of corporate e-mail.[37] Microsoft was not alone in its lack of internal e-mail regulation. One survey estimated that at that time of the Microsoft trial only around a third of all businesses had formal policies on the content, handling and archiving of e-mail.[38] Even workplaces with enough foresight to institute such policies usually had no enforcement mechanism.[39]

The Microsoft case so publicized the danger of unrestricted e-mail retention that corporations are finally beginning to modernize paper-based records programs to reflect the importance of electronic communications. Although "[t]he proper handling of electronic data is fundamentally different than that of paper,"[40] the starting point of any effective document retention program is the same. Only necessary data should be retained. All other data should be periodically and effectively deleted.

A typical e-mail retention policy might require deletion of e-mail messages after 60 days, unless the user takes affirmative steps to keep the message.[41] Generally, the corporation will simply program the business's computers to review dates of stored e-mails and automatically (and permanently) delete those beyond the allowed limit using special software.[42]

In particular, an effective electronic file management program should:

- organize electronic data so that it can be found and retrieved efficiently for litigation, but in a way that it does not invite wholesale discovery beyond what is relevant;
- identify and preserve necessarily business documents while keeping the number of unnecessary documents to a minimum;
- identify preventative measures for reducing abuse of e-mail and other computer systems; and
- define and implement retention policies that support these and keep necessary business documents from accumulating past their useful lives.[43]

IV. The Duty to Preserve Electronic Evidence

Sound risk management principles dictate that a corporation institute document retention policies that account for electronic documents. A corporation ordinarily has a right to destroy documents that it is not required by law to maintain.[44] Once it has received notice that it is the subject of a criminal investigation, however, destroying potentially relevant documents may become unlawful. At this point, a corporation, like any other defendant, is under an affirmative duty to preserve relevant evidence.[45] As a result, the corporation's continued destruction of documents under its routine policies may subject it to discovery sanctions, criminal penalties, sentence enhancement, and other consequences.[46]

Typically, the first notice a corporation will receive that it is the target of a government investigation will be a subpoena served on the corporation from a grand jury or a regulating agency.[47] Notice need not come formally to the corporation itself. Knowledge (or reasonably imputed knowledge) by a responsible officer or executive of a pending investigation is enough to trigger the duty to preserve evidence.[48] An informal request for information from a prosecuting agency or inspector general should thus alert a corporation that something is in the wind. Even an investigation of a person or other entity doing business with the corporation may be notice enough that their common dealings are under investigation. By way of illustration, if Acorp has conspired with Bcorp to fix prices and then learns that Bcorp is under investigation by the Antitrust Division, it may be difficult for it later to persuade others that it was unaware its own records might be sought as evidence.

Of course, a subpoena is the clearest indication that standard business records or documents, subject to purging at will, are now potential evidence, subject to a duty of preservation. As noted, however, the duty can arise before that point. For example, in *United States v. Ruggiero,* the court held that "destroying documents **in anticipation** of a subpoena can constitute obstruction."[49] Even the destruction of relevant documents after mere knowledge that a grand jury investigation has begun can support a verdict of obstruction. In *United States v Platt*, for example, the defendant argued that she could not be charged with attempting to destroy and conceal evidence pertaining to a criminal investigation unless the evidence at issue had first been requested by the government.[50] The court rejected the defendant's argument, holding that "it is enough for a defendant to have had knowledge of a grand jury investigation and to have attempted destruction of a relevant document to keep it out of the grand jury's hands -- no subpoena is necessary."[51]

Once a subpoena has actually been issued, objections to compliance are limited. A corporation, as a "collective entity," has no privilege against self-incrimination and may not assert the Fifth Amendment as a defense to production.[52] And the majority rule is that the government does not need to make a preliminary showing of relevance in order to enforce a document subpoena.[53]

Grand jury subpoenas of corporate records may not be used to compel production that would be unreasonable or oppressive, however. Thus, a grand jury subpoena may be quashed when the request is unreasonably broad.[54] This is as true of electronic documents as of paper ones. For example, in *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, the court held that a grand jury subpoena issued for all a corporation's hard disk drives and floppy diskettes was unreasonably broad.[55] There, the subpoena had called for documents that were completely irrelevant to the investigation, even though the government had acknowledged that the relevant documents could be isolated through keyword searching. Analogizing to a prior case holding overbroad a subpoena demanding the entire contents of particular filing cabinets, the court reasoned that although the issue had not been considered before in the context of demands for electronic evidence, there was little distinction between computers full of electronic documents and filing cabinets full of paper documents.[56]

Since 1994, the U.S. Department of Justice ("DOJ") has followed formal guidelines in order to help federal agents and attorneys identify and obtain electronic evidence.[57] These guidelines give the attorney insight into what the government may be looking for from a law enforcement perspective. The Guidelines propose the following four-step procedure to "maximize the likelihood of a successful search and seizure"[58]:

> 1) assemble a team consisting of the case agent, the prosecutor, and a technical expert as far in advance of the search as possible; 2) learn as much as possible about the computer system that will be searched before devising a search strategy or drafting the warrant; 3) formulate a strategy for conducting the search (including a backup plan) based on known information about the targeted computer system; and 4) draft the warrant, taking special care to describe the object of the search and the property to be seized accurately and particularly, and explain the search strategy in the supporting affidavit.[59]

The DOJ Guidelines recognize that in order to obtain electronic evidence effectively, law enforcement personnel will need a certain amount of technical sophistication. Thus, the Guidelines note that:

> Despite the common legal framework, computer searches differ from other searches because computer technologies frequently force agents to execute computer searches in nontraditional ways. Consider the traditional case of a warrant to seize a stolen car from a private parking lot. Agents generally can assume that the lot will still exist in its prior location when the agents execute the search, and can assume they will be able to identify the stolen car quickly based on the car's model, make, license plate, or Vehicle Identification Number. As a result, the process of drafting the warrant and executing the search is relatively simple * * * Searches for computer files tend to be more complicated. Because computer files consist of electrical impulses that can be stored on the head of a pin and moved around the world in an instant, agents may not know where computer files are stored, or in what form. Files may be stored on a floppy diskette, on a hidden directory in a suspect's laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly titled, stored in unusual formats, or commingled with millions of unrelated, innocuous, and even statutorily protected files. As a result of these uncertainties, agents cannot simply establish probable cause, describe the files they need, and then "go" and "retrieve" the data. Instead, they must understand the technical limits of different search techniques, plan the search carefully, and then draft the warrant in a manner that authorizes the agents to take necessary steps to obtain the evidence they need.[60]

Responding to demand from law enforcement, private courses are now being offered to train personnel in issues and procedures related to electronic evidence. One website advertises a course in "computer forensics" specifically designed for law enforcement.[61] It promises to provide "the tools to both understand the structure, functionality, and organization of seized personal computers and effectively determine, extract, and analyze evidence that may reside within the storage equipment that has been seized."[62]

Many federal investigating agencies now retain computer experts on staff to assist with seizing computer evidence and analyzing the evidence once it has been seized.[63] For example, the FBI has created a specialized team called the "Computer Analysis and Response Team" (known as "CART") that examines computer evidence for FBI agents across the country, the Secret Service has the "Electronic Crime Special Agent Program," and the IRS has "Seized Computer Evidence Recovery Specialists."[64]

V. Consequences of Failing to Preserve Electronic Evidence

A. Spoliation of Evidence

Spoliation means the "intentional destruction of evidence."[65] The consequences of spoliation can include allowing the fact-finder to draw an adverse inference -- that the evidence destroyed was unfavorable to the party responsible destroying it.[66] The inference is based on the belief that a party would not destroy or fail to produce favorable evidence. Accordingly, "[a] party's failure to produce evidence when he is free to produce or withhold may . . . be treated as an admission."[67]

Although more familiar in the civil context, the spoliation concept has been applied in criminal cases as well. For example, in *United States v. Marchesani*, the

defendants were accused of conspiring to use extortionate means to collect debts.[68] The prosecution introduced evidence that the defendants had destroyed incriminating promissory notes, and the court instructed the jury that, if it believed this evidence, it could regard the destruction of notes as evidence of a consciousness of guilt.[69] Holding the instruction proper, the Sixth Circuit stated that "[e]vidence of a variance between the stated and actual interest rates of such notes, followed by their destruction upon repayment under the circumstances of this case, could well have been construed by the jury as establishing a guilty conscience on the part of appellants and as showing an awareness by them of the fact that the transactions were illegal."[70] In *State v. Hilbert*, the Missouri Supreme Court recently held that burning a car used in a murder and kidnapping constituted spoliation and could support an inference of consciousness of guilt.[71]

Because of their severity, spoliation sanctions usually require the intentional destruction of evidence. For example, in *State v. Langlet*, the Iowa Supreme Court held that spoliation "involves more than destruction of evidence. Application of the concept requires an intentional act of destruction. Only intentional destruction supports the rationale of the rule that the destruction amounts to an admission by conduct of the weakness of one's case."[72] In *Langlet,* the state had destroyed tape-recorded conversations made by the defendant after his arrest, but had done so under a standing city policy requiring periodic erasures and before Langlet asked that they be produced. Langlet did not claim that the destruction was intentional, and so the adverse inference was not applied.[73]

Courts in the civil context have similarly held that the spoliation inference may not be applied in cases of destruction under a pre-existing records retention policy. A case in point is *Vick v. Texas Employment Commission*, in which the records at issue had been destroyed following routine procedures in place well in advance of the interrogatories requesting information the records had contained.[74] Not all jurisdictions agree, however, and some have dispensed with the bad faith requirement for spoliation altogether. For example, in *Anderson v. Litzenberg*, a Maryland court held that a spoliation instruction permitting an adverse presumption was proper against a spoliator even in the absence of fraudulent intent.[75]

Destroying evidence can also expose the spoliator to discovery sanctions. Rule 37 of the Federal Rules of Civil Procedure lists an array of such sanctions, including taking disputed facts as established, forbidding a party to support or oppose designated claims, and even dismissing the action.[76] Similar rules appear in state statutes.[77] While these sanctions will not ordinarily apply in criminal cases, they will apply in quasi-criminal proceedings such as those for forfeiture and civil penalties. They may also apply where, as in California, there is a reciprocal element in criminal discovery.[78]

B. Obstruction of Justice

The main criminal sanction for destroying evidence, electronic or otherwise, is a prosecution for obstruction of justice. Three sections of Title 18 of the United States Code -- sections 1503, 1505 and 1510 -- prohibit the destruction of evidence at all stages of a government inquiry.

Section 1503, the general federal obstruction of justice statute, does not expressly prohibit the destruction of documents.[79] Courts have nevertheless generally

interpreted it to apply in cases of willful document concealment or destruction.[80] To violate Section 1503, a defendant must destroy documents during an ongoing or pending judicial proceeding, and must have had notice that the proceeding had been undertaken. Notice may take the form of a complaint or a subpoena. From that point forward, destruction of pertinent data constitutes an obstruction. The situation before that point is less certain -- much depends on what the accused knew about the pending proceeding, or what knowledge may be imputed to her.[81]

Concealing, altering or distorting a document has been held to constitute obstruction of justice as well.[82] As noted, electronic evidence is easily altered or destroyed through routine procedures in computers and networks. Also relevant to electronic documentation is that outright concealment is not required to convict under 1503 -- an attempt to conceal it is enough.[83] Thus, when electronic documents have been deleted, but can still be recovered, prosecution may still lie under § 1503.

The federal circuits are in conflict as to the exact intent required under § 1503. Some circuits require knowledge on the part of the defendant that the probable outcome of the destruction will be to obstruct justice.[84] In *United States v. Neiswender,* the Fourth Circuit took a different approach and held for a negligence standard.[85] In that case, Nieswander told an attorney representing a criminal defendant that he could ensure an acquittal in the criminal trial for $20,000 because he had a juror under his control. Nieswander knew he had no ability to obstruct justice, however, as his scheme was entirely fraudulent. The court held he could be convicted under § 1503 anyway because Neiswender's fraud could have resulted in the defense attorney advocating less vigorously for his client.[86] The *Neiswender* approach thus ignores a defendant's subjective motivations, substituting instead the following test: is it **reasonably foreseeable** that the defendant's actions would have the effect of obstructing justice?[87] Other jurisdictions have since followed *Neiswender.*[88] The question is of particular importance for electronic records, because where a specific purpose to obstruct justice is required, destruction of electronic documents under a reasonable document retention policy would be unlikely to support a conviction (or even warrant an indictment), while in a *Neiswender* jurisdiction that may not be so.[89]

Section 1503, which applies to judicial proceedings, is complemented by § 1505, which applies to Congressional and agency proceedings.[90] One authority lists the following circumstances at which destruction becomes criminal under § 1505: "when the agency is first notified of potential violations; when pre-investigations begins; when an informal inquiry begins; or, when a formal order is issued directing investigation to begin."[91] Exactly what constitutes notice that an agency investigation has begun under 1505 is unclear, but receipt of informal notice that an investigation is **about to begin** would probably be sufficient to institute the duty to preserve relevant documents.

Conviction under this section for document destruction requires a showing of some connection between the destruction and an effort to frustrate agency evidence-gathering. Here, too, it is not yet quite clear whether destruction of records under a pre-existing written document management policy would be a violation.[92] In other words, would deliberate failure to suspend routine electronic document deletion procedures despite **unofficial, informally obtained** knowledge that a government investigation is pending expose the corporation to criminal liability? How firm would this informal notice have to be? To what extent can knowledge restricted to high management circles be imputed to the employees running the document retention policy

or to the corporation itself?[93] Without clear guidance from the caselaw, attorneys must be cautious in advising their clients.

Section 1510 forbids obstructing the transmission of information regarding criminal activity to federal investigators even without active judicial, administrative or legislative proceedings.[94] The elements required to prosecute under this section basically track the requirements of the other two obstruction statutes.[95]

C. Other Criminal Charges

In addition to the general obstruction of justice statutes, other criminal laws can affect corporations, as well as their officers and their employees, that engage in the destruction of evidence.

The *general conspiracy statute*, 18 U.S.C. § 371, is one of the most frequently used statutes in cases involving multiple defendants.[96] This statute prohibits agreements between two or more persons to commit illegal acts, and a corporation may be convicted for conspiracy with its employees under the statute.[97] Thus, a corporation may in theory be convicted under Section 371 for conspiring to obstruct justice, for example by destroying or tampering with potential evidence, including electronic documents.[98]

The *federal contempt statute*, 18 U.S.C.§ 401,[99] authorizes courts to punish those who disobey court orders, including subpoenas and grand jury subpoenas. Courts may thus hold a party in contempt for deliberately destroying documents that the court has ordered the party to produce.[100] Some authorities equate liability under sections 401 and 1503.[101] There are important differences, however. The contempt statute relates to conduct in court or in defiance of court orders, while the obstruction of justice statute is limited to conduct occurring out of court.

Acts that obstruct justice may also be penalized as *misprision of felony* under 18 U.S.C. § 4.[102] This section prohibits concealment of a felony and could theoretically be applied in a case involving the destruction of documents. In order to establish liability under Section 4 based on a routine document destruction policy, however, the government would need to prove that the policy was implemented or continued with the intent to conceal a felony, rather than just with the intent to eliminate unnecessary records.

Many states have statutes in place that specifically prohibit the destruction of evidence. For example, under Florida law, when a person knows a proceeding is pending, destruction of evidence constitutes a third-degree felony.[103] In California, it is a misdemeanor willfully to destroy or conceal anything one knows is about to be produced in evidence upon any trial, inquiry, or investigation authorized by law.[104] Other states have comparable provisions.[105]

D. Sentencing Guidelines Enhancement

As an alternative to charging criminal defendants with obstruction of justice, federal prosecutors may choose to use destruction of evidence as a ground for a sentence enhancement.

United States Sentencing Guideline Section 3C1.1 provides for a two-point offense level increase in sentencing when a defendant has "willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice."[106] Application note 4(d) to the Guideline lists "destroying or concealing or directing or procuring another person to destroy or conceal evidence that is material to an official investigation or judicial proceeding (e.g., shredding a document or destroying ledgers upon learning that an official investigation has commenced or is about to commence)."[107] Sentencing courts have proved quite willing to apply this sanction in appropriate cases.[108]

Although the Section 3C1.1 enhancement cases seem all to have involved individual defendants, it need not remain so. Chapter 8 of the Guidelines deals specifically with sentencing of organizations, and provides for increased fines when sentencing enhancements are applied to corporations.

State law may also allow for obstruction enhancements. For example, the defendant in *State v. Vaughn*, who was convicted of a sex crime, suffered an enhancement for trying to alter files on his computer to hide evidence and create an alibi on which he then relied after his arrest.[109] He had attempted to make it appear that he had been composing a letter at the time of the crime, and had deleted pornographic material from his computer -- though he backed up the material so he would not lose it.[110]

E. Professional Sanctions Against Attorneys

Attorneys may breach professional standards if they participate in the destruction of evidence or advise their clients to do so. For example, Model Rule of Professional Conduct ("MRPC") 3.4(a) imposes on an attorney an obligation of fairness in dealing with opposing parties and counsel, and forbids a lawyer to alter or destroy (or counsel another to alter or destroy) documents having "potential evidentiary value."[111] The range of sanctions that can be imposed by a state bar for violations of the ethical rules include disbarment, suspension from practice for an indefinite period, suspension for a limited period, and a reprimand.[112] As noted above, destruction of evidence may also violate criminal statutes, and an attorney is not immune from criminal responsibility for complicity in these actions.[113]

The case of *Bratka v. Anheuser-Busch* provides useful insight into the expectations that courts have of attorneys to oversee the production of evidence by their clients.[114] The defendant in that case was a large corporation that failed to produce highly relevant documents after repeated discovery requests. The court ultimately sanctioned the defendant by granting a default judgment to the plaintiff on the issue of liability, and accused the attorney of "gross negligence" in his handling of the discovery requests.[115]

The court found that the defendant's lack of diligence in planning and executing an effective search for the relevant documents evidenced an absence of good faith.[116] The court also set out the minimum procedures an attorney should follow after receiving a document request. Thus, the court stated that an attorney must at the very least formulate a plan of action that would include:

> [C]ommunicating with the client to identify the person having responsibility for the matters which are the subject of the discovery request and all employees likely to have been the authors, recipients or custodians of

> documents falling within the request. The plan should ensure that all such individuals are contacted and interviewed regarding their knowledge of the existence of any documents covered by the discovery request and should include steps to ensure that all documents within their knowledge are retrieved. All documents received from the client should be reviewed by counsel to see whether they indicate the existence of other documents not retrieved or the existence of other individuals who might have documents, and there should be appropriate follow up.[117]

The *Busch* case, while decided in the civil context, demonstrates the importance of diligence on the part of counsel in conducting a search for documents. With respect to electronic documents that can be found on hard drives, diskettes, network systems and even home computers, the location and the existence of such documents may not be readily apparent to counsel. Nevertheless, *Busch* demonstrates that counsel is under an obligation to formulate a plan to recover such documents. This may mean working directly interfacing with and supervising the corporation's information systems personnel in recovering documents.

In addition, a lawyer who fails to take affirmative steps to preserve and safeguard relevant evidence runs the risk that the client's destruction will be imputed to the attorney. As the Supreme Court of California has noted:

> [T]he risk that a client's act of spoliation may suggest that the lawyer was also somehow involved encourages lawyers to take steps to protect against the spoliation of evidence. Lawyers are subject to discipline, including suspension and disbarment, for participating in the suppression or destruction of evidence. * * * The purposeful destruction of evidence by a client while represented by a lawyer may raise suspicions that the lawyer participated as well. Even if these suspicions are incorrect, a prudent lawyer will wish to avoid them and the burden of disciplinary proceedings to which they may give rise and will take affirmative steps to preserve and safeguard relevant evidence.[118]

VI. Summary and Conclusion: Advising the Client

Considering the range of sanctions and penalties that may be assessed against both lawyer and client, counsel should be careful to consider electronic evidence when advising the client regarding the duty to preserve evidence after notice.

A. The Duty to Preserve Evidence

Whether or not the corporation is the subject of an investigation or proceeding, it is advisable that the client maintain a document retention program that accounts for electronic data. In other words, the corporation should regularly and permanently delete all unnecessary electronic data it is not required by law to maintain. The policy should be set out clearly in writing. It should include a protocol for suspension when knowledge of a pending investigation or lawsuit raises a duty to preserve evidence, specifying the circumstances under which an officer, executive or counsel can order modification of the program in order to preserve evidence. Moreover, the policy should mandate procedures with specificity (i.e., purging "after 90 days" as opposed to "after a reasonable time") so as to avoid confusion and lack of effective implementation. Finally, the program should specify business-related, non-controversial reasons for its existence and parameters.

Once the corporation receives a subpoena, formal letter, or other unequivocal notice that it is the target of, or witness in, a criminal investigation or other proceeding, the corporation may not destroy any documents which might reasonably be expected to be relevant to the inquiry, or to lead to other relevant evidence. Counsel is under a professional, as well as an ethical, obligation to ensure that a corporate client preserve any data that might be relevant to an investigation or other proceeding of which it has actual notice.

When notice is less clear, so is the duty to preserve. Because the case law is not precise, counsel would be well-advised to err on the side of caution -- preserving rather than destroying until such time as the costly, and probably disruptive, effort to preserve can be either negotiated with the investigating authority or pared down through court action. Some general guidelines include the following: when the corporation or its responsible officers possess actual awareness, however obtained, that an investigation or proceeding is pending in which its documents are potential evidence, the corporation should take affirmative steps to preserve data that may reasonably be expected to be relevant. These steps should include suspending a document retention policy as far as relevant data is concerned. Counsel should also consider hiring a computer expert to assist with this process. Although this rule appears harsh, an attorney should keep in mind that the penalties for destroying evidence are likely to harm the client "as much or more than the evidence itself."[119] Cost to the client should also be kept in mind. Where advisable, therefore, an effort should be made to negotiate with the investigating agency the scope of data that needs to be preserved.

In sum, factors that counsel should consider prior to advising a client at the notice stage include:

- **What type of "notice" has the client received?** Has the client received actual notice, or something less formal? If the notice is informal, how reliable is it? For example, an informal phone call from an investigating agency would be a fairly reliable indicator, while word of an investigation of another company with which the client does business would be much weaker.
- **What is the scope of the inquiry thought to be pending?** How serious a matter is under investigation? Is the client likely to be damaged if the fact of the investigation and the scope of the document retention to be required is discussed with the investigating agency?
- **How strong is the connection between the circumstances and the company?** How likely is it that the corporation possesses data that is relevant to the inquiry? What employees have access to this data? The lawyer should also consider the possibility that its actions at this point may alert target employees to the investigation.
- **What type of computer system does the client have?** At a minimum, a lawyer should gain some understanding of what types of computers, systems, and software the client is using.
- **Does the client have a document management system that accounts for electronic documents?** Does the client have a written policy? The lawyer should find out what the client's backup procedure is, and most importantly: how regularly documents are deleted.

B. The Effect of Notice on Existing Document Retention Programs

The effect of notice on existing document retention programs is one of the most unsettled questions in the area of electronic evidence. In other words, if documents are destroyed by the corporation pursuant to a pre-existing policy, to what extent is that a defense to later charges of spoliation or obstruction?

If documents are to be purged at all, they should be destroyed pursuant to an established, written retention policy. Having such a policy in place may provide an innocent explanation for the destruction of documents. If a client has such a policy in place, counsel should review it thoroughly.

Case law in the civil context suggests that continued use of a reasonable document retention program in the normal course of business may provide a justification for failing to produce requested evidence.[120] At the same time, sanctions have been assessed in civil cases against corporations that failed to suspend normal electronic document destruction policies.[121] For example, in *Linnen v. A.H. Robbins Co.*, the defendant had maintained several different software systems for providing intra-office communication capabilities over the years prior to the start of litigation.[122] Each of these systems was regularly backed up onto tapes, and the corporation's document retention policy provided for recycling of the backup tapes (deletion of the existing information) after three months of storage. The defendant failed to suspend the recycling process for three months after receiving plaintiffs' requests for the production of documents. As a sanction for the destruction of the backup tapes, the court granted plaintiffs' request for an adverse inference instruction.[123]

Considering the unsettled nature of the law, caution is required. This entails considering whether, and if so, how, the costly effort to preserve documents can be ameliorated by agreement with the investigating agency, and in any event advising the client to suspend established retention policies to the extent necessary for the corporation to comply with its duty to preserve evidence. Once the duty to preserve evidence arises:

> Clearly, it behooves respondent's counsel to advise clients to preserve existing computer data and, if necessary, disable any automated procedures on the computer that will destroy relevant evidence on the computer's storage. Further, counsel should advise corporate clients to include electronic data in its document retention program or be prepared to explain why data was unnecessarily retained or inadvertently destroyed.[124]

This admonition, while not likely to be popular with corporate executives in the short run, may offer the best means of insuring that a potentially bad situation is not made even worse.

---

* Douglas R. Young is a partner in the San Francisco law firm of Farella Braun & Martel LLP, where he heads the white collar crime group. He is a Fellow of the American College of Trial Lawyers, President of the Bar Association of San Francisco, immediate past President of the Northern California Chapter of the Association of Business Trial Lawyers, and past president of the California Academy of Appellate Lawyers. He can be reached at *dyoung@fbm.com*. He thanks Tania Mortensen, also of Farella Braun & Martel, for her help in preparing this article for publication.

[1] *See Commonwealth v. Copenhefer*, 526 Pa. 555, 587 A.2d 1353 (1991).

[2] *See United States v. Machado*, 195 F.3d 454 (9th Cir. 1999).

[3] *See id.*

[4] *See* Larry Neumeister, "Terror Trial Opens Against Embassy Bombing Suspect," SAN FRANCISCO CHRONICLE, Jan. 3, 2001, at A4.

[5] *See* J. Gregory Whitehair and Kimberly Koontz, "Discoverability of Electronic Data," Colorado Lawyer, Oct. 1998, at 45.

[6] Gregory S. Johnson, "A Practitioner's Overview of Digital Discovery," 33 Gonzaga Law Review 347, 358 (1998).

[7] *Ibid.*

[8] Mark D. Robins, "Computers and the Discovery of Evidence - A New Dimension to Civil Procedures," 17 JOHN Marshall Journal of Computer & Information Law 411, 414 (1999).

[9] *Ibid.*

[10] *Ibid.*

[11] Joan E. Feldman and Rodger I. Kohn, "The Essentials of Computer Discovery," in Third Annual Internet Law Institute, 564 PLI/PAT 51, 56 (1999).

[12] Gregory S. Johnson, *supra* note 6, at 367.

[13] Peter Brown, "Policies for Corporate Internet and E-Mail Use," in Third Annual Internet Law Institute, 564 PLI/PAT 637, 645-646 (1999).

[14] Electronic Evidence Discovery, Inc., "What You Need to Know About Use of Electronic Data in Litigation," May 18, 1999 (unpaginated, on file with author) (hereafter "What You Need to Know"). Electronic Evidence Discovery was founded in 1987 and provides a range of services geared toward assisting law firms and companies with electronic discovery.

[15] *See Armstrong v. Executive Office of the President, Office of Administration*, 1 F.3d 1274, 1283 (D.C. Cir. 1993) ("[T]he two documents cannot accurately be termed 'copies' -- identical twins -- but are, at most, 'kissing cousins.'").

[16] *See* Robins, *supra* note 8, at 414-15.

[17] *See* Susan E. Davis, "Elementary Discovery, My Dear Watson," California Lawyer, March 1996 at 54 (noting that system history files may also reveal attempts to destroy or obscure evidence).

[18] Kevin Andronos, "Legal Risk and Admissibility of Electronic Documents and Records," at 6 ¶ 4 (June 1997). <http://www.gtlaw.com.au/pubs/legalrisk.html> (visited Dec. 18, 2000).

[19] Robins, *supra* note 8, at 416.

[20] *See* Johnson, *supra* note 6, at 366-67.

[21] Davis, *supra* note 17, at 53.

[22] *Ibid.*

[23] *See* Robins, *supra* note 8.

[24] *Ibid.*

[25] *Ibid.*

[26] Jerry Adler, "When E-Mail Bites Back," Newsweek, November 23, 1998, at 45 (1998 WL 17010785).

[27] *Ibid.*

[28] Mike Tonsing, "Netscape Provides Lessons for Cyberian Lawyers," Federal Lawyer, January 1999, at 22.

[29] Electronic Discovery, Inc., "Recent Developments," August 1998, at 2.

[30] "What You Need to Know," *supra* note 14.

[31] Joan E. Feldman & Rodger I. Kohn, "The Essentials of Computer Discovery," in Third Annual Internet Law Institute, PLI/PAT 51, 53 (1999).

[32] *See id.* at 54.

[33] *See United States v. Microsoft Corp.*, 84 F. Supp. 2d 9 (D.D.C. 1999). On May 18, 1998, the federal government, along with 28 states, filed antitrust suits against Microsoft, alleging that it had unlawfully leveraged its monopoly in the Windows operating system. *See also* Aremen Artinyan, "Legal Impediments to Discovery and Destruction of E-Mail," 2 Journal of Legal Advocacy & Practice 95 (2000).

[34] *See* Adler, *supra* note 26.

[35] *See,* e.g., Armen Artinyan, *supra* note 33 at 111. *See also United States v. Microsoft Corp.,* No. 98-1232, U.S. District Court, District of Columbia. This document may be found at <http://www.usdoj.gov/atr/cases/f1700/1763.htm> (visited Jan. 18, 2001).

[36] *See* Artinyan, *supra* note 33, at 111.

[37] *See* Adler, *supra* note 26, at 45.

[38] *Ibid.*

[39] *Ibid.*

[40] "What You Need to Know," *supra* note 14.

[41] *See* Michael R. Overly, OVERLY ON ELECTRONIC EVIDENCE IN CALIFORNIA, § 6.01 (comment).

[42] *See id.*

[43] List adapted from John H. Jessen and Kenneth R. Shear, "The Role of Electronic Data Discovery in Today's Litigation," State Bar of California Litigation Section (1994) at 10.

[44] Many statutes and regulations require that businesses maintain certain records for stated periods of time. *See,* e.g., 29 U.S.C. § 1027 (ERISA records to be retained for six years). These requirements typically have their own sets of penalties for violations. *See,* e.g., 7 U.S.C. § 136i-1 (1999) (requiring use records for restricted pesticides); 7 C.F.R. § 110.3(d) (records required by foregoing statute to be kept for two years); 7 CFR § 110.7 (imposing civil penalties for failing to do so). *See also* Overly, *supra* note 41 § 6.01.

[45] *See United States v. Ruggiero*, 934 F.2d 440, 450 (2d Cir. 1991); *United States v. Platt*, 1985 WL 32444 *1 (N.D.Ill. Sept. 5, 1985).

[46] Even largely civil consequences, such as discovery sanctions, can be applied in quasi-criminal actions such as habeas corpus, forfeiture, contempt, civil penalty proceedings, antitrust actions, and injunctions.

[47] *See* Jamie S. Gorelick, "Effective Representation of the Corporation, Its Directors, Officers, and Employees in Grand Jury and Agency Investigations," in THE CORPORATE LITIGATOR at 670, 670 (1989).

[48] *See*, e.g., *United States v. Conneaut Industries, Inc.*, 852 F. Supp. 116, 125 (D.R.I. 1994) (corporation liable under obstruction statute, 18 U.S.C. § 1512, for document-tampering ordered by office manager who acted "because she realized that a federal proceeding could be commenced in the future").

[49] *Ruggiero,* 934 F.2d at 450 (2d Cir. 1991) (emphasis added).

[50] *United States v. Platt,* 1985 WL 3244 at *1.

[51] *Ibid.*

[52] *See*, e.g., *Braswell v. United States*, 487 U.S. 99, 108 S.Ct. 2284, 2285 (1988). In *Braswell*, the Court held that the government did not need to offer "act of production" immunity to a custodian of records of a corporate entity, even if the records would personally incriminate the custodian. *See ibid.* The Court suggested a possible exception when the custodian is the sole employee and officer of the corporation. *See id.* at 118-19, n11.

[53] *See In re Grand Jury Subpoena (Battle),* 748 F.2d 327, 330 (6th Cir. 1984); *In re Liberatore*, 574 F.2d 78, 83 (2d. Cir. 1978); *In re Grand Jury Proceedings (Guerrero),* 567 F.2d 281, 283 (5th Cir. 1978); *In re Hergenroeder*, 555 F.2d 686 (9th Cir. 1977) (per curiam). *But see In re Grand Jury Subpoena*, 697 F.2d 277 (10th Cir. 1983); *In re Grand Jury Proceedings (Schofield)*, 486 F.2d 85 (3d Cir. 1973).

[54] A grand jury subpoena duces tecum is unreasonably broad under Federal Rule of Criminal Procedure 17(c) if there is "no reasonable probability that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994).

[55] *Id.* at 13-14.

[56] *Id.* at 12-13 (noting that computers and electronic documents are simply analogues of earlier methods of storing information).

[57] U.S. Dept. of Justice, Criminal Division, Computer Crime and Intellectual Property Section, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, Jan. 2001, at Preface. This document may be found at <http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm>.

[58] *Id.* at § II.A.

[59] *Ibid.*

[60] *Id.* at § II.A.

[61] The website describes *computer forensics* as "the application of computer investigation and analysis techniques in the interests of determining potential legal evidence." <http://www.knock-knock.com/forens01.htm> (visited Dec. 21, 2000).

[62] <http://www.computerforensics.net/copgoals.htm> (visited Dec. 21, 2000).

[63] *See* U.S. Dept. of Justice, *supra* note 57, at § II.A.

[64] *Ibid.*

[65] *State v. Langlet*, 283 N.W.2d 330, 333 (Iowa 1979).

[66] *See ibid.*

[67] *Ibid.*

[68] *United States v. Marchesani*, 457 F.2d 1291 (6th Cir. 1972).

[69] *See id.* at 1298.

[70] *Ibid.*

[71] *State v. Hilbert*, 14 S.W.3d 249, 253 (Mo. 2000).

[72] *Langlet*, 283 N.W.2d at 333.

[73] *See id.* at 332

[74] *Vick v. Texas Employment Commission*, 514 F.2d 734, 737 (5th Cir. 1975).

[75] *Anderson v. Litzenberg*, 115 Md. App. 549, 561, 694 A.2d 150, 156 (1997).

[76] *See* F.R. Civ. Proc. 37(b)(2) (2000).

[77] *See*, e.g., Cal. Civ. Proc. Code § 2023(b) (1998).

[78] *See* California Penal Code § 1054.3 (West Supp. 2001). For a case upholding the constitutionality of California's reciprocal criminal discovery procedure, see *Izazaga v. Superior Court*, 54 Cal.3d 356, 815 P.2d 304, 285 Cal.Rptr. 231(1991).

[79] 18 U.S.C. § 1503 (1996) provides that: "[W]hoever corruptly . . . influences, obstructs, or impedes, or endeavors to influence, obstruct, or impede, the due administration of justice, shall be punished . . . ."

[80] *See*, e.g., *United States v. Lundwall*, 1 F.Supp.2d 249, 251 (S.D.N.Y. 1998) (prosecution under § 1503 for destroying evidence sought by discovery in civil case); *United States v. Ruggiero*, 934 F.2d 440 (2d Cir. 1991) (prosecution under § 1503 for concealing documents from grand jury).

[81] *See* Solum and Marzen, "Truth and Uncertainty: Legal Control of the Destruction of Evidence," 36 EMORY LAW JOURNAL 1085, 1109-1110 (1987).

[82] *See*, e.g., *United States v. Lench*, 805 F.2d 1443 (9th Cir. 1986) (affirming defendant's sentence for obstruction of justice where vice-president of corporation had instructed employees to destroy relevant materials and had moved boxes containing relevant documents after representing that the corporation did not maintain such records); *United States v. Faudman*, 640 F.2d 20 (6th Cir. 1981) (altering corporate records subpoenaed by a grand jury violated § 1503).

[83] *See United States v. Washington Water Power Co.*, 793 F.2d 1079, 1085 (9th Cir. 1986).

[84] *See United States v. Jeter*, 775 F.2d 670, 679 (6th Cir. 1985), *cert. denied*, 475 U.S. 1142 (1985); *United States v. Rasheed*, 663 F.2d 843, 852 (9th Cir. 1981), *cert. denied*, 454 U.S. 1157 (1982). *See also* Matthew J. Bester, "A Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence" (Comment), 6 CommLaw Conspectus 75, 80-81 (1998).

[85] *United States v. Neiswender*, 590 F.2d 1269 (4th Cir. 1979).

[86] *See id.* at 1274 (concluding that the intent may be inferred from the natural and probable consequences of a defendant's acts).

[87] *See* Joseph V. De Marco, "A Funny Thing Happened On the Way To the Courthouse: Mens Rea, Document Destruction, And the Federal Obstruction of Justice Statute," 67 New York Univ. Law Review 570, 581-583 (1992).

[88] Support for the *Neiswender* approach can be found in the Second, Seventh and Eleventh Circuits. *See,* e.g., *United States v. Buffalano*, 727 F.2d 50, 54 (2d Cir. 1984); *United States v. Machi*, 811 F.2d 991, 998 (7th Cir. 1987); *United States v. Thomas*, 916 F.2d 647, 651 (11th Cir. 1990). For a fuller discussion of the *Neiswender* approach, and jurisdictions in which it has been adopted, *see* De Marco, *supra* note 87.

[89] *See* De Marco, *supra* note 87, at 601-603.

[90] 18 U.S.C. § 1505 (2001) provides: "[w]hoever corruptly, . . . obstructs, or impedes or endeavors to . . . obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress, shall be fined . . . ." Section 1505 also provides punishment for "[w]hoever, with intent to avoid, evade, prevent, or obstruct compliance, in whole or in part, with any civil investigative demand duly and properly made under the Antitrust Civil Process Act, willfully withholds, misrepresents, removes from any place, conceals, covers up, destroys, mutilates, alters, or by other means falsifies any documentary material, answers to written interrogatories, or oral testimony, which is the subject of such demand; or attempts to do so or solicits another to do so . . .".

[91] John M. Fedders and Lauryn H. Guttenplan, "Document Retention and Destruction: Practical, Legal and Ethical Considerations," 56:5 Notre Dame Lawyer 24 (1980) (internal numbering omitted). *Compare Rice v. United States*, 356 F.2d 709, 714 (8th Cir. 1966) (holding filing of charges adequate to trigger Section 1505) *with United States v. Fruchtman*, 421 F.2d 1019, 1021 (6th Cir. 1970) (preliminary staff investigation constitutes "proceeding" under 1505).

[92] *See* S. Marzen and L. Solum, *supra* note 81, at 1189-1191.

[93] *See ibid.*

[94] 18 U.S.C. § 1510(a) provides that: "Whoever willfully endeavors by . . . misrepresentation . . . to obstruct, delay, or prevent the communication of information relating to a violation of any criminal statute of the United States by any person to a criminal investigator shall be fined . . . , or imprisoned . . . ." As used in this section, the term "criminal investigator" means "any individual duly authorized by a department, agency, or armed force of the United States to conduct or engage in investigations of or prosecutions for violations of the criminal laws of the United States." 18 U.S.C. § 1510(c) (2001).

[95] *See United States v. Lippman*, 492 F.2d 314, 316 (6th Cir. 1974), cert denied, 419 U.S. 1107 (1975) (upholding constitutionality of statute).

[96] 18 U.S.C. § 371 (2001) provides that: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

[97] *See United States v. Hartley*, 678 F.2d 961, 972 (11th Cir. 1982).

[98] For a discussion of the application of Section 371 in the context of document destruction, see generally Fedders and Guttenplan, *supra* note 92 at 31 ("The Department of Justice has brought conspiracy charges against persons who selectively destroy corporate records after a subpoena has been issued. It is especially likely to bring such charges when the obstruction has been thwarted or an essential element of the substantive offense is missing. Yet conspiracy charges are difficult to prove, and may unnecessarily complicate the prosecution's task since conspiracy requires proof of three elements while obstruction only requires proof that a single person acted deliberately to obstruct justice.").

[99] 18 U.S.C. § 401 (2001) provides that: "A court of the United States shall have power to punish by fine or imprisonment, at its discretion, such contempt of its authority, and none other, as — (1) Misbehavior of any person in its presence or so near thereto as to obstruct the administration of justice; (2) Misbehavior of any of its officers in their official transactions; (3) Disobedience or resistance to its lawful writ, process, order, rule, decree, or command."

[100] *See* Solum and Marzen, *supra* note 81, at 1113. For further discussion of the contempt statute in relation to document destruction, *see* Fedders and Guttenplan, *supra* note 91, at 31-34.

[101] Indeed, courts have sometimes found a single act of document destruction to violate both statutes. *See,* e.g., *United States v. Walasek*, 527 F.2d 676, 680 (3d Cir. 1975).

[102] 18 U.S.C. § 4 (2001) provides that: "Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both."

[103] *See* Florida Stat. § 918.13 (2001).

[104] *See* California Penal Code § 135 (1999).

[105] *See* Solum and Marzen, *supra* note 81, at 1115. At the time their article was written in 1987, 36 states and the District of Columbia had document destruction statutes. *Ibid. See also* Fedders and Guttenplan, *supra* note 91 at 35-36.

[106] U.S. SENTENCING GUIDELINES MANUAL, § 3C1.1 (2000).

[107] *Id.* at Application Note 4(d).

[108] *See United States v. Charria*, 919 F.2d 842, 849 (2d Cir. 1990), *cert. denied* 502 U.S. 813 (1991) (holding obstruction determination proper where defendant lied to government agents about drug records and attempted to destroy documents).

[109] *State v. Vaughn*, 83 Wash. App. 669, 679 P.2d 27, 33 (1996).

[110] *See id.* at 30.

[111] Model Rules of Professional Conduct Rule 3.4(a) comment 2 (1999). *See also* Huang and Muriel, "Spoliation of Evidence: Defining the Ethical Boundaries of Destroying Evidence," 22 American Journal of Trial Advocacy 191, 192-98 (1998)(discussing the ordinary course of business exception to the imposition of sanctions under MRPC 3.4(a) and noting that "courts have refrained from imposing sanctions . . . in two situations: (a) when the act of destruction occurred in the ordinary course of business; and (b) when the act was not motivated by consciousness of a weak case.").

[112] *See* Solum and Marzen, *supra* note 81 at 1136. In California, an attorney is also subject to discipline under the Business & Professions Code. *See* Cal. Bus. & Prof. Code § 6106 (1990) ("The commission of any act involving moral turpitude, dishonesty or corruption . . . constitutes a cause for disbarment or suspension.").

[113] *See* Solum and Marzan, *supra* note 81 at 1136. One author posits the following scenario: Suppose an attorney visits a corporate client's archives and determines that the MPC requires the attorney to directly convey certain documents to the government. Suppose further that the attorney determines to contact the U.S. Attorney responsible for the matter the following morning in order to arrange for the transfer of the documents, but that the documents are destroyed pursuant to the corporation's regular document retention policy that evening. Under the approach followed in some jurisdictions, the attorney could be charged with obstructing justice as long as the destruction of documents was reasonably foreseeable. *See* DeMarco, *supra* note 87, at 603-604.

[114] *Bratka v. Anheuser-Busch,* 164 F.R.D. 448 (S.D. Ohio 1995).

[115] *Id.* at 460. While Busch's counsel claimed his failure to produce certain highly relevant and responsive documents was due to inadvertence, the manner in which he conducted his search for documents reveals several crucial mistakes. *See id.* at 457. First, he left the responsibility for obtaining documents entirely to Mr. Bassett, Busch's in-house counsel. *See id.* at 460. Bassett then designated responsibility to a corporate risk manager, a non-lawyer, to collect responsive documents without giving him specific instructions or supervision. *See id.* at 461. Bassett further failed to ask the one person who was likely to have the most information relevant to plaintiff's discovery request to collect documents. *See id.* at 458.

Finally, in-house counsel did not recheck the manner in which the risk manager had carried out his assignment to retrieve documents. *See id.*

[116] *Id.* at 460.

[117] *Id.* at 461.

[118] *Cedars-Sinai Medical Center v. Superior Court*, 18 Cal. 4th 1, 13, 954 P.2d 511, 74 Cal.Rptr.2d 248 (1998).

[119] *Ibid.*

[120] *See Carlucci v. Piper Aircraft Corp*, 102 F.R.D. 472, 486 (S.D. Fla. 1984) (noting that a "reasonable" document retention program might survive judicial review, and suggesting that "the good faith disposal of documents pursuant to a bona fide, consistent and reasonable document retention policy" might provide a justification for failing to produce documents in response to discovery requests).

[121] *See Linnen v. A.H. Robbins Co,* 1999 WL 462015, at *11 (Mass. Super. June 16, 1999); *Hartford Ins. Co. of the Midwest v. American Automatic Sprinkler Systems Inc.*, 23 F. Supp. 2d 623, 626 (D. Md. 1998) (noting that a court has broad discretion to permit a jury to draw adverse inferences from a party's failure to preserve evidence, even in the absence of bad faith).

[122] *See Linnen,* 1999 WL 462015, at *11. *But see New York State N.O.W. v. Cuomo*, 1998 WL 395320, at *2-3 (S.D.N.Y. July 14, 1998) (adverse instruction unavailable where destruction occurred as part of a general purging of records, and thus was merely negligent rather than an intentional effort to impede litigation).

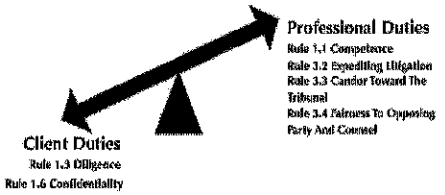
[123] *See Linnen,* 1999 WL 462015, at *11.

[124] Susan Silvernail, "Electronic Evidence: Discovery in the Computer Age," 58 Alabama Lawyer, 176, 180 (1997).

Ethics of Electronic Discovery – Part Two

For Part One, see here.

Ethical Analysis of the Hypothetical



What ethical considerations and rules or professional conduct come into play in this scenario? Let us analyze the facts of the hypothetical one rule at a time and consider the impact of all six of the key rules: Rule 1.1 – Competence; Rule 1.3 – Diligence; Rule 1.6 – Confidentiality; Rule 3.2 – Expediting Litigation; Rule 3.3 – Candor Toward the Tribunal; and, Rule 3.4 – Fairness to Opposing Party and Counsel.

Competence. The competency issue here is critical, as it is in most ethical considerations. One party here, the plaintiffs' counsel, does not really understood e-discovery. For instance, they did not really understand many of the technical reasons behind defendant's position, such as deduplication and email copies throughout the system, nor the sampling disclosures. They did not understand the benefits of phased discovery and going first for the low hanging fruit, the emails of the best key custodians.

They did not cooperate in e-discovery because they did not know how. They probably had never even seen the cooperative model in action before, and so when they saw it here, they did not recognize it. They may instead have mistaken it for weak or timid opposing counsel. It just provoked them to be more *caveman* like. They got more aggressive in the face of the unknown. They also ran away from any real discussion on technical issues. A classic case of the *fight or flight* instincts of a pre-computer-literate-lawyer faced with e-discovery.

Plaintiffs' counsel in this hypothetical did not trust the other side because they assumed they were like them. They were not competent enough to recognize or understand the new approach. They only understood "cooperation" from the outside, as just another tool, or keyword, in the game of hide-the-ball. They certainly had not read Professor Gensler's article and had no understanding at all on how the new cooperative, trans-negotiation model might help their clients. In Professor Genzler's words:

The Cooperation Proclamation is exactly right when it urges lawyers to see cooperation as a means for advancing their clients' interests and not as a retreat from their duties as loyal advocates. As I have written elsewhere, the lawyers who default to battle mode in discovery – who fail even to consider whether cooperation might yield better results – are the ones who truly fail to serve their clients' interests.

The Bull's-Eye View of Cooperation in Discovery, 10 Sedona Conf. J. 363, at 363 (2009 Supp.)

They had also not read the article by the Sedona Conference making the legal case for cooperation, *The Case for Cooperation, supra.* The editor-in-chief of this article was well-known plaintiff's counsel, William P. Butterfield. The concluding paragraph of *The Case for Cooperation* succulently warns of what may happen to our system of justice if the new cooperative model to discovery is not adopted:

If parties are expected to continue to manage discovery in the manner envisioned by the Federal Rules of Civil Procedure, cooperation will be necessary. Without such cooperation, discovery will become too expensive and time consuming for parties to effectively litigate their disputes.

The Case for Cooperation, Id. at 362.

Plaintiffs' counsel here did not even seem to understand what most truly competent plaintiff's counsel do, that every dollar spent on useless discovery is another dollar not available for settlement. The best, most competent counsel have always saved their powder for the real battles that count, on the law and application of the law to the facts. They have always understood that the true, and only valid purpose of discovery is to get at the key facts to allow reasoned evaluation of the case, not to prepare mountains of data, or extort the responding party, or bury the requesting party in a document dump. Competent legal counsel do not engage in *discovery as abuse*. Those that do soon develop a reputation that follows them into a court room, even if it is on the other side of the country of where they usually practice. *See Discovery As Abuse*, 69 B.U. L. REV. 635 (1989). As the Sedona Conference noted, the "risk of gaining a reputation among the judiciary as unduly combative during discovery, encourages cooperative behavior." *The Case for Cooperation, supra* at pg. 362.

The only possible conclusion here is that Plaintiffs' were not competent to handle the e-discovery issues in this class-action employment case. For that reason alone, under this scenario they behaved unethically. They violated Rule 1.1.

Many attorneys in this situation attempt to meet their ethical obligation of competence by hiring an e-discovery vendor to advise them. Unfortunately, this usually does not work, for such *experts* frequently only tell the attorneys who hired them what they want to hear. The *hired guns* simply supply arguments jazzed up with tech-speak to support the legal argument of the attorneys who hired them.

In any event, e-discovery vendors are technologists, not lawyers, and even when a rare e-discovery expert at a vendor does also have a law degree, they do not provide legal advice. They are not allowed to provide legal advice. The only way an attorney who is not competent in the law and practice of e-discovery can fulfill their ethical duty is by taking the time and considerable efforts needed to become competent, or by bringing in legal counsel who is competent to assist him or her. Vendors cannot do that. They cannot render legal advice, but I appear to be the only one pointing out that obvious fact. See *EDRM Model Code of Conduct*. In fact, the EDRM proposed vendor ethical code of conduct, *Principle 4 – Sound Process*, seems like it encourages vendors to provide legal advice: "Service Providers should define, implement

and audit documented sound processes that are designed to preserve legal defensibility." This is a gray I know, but I strongly encourage the experts who are involved in this EDRM project to carefully consider the whole UPL issue and clarify draft Principle 4 and its comments on *legal defensibility*. By the way, except for my issue with Principle 4 and UPL, I am favorably impressed with the proposed model e-discovery vendor ethics guidelines that EDRM has come up with and encourage all vendors to study it carefully.

Diligence. Plaintiff's counsel here thought they were being diligent because they were engaging in what they saw as vigorous advocacy. Too bad they were playing the wrong game. True vigorous advocacy here would have entailed detailed examination of the reasons provided by defense counsel for the five custodians and seven issues. It would have required reciprocal disclosures on their part on their thinking and analysis of the importance of the various custodians to the case. Diligence would have required immediate study of the emails produced. It would have taken the dispute out of rhetoric and knee-jerk opposition to everything the other side proposes, and into the facts and legal analysis.

Plaintiffs' counsel in this scenario was not diligent at all. Their incompetence made that impossible. They thought they were being very diligent, and no doubt so did their clients, who are usually very easily impressed by the kind of saber-rattling in which they engaged. But in fact they did all of the wrong things. They engaged in knee-jerk opposition to everything the other side proposed, and this pretend diligence was really not diligent at all. Discovery as abuse is not an exercise in competent diligence. It is abuse, pure and simple.

Confidentiality. Plaintiffs' counsel here thought they were being very ethical by refusing to disclose their work product. They would not give the defendant an idea on their thinking of the case, on what information they thought would be highly relevant. They would not disclose why they thought some custodians and issues were more important. That was their confidential thinking, and they thought they should keep it secret. They hoped to keep their analysis of the case (assume they had one, and this was not just a superficial form-driven lawsuit) to themselves. They wanted to surprise defendants as much as possible. Indeed, they were initially surprised by how much confidential information the defense counsel here provided, which, again, they mistakenly mistook as a sign of weakness and egged them on to keep demanding more and more. Then they were surprised again when defense counsel said no, and never budged from the initial 5/7. And finally were surprised again by the court ruling against them and went with the defense plan.

So which attorneys in this scenario met their ethical duty under Rule 1.6 to "not reveal information relating to the representation of a client" and which did not? Rule 1.6 has numerous exceptions to the duty of client confidentiality, including where the client gives informed consent or the "disclosure is impliedly authorized in order to carry out the representation."

Here the disclosure by defense counsel was needed to carry out the representation and so impliedly authorized, even if not specifically authorized. Note that under the scenario no attorney-client privileged documents are disclosed, nor any privileged communications. Even client confidential documents are protected under a strong confidentiality order. Any non-

relevant documents produced would also be covered by the confidentiality order and would be promptly returned. Further protection was provided by a strong clawback order.

The only confidential information disclosed here is *some* of the work-product privileged thinking and analysis of defense counsel. Unlike the attorney-client privilege, which is held by the client and can only be released by the client, the work-product privilege is held by the attorney, and released by the attorney. The disclosure of the attorney's work product was made here to advance their client's interests. It was made to facilitate efficient, cost-effective search and production, and later to obtain a protective order preventing unduly burdensome, disproportionate e-discovery. This kind of disclosure does not violate defense counsel's duties under Rule 1.6.

My conclusion is based on an understanding of how work product privilege waiver is different from attorney-client privileged waiver. It does not automatically open up the door for further inquiries as attorney-client waiver might do. My thanks to Professor Mark S. Sidoti, who is part of Professor Hamilton's excellent email discussion group for e-discovery professors, full-time and adjunct. Professor Sidoti, whose day job is at Gibbons, pointed out a key case in this area, *Williams & Connolly LLP v. U.S. Securities and Exchange Commission,* 2010 U.S. Dist. LEXIS 78570 (D.D.C. Aug. 4, 2010):

The work product doctrine protects both deliberative materials such as mental impressions, conclusions, opinions, and legal theories and factual materials prepared in anticipation of litigation. *** In his declaration in support of summary judgment, David Frohlich, an Assistant Director in the SEC's Division of Enforcement, explains that the handwritten notes sought by Plaintiff were generated during the Cendant investigation in anticipation of litigation with Mr. Corigliano, Mr. Kearney, and others. Plaintiff does not dispute this statement and concedes that these documents qualify as attorney work product. However, Plaintiff contends that the SEC has waived any work product privilege with respect to these documents because similar handwritten notes were disclosed to Plaintiff during the criminal prosecution of Mr. Forbes. According to the declaration of Christopher R. Hart, an attorney at Williams & Connolly LLP, at least eleven of the documents of handwritten notes identified in the Vaughn index were produced by the government during the Forbes matter. Plaintiff thus contends that the government has "waived the work product privilege as to entire subject matter of handwritten notes between SEC staff and Corigliano, Kearney, or their respective counsel."

As with the attorney-client privilege, a party may waive the work product privilege through disclosure. *See In re United Mine Workers of Am. Employee Benefit Plans Litig.*, 159 F.R.D. 307, 310 (D.D.C. 1994) ("It seems . . . clear in this Circuit that the disclosure of documents protected by the attorney work product privilege waives the protections of the attorney work product privilege as to the documents disclosed."). **However, "the test for waiving attorney work product protection is more stringent than the test for waiving attorney-client privilege."** *Goodrich Corp. v. U.S. Envtl. Prot. Agency*, 593 F. Supp. 2d 184, 191 (D.D.C. 2009). Although disclosure of documents waives attorney-client privilege with respect to all other communications related to the same subject matter, **the scope of "subject matter waiver" with respect to work product materials is more limited. "[A] subject-matter waiver of the attorney work product privilege should only be found when it would be inconsistent with**

the purposes of the work product privilege to limit the waiver to the actual documents disclosed." "Several factors figure into the analysis: whether disclosure was intentional or inadvertent, the breadth of the waiver sought, and the extent to which the requested documents would reveal litigation strategies or trial preparations." (emphasis added)

The law provides greater protection to work-product waiver and so the disclosures made in the hypothetical should leave defense counsel protected from any further unwanted intrusions. *Also see* Rule 502 *Federal Rules of Evidence*, and note that our hypothetical assumes a strong confidentiality and clawback order under Rule 502(d).

As for the conduct of plaintiff's counsel, it may surprise you to know that I do not conclude they have violated Rule 1.6. I must conclude that plaintiffs stonewalling actions in this case are also consistent with Rule 1.6. Although their behavior in this hypothetical was unethical under the other rules here considered, it was not under Rule 1.6. They have the right to keep all of their work product to themselves, even though it was stupid to do so, and thus a probable violation of Rule 1.1 on competence, but it is was *their* work-product. Of course, no rule should be considered in isolation, and work-product thinking is required to be disclosed under many rules of civil procedures, including especially Rule 26(f), and any time you are seeking relief from the court, or making final preparation for trial, not to mention trial itself.

In the same professorial discussion group my esteemed LegalTech debating adversary, Professor Craig Ball, had this to say concerning the policy behind limited work product disclosures, starting with a comment on pre-digital paper productions:

You may argue that we never got to look behind a lawyer's decisions to produce or withhold even if the lawyer made the selections by throwing documents down the stairs and producing only what hit the next landing. But perhaps that's not an approach we want to replicate in post-digital practice. We indulged ourselves in the belief that, right or wrong, relevance and privilege determinations were a lawyer's to make and largely immune from being second-guessed absent evidence of gross dereliction or misconduct. But, as we move into the realm of search technology–and especially those like keyword search only lately appreciated to be deeply flawed–the tools and methods employed must be closely examined and tested, including by exposing them to adversarial challenge.

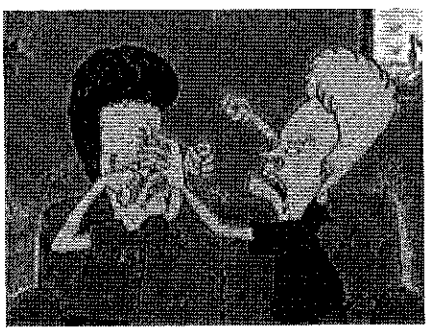
Perhaps we need to step away from our reflexive "we are lawyers and we are special," in order to consider what approaches are calculated to best serve the ends of justice. Cooperation demands communication. If you believe the first is more than a pipe dream, you need to embrace the latter.

I have to agree with Craig on this one. Opposing counsel need to talk with each other and explain what they are doing in the area of search and production. You do not have to give up all your trade secrets, nor reveal all of your strategies, but you have to be prepared to disclose enough to show your reasonable, good faith efforts. What does cooperation look like? It looks like lawyers talking and making mutual disclosures needed to plan discovery in a case.

Expediting Litigation. The conduct of plaintiffs' counsel here violated their duty to expedite litigation. They did so in spite of the fact that expedited litigation is almost always consistent with a plaintiff's interest in a civil proceeding for a speedy trial. Plaintiffs' counsel here unethically violated this duty to expedite by forcing unnecessary motion practice. Further, the closed approach of plaintiffs' counsel to try to conceal the facts they really wanted in discovery probably also violated Rule 3.2, even of it did not violate Rule 1.6. *See eg. DeGeer v. Gillis,* 755 F. Supp. 2d 909, 930 (N.D. Ill. 2010) (if parties had participated in "candid, meaningful discussion of ESI at the outset of the case," expensive and time consuming discovery and motions practice could have been avoided).

Candor Toward the Tribunal. I think the conduct of plaintiffs' counsel in this hypothetical violated this fundamental Rule of Professional Conduct too, but admit their violation might be seen as technical, and is certainly the kind of conduct that goes on every day and is tolerated by both Bench and Bar. Plaintiffs' counsel here did not "*make a false statement of fact or law to a tribunal ... or, offer evidence that the lawyer knows to be false.*" But they did not provide the whole truth either. They made a demand in their motion to compel for 30 custodians and 30 issues, and they continued in this demand at the hearing before the tribunal. Let us assume that they also made oral representations to the judge at a hearing that they thought this 30/30 demand was necessary and appropriate under the facts of the case and governing law. But that is at best a half-truth because they have been willing all along to accept 20/20.

For that reason they did not display the kind of candor to the tribunal that I personally think is appropriate. Instead, they continued to play the only game they knew how, the *negotiation game*, and they treated the judge as just another player in the game. In a negotiation game, you are never completely candid. That would defeat the whole point of the game. If plaintiff's counsel here were in fact candid to the tribunal, they would admit that 20/20 is their goal, but then again, that could be a slippery slope for them. It could also lead to admission of their basic incompetence to do e-discovery to begin with, to engage in meaningful discussion and analysis, much less to enter into a true cooperative dialogue with the other side.



Fairness to Opposing Party and Counsel. Some attorneys are surprised when they see the terms of this important Rule of Professional Conduct. Candor to the tribunal is one thing, but fairness to the opposing party and their attorneys? That is simply not part of the culture of many lawyers and law firms! They seem surprised when they are reminded that the requirement is built into our rules of ethics. It is not a mere professional courtesy, as some think, it is an ethical imperative. Under Rule 3.4 a lawyer shall not "*unlawfully obstruct another party's access to evidence.*" A lawyer shall not "*conceal a document or other material that the lawyer knows or*

reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act." A lawyer shall not in "*make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party.*"

The attorneys for the party responding to the discovery request in this hypothetical, defense counsel, complied with their ethical duties. My conclusion assumes that they sought to limit discovery for the grounds stated, burdensomeness and likely relevance. I assume they did not have any bad faith ulterior motives, such as an attempt to conceal evidence that they knew to be unfavorable to their client. I assume they were not just trying to obstruct access to evidence or conceal relevant ESI. Finally, I assume that their search and production efforts were reasonably diligent.

With these assumptions I conclude defense counsel acted ethically because their refusal to review and produce any more that five custodians and seven issues in the first round of phased discovery did not prevent disclosure of any evidence they knew to be relevant, and did not prevent plaintiffs' later discovery from other custodians or issues that might prove necessary. It might *delay* it to a second phase, but not *prevent* it. If defense counsel should uncover a document outside of this scope, one that is obviously relevant, then under this rule they would be required to disclose such a document and should not conceal it.

I conclude to the contrary that under the given facts plaintiffs' counsel violated the duty of fairness to opposing counsel because their initial request for discovery was frivolous. They signed and served a discovery request for 50 custodians and 50 issues, knowing that was excessive, and for that reason quickly dropping to 30/30, and ready to accept 20/20, which is what they really thought was reasonable all along. They used a request for production as a mere negotiation tool, and in so doing made an unethically frivolous discovery request. Note they also violated Rule 26(g) FRCP, which Judge Grimm in *Mancia* said was the most misunderstood and under utilized of all rules of procedure. Rule 26(g) is similar to Rule 11, but applies only to the discovery pleadings. Rule 26(g)(1)(B) states that a signature on a discovery request constitutes an attorney's certification that the request is:

(ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and…

(iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

They thought 20 custodians and 20 issues was proportional, yet they signed a request for production seeking 50. They did so for purposes of setting up a negotiation. This is, I suggest, an improper purpose under 26(g)(1)(B)(ii). They knew 50 was unreasonable and unduly burdensome, yet they still signed the discovery request. Plaintiffs counsel in this hypothetical thereby intentionally violated 26(g)(1)(B)(iii) triggering a mandatory obligation under the rule for the court to impose sanctions.

This conduct by the requesting party was not only a civil rule violation, it was unethical. It violated Professional Rule of Conduct 34(c) by "knowingly disobeying an obligation under the rules of a tribunal," namely Rule 26(g)(1)(B) and as explained before, violated ethics Rule 3.4(d) because it was frivolous.

Conclusion

Some may say my hypothetical is far-fetched, that attorneys do not engage in this type of behavior. I say, *get real.* It is an everyday occurrence. The only thing far-fetched about it is the simplicity of the facts, which I necessary injected into the hypothetical, and, the relatively mild nature of the violations. In my position as national e-discovery counsel for a 700 attorney law firm with 48 offices around the country, I see equivalent or worse behavior by opposing counsel almost every week. It is not exactly a crazy hell-zone as I used to suspect, and many still believe. *Krueger v. Pelican Products Corp.*, C/A No. 87-2385-A (W.D. Okla. 1989) (J. Alley) ("If there is a hell to which disputatious, uncivil, vituperative lawyers go, let it be one in which the damned are eternally locked in discovery disputes with other lawyers of equally repugnant attributes.") But it is bad, and we need to work together as a profession to break out of this prison.

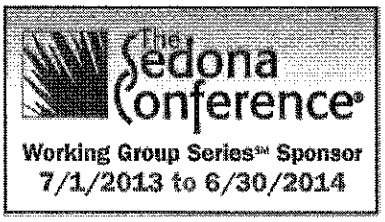
Even though this hypothetical is an all-too-common scenario, as far as I know, no attorney has ever been reprimanded for an ethical violation of Rule 34 upon these circumstances. This ethics rule, like the 26(g) procedure rule, is a paper tiger. Indeed, you could say that about all of the ethics rules here discussed in the context of e-discovery. It is a new area of the law and State Bar Associations are naturally reluctant to enforce its rules in this virgin territory.

But just because attorneys are no yet being reprimanded or losing their licenses for these kinds of rule violations, does not mean we should not care about compliance. Following these well-established rules is the best way to stay on the *straight and narrow* when it comes to e-discovery. We cannot let old *hide-the-ball* practices morph into *hide-the-byte* operating systems.

Compliance with the rules of professional conduct, and the new doctrine of Cooperation that implements these rules (and the rules of civil procedure as Judge Grimm and Professor Genzler have pointed out), is the best way to avoid the threat warned of by Sedona and many others. It is the best way to avoid a future world of litigation where standard *hide-the-byte* operating systems make "*discovery too expensive and time consuming for parties to effectively litigate their disputes.*" *The Case for Cooperation, Supra* at 362.

Although a good argument can be made for the enactment of more new rules of civil procedure to adapt to the challenges of e-discovery, new rules of professional conduct are not needed. The ones we have are sufficient to guide us, but we need to take the time and effort to study and understand these rules. We need to discuss these rules and how they apply to the new situations presented in e-discovery practice. It is my hope that this early effort in that direction will stimulate more discussion and analysis of the subject.

Sedona Principles, 2nd Ed.



1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

5. The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

11. A responding party may satisfy its good faith obligation to preserve and produce relevant electronically stored information by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.

14. Sanctions, including spoliationfindings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

HOW MUCH DATA DO YOU HAVE?

CD = 650 MB = 50,000 pages. DVD = 4.7 GB = 350,000 pages. DLT Tape = 40/80 GB = 3 to 6 Million pages.
Super DLT Tape = 60/120 GB = 4 to 9 Million pages.

****

Page Estimates:
1 MB is about 75 pages;
1 GB is about 75,000 pages (pick-up truck full of documents).

Aver. pgs. per email: 1.5 (100,099 pages per GB).
Aver. pgs. per word document: 8 (64,782 pages per GB).
Aver. pgs. per spreadsheet: 50 (165,791 pages per GB).
Aver. pgs. per power point: 14 (17,552 pages per GB).

****

For the average .PST or .NSF Email File:
100 MB .PST file is 900 emails and 300 attachments.
400 MB .PST file is 3,500 emails and 1,200 attachments.
600 MB .PST file is 5,500 emails and 1,600 attachments.
A 1.00 GB .NSF file is 9,000 emails and 3,000 attachments.
A 1.5 GB .NSF file is 13,500 emails and 4,500 attachments.

****

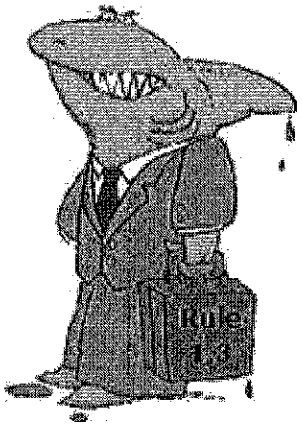
Note: Many variables will affect ALL of the actual numbers above, including especially large image and video files, and recursive files.

****

Bits and Bytes Sizes:
•8 bits are equal to 1 ***byte*** *(one or two words),*
•1,024 bytes are equal to 1 ***kilobyte (KB).***
•1,024 kilobytes (KB) are equal to 1 ***megabyte (MB or Meg).***
•1,024 megabytes are equal to 1 ***gigabyte (GB or Gig)*** *(truck full of paper).*
•1,024 gigabytes are equal to 1 ***terabyte (TB)*** *(50,000 trees of paper).*
•1,024 terabytes are equal to 1 ***petabyte (PB)*** *(250 Billion Pgs. of Text).*
•1,024 petabytes are equal to 1 ***exabytes (EB)*** *(1 000 000 000 000 000 000 bytes).*

http://e-discoveryteam.com/2012/03/04/ethics-of-electronic-discovery-part-one/

Ethics of Electronic Discovery – Part One



I have been interested in the ethical issues surrounding electronic discovery since 2006. At that time I phased out my general trial practice, went full-time e-discovery, joined The Sedona Conference®, and started this *e-Discovery Team®* blog. As part of my practice I read most of the opinions around the country written on e-discovery. I quickly noticed something I had not seen before in any other field of law. The case law is dominated by sanctions cases involving spoliation of evidence. Not only that, attorneys are often directly implicated in this spoliation and accused of many other types of intentional or negligent misconduct. I began to wonder if I had stepped into a crazy zone of the law where all attorneys acted like sharks.

This suspicion me to think, write, and speak often on the subject of e-discovery ethics, which culminated in my article, *Lawyers Behaving Badly: Understanding Unprofessional Conduct in e-Discovery,* 60 Mercer L. Rev. 983 (Spring 2009). The article led to my participation in a full day academic seminar on the subject at Mercer Law School with noted e-discovery experts, Judge John Facciola, Judge David Baker, Jason R. Baron, William Hamilton, and Professor Monroe Freedman, and Chilton Varner, the transcript for which is published at 60 Mercer L. Rev. 863 (Spring 2009). I came to understand that I had not wandered into a special zone of hell, and that lawyers doing e-discovery were no worse, or no better, than other lawyers. But they were put to special challenges and conditions unique to this new field of law, and the end result was many more errors in judgment than you can find anywhere else. These errors continue as shown by surveys of case law. *See eg.* Willoughby, Jones, Antine, *Sanctions for E-Discovery Violations: By the Numbers, 60 Duke L.J. 789 (2010).*

Lawyers Behaving Badly

In my 2009 law review article, Lawyers Behaving Badly, I concluded that:

[T]he profession has not suddenly become more sinister than before. Although, some suggest that the dominance of large firms as mega-business enterprises is causing a significant decline in overall ethics. See Marc Galanter & William Henderson, The Elastic Tournament: A Second Transformation of the Big Law Firm, 60 STAN. L. REV. 1867 (2008). There may be some truth to this, but a general decline in ethical standards does not explain why e-discovery jurisprudence is so rife with malfeasance.

Id. at pg. 985. Instead, I hypothesized four reasons to explain the apparent frequent bad behavior of so many attorneys in the field of electronic discovery:

There are four fundamental forces at work in e-discovery, which when considered together, explain most attorney misconduct:

(1) a general lack of technological sophistication,

(2) over-zealous attorney conduct,
(3) a lack of development of professional duties as an advocate, and
(4) legal incompetence.
These "Wicked Quadrants" are depicted in the circular diagram below.

I am not going to explore the ins and outs of the *Wicked Quadrant* in this essay, nor rehash the reasons so many lawyers fall astray in e-discovery. (Interested readers are directed to the article and symposium transcript) Instead, I am going to review and briefly analyze the primary Rules of Professional Conduct that are implicated in e-discovery ethics. These are the rules that we should understand and rely upon to keep us on the *straight and narrow*, and out of the sanctions penalty box. At the end of Part One I will present a common hypothetical where the ethics of many lawyers involved in e-discovery productions are severely tested . In Part Two I will analyze the hypothetical and show how these rules of Professional Conduct should apply.

ABA's Model Rules of Professional Conduct

The ethical codes require all lawyers to be competent, and, if faced with a legal task wherein they are not competent, such as e-discovery, to bring in other attorneys who are. **Rule 1.1**:
A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.
Our ethics also requires diligence, a task that is impossible unless you are competent and actually know what to do and when to do it. **Rule 1.3**:
A lawyer shall act with reasonable diligence and promptness in representing a client.
Fast and efficient action is built into our code. It is emphasized again by **Rule 3.2** that requires lawyers to expedite litigation:
A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.
The duty of confidentiality is also a core value that often comes into play in e-discovery practice. It is embodied in **Rule 1.6**:
A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

Our fundamental values embodied by our Rules of Professional Conduct also require candor towards the tribunal, the judges. Candor means openness and complete honesty. It is a core value that may never be broken under any circumstances. Should it violate your duty of loyalty to your client, you are required to withdraw from representation, rather than ever be dishonest and closed to the presiding judge. Here are the exact words of this most important of rules, **Rule 3.3**:
(a) A lawyer shall not knowingly:
(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer; . . .
(3) offer evidence that the lawyer knows to be false. . . ."
Our core values as lawyers also require fairness to the opposing party in litigation and fairness to the opposing counsel. This means, among other things, that games of hide-the-ball are forbidden. This does not mean that you should provide evidence harmful to your client that was not requested, or not relevant, or that you are not legally required to produce such as privileged information. But if it was requested, is relevant, and you are legally required to produce it, it is unethical not to do so. If the client refuses to do so, you should withdraw. **Rule 3.4** states:
A lawyer shall not:
(a) unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act.
(b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;
(c) knowingly disobey an obligation under the rules of a tribunal, except for an open refusal based on an assertion that no valid obligation exists;
(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party.
This last point is sub-section (d) of 3.4 is specifically directed to discovery requests and will be closely examined in our concluding hypothetical.

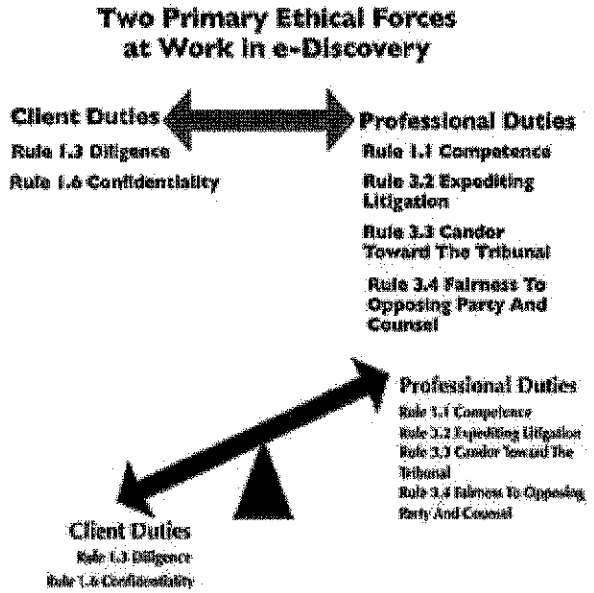
Brief Analysis of the Rules

To summarize our review of the ABA Model Rules of Professional Conduct, six rules seems especially important to the field of e-discovery:

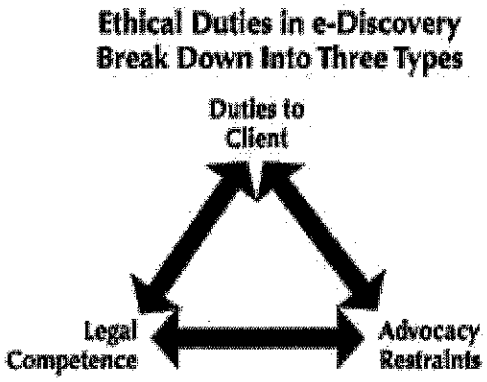
1. Rule 1.1 – Competence
2. Rule 1.3 – Diligence
3. Rule 1.6 – Confidentiality
4. Rule 3.2 – Expediting Litigation
5. Rule 3.3 – Candor Toward the Tribunal
6. Rule 3.4 – Fairness to Opposing Party and Counsel

Rules 1.3 and 1.6, competence and confidentiality, are often considered client related duties, whereas the other rules listed above are considered professional duties. I examined the inherent tension between these rules in *Lawyers Behaving Badly,* which I illustrated with several diagrams.
My article suggests that many lawyers neglect their professional duties, and instead over-inflate client duties instead of crafting a careful balance. I speculate that one reason for this imbalance is that the discharge of client-centric duties tends to receive immediate financial rewards from appreciative, perhaps over-impressed, clients. On the other hand, the reputation gains and societal values from fulfillment of professional duties are more long term and abstract. In the

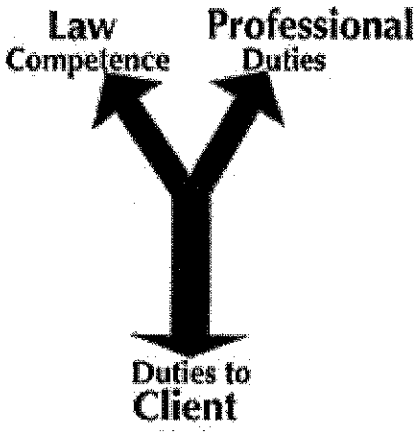
hope that a picture actually may be worth a thousand words, and so spare you unnecessary reading at this time, I provide these diagrams below. I suggest you seek the original article for a full explanation should your curiosity be stimulated.



Attorney competence, Rule 1.1, is such a powerful forces in our legal tradition, that it is an over-simplification to look solely at the problem of ethics in e-discovery in a dualistic manner – client versus profession – as the above diagrams suggest. Another element of complexity must be added to get a better understanding of the problem. Competence should be understood as its own ethical force, and the issue should be triangulated as shown below.



This three-fold structural analysis allows for a deeper understanding of the true dynamics of legal practice. Legal competence serves as an independent upward force, along with professional duties, to counter-balance the pressures and temptations involved with fulfillment of duties to clients. The forces of law and profession work hand-in-hand to offset the demands of some clients, typically implied, to prevail over their adversaries at all costs.



Most of the time the temptations of greed and power do not cause "lawyers to behave badly." Certainly, lawyers do not make a practice of lying to courts and opposing counsel, even though they could probably get away with it in many instances and maximize their income in the process. There is more to this picture than simple economics. The law, after all, attracts many who are concerned with justice and care about doing the right thing. Most lawyers have strong moral fiber and need little encouragement to do the right thing. They are more than *pen-and-quill mercenaries*. Integrity, professional pride, and competence temper their financial motivations. Moreover, some enlightened clients recognize and financially reward professional competence and are influenced by professional reputation in the lawyer selection and compensation processes.

Cooperation

The strategy demanded in e-discovery when it is performed competently, is fundamentally different than traditional adversarial strategy for courtroom arguments. It involves *cooperation* on discovery, buttressed by liberal disclosure by both sides (party requesting information, and party responding to the discovery requests). The need for this new strategy, and the name given therefore of *cooperation*, was initiated by Richard Braman, the founder of the Sedona Conference. Richard set forth this Sedona initiative in a press conference followed by a written, online *Sedona Conference Cooperation Proclamation* (2008). This is a brief document of only two and a half pages. It is well summarized by its conclusion, which states:

It is time to build upon modern Rules amendments, state and federal, which address e-discovery. Using this springboard, the legal profession can engage in a comprehensive effort to promote pre-trial discovery cooperation. Our "officer of the court" duties demand no less. This project is not utopian; rather, it is a tailored effort to effectuate the mandate of court rules calling for a "just, speedy, and inexpensive determination of every action" and the fundamental ethical principles governing our profession.

Although the proclamation was short, it was elaborated at length in *The Case for Cooperation*, 10 Sedona Conf. J. 339 (2009 Supp.) The article was written by a group of Sedona contributors led by Bill Butterfield of Hausfeld LLP. The executive editors were Richard G. Braman and Kenneth J. Withers, both of The Sedona Conference®. This initial proclamation and article were followed by case law where all of the leading e-discovery judges weighed in with their strong support of the new doctrine, and many more articles. *Mancia v. Mayflower Textile Services Co.*253 F.R.D. 354 (D.Md. Oct. 15, 2008) (landmark case on cooperation by Judge Paul Grimm that details the basis in the rules and reasonable, ethical practice for a cooperative approach to

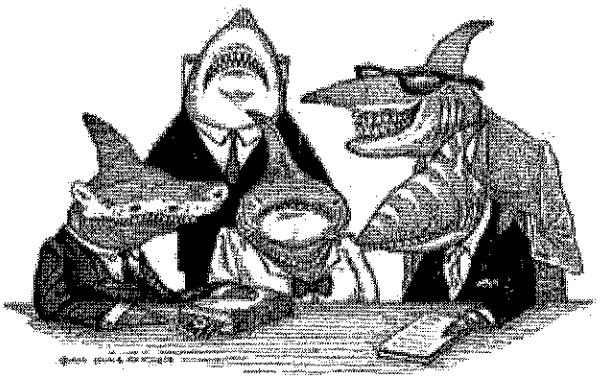
discovery, especially e-discovery); Losey, R., *Mancia v. Mayflower Begins a Pilgrimage to the New World of Cooperation,* 10 Sedona Conf. J. 377 (2009 Supp.) (reviews initial case law adopting the Cooperation Proclamation); Gensler, S., *The Bull's-Eye View of Cooperation in Discovery*, 10 Sedona Conf. J. 363 (2009 Supp.) (Professor Gensler provides a scholarly basis and analysis of the new doctrine and its benefits to litigants); *Also see DeGeer v. Gillis*, 2010 WL 5096563 (N.D. Ill. Dec. 8, 2010) (J. Nolan) (found that the absence of a "spirit of cooperation [and] efficiency" was the controlling factor in determining whether cost shifting was warranted for discovery of nonparty ESI).

The *cooperation challenge* is still beyond the skill of most attorneys, at least when it comes to making e-discovery related decisions and communications. The competence weakness in turn limits the restraints on unethical conduct. The hardest ethical decisions have to be made where you are not sure what to do. As practitioners of e-discovery improve their technical competence, they realize that the cooperative model must be employed to focus on the issues and to control costs. I have yet to meet an experienced attorney in this field who does not agree with this proposition, one who knows both discovery and trial Practice.

Hypothetical

Let us assume for purposes of this hypothetical that the attorneys for one side, the defendant employer in a class action case, have shifted to the new paradigm of Cooperation, and the attorneys for the other side, here the plaintiffs' counsel, have not. This means plaintiffs' counsel are still stuck in the old school attitude of attacking all of the other side's proposals without first considering their merits, without any objective analysis of reasonability.

They do this because they assume that if the other side wants something, then it must be bad for their side. They assume that any proposal is not genuine, that it is instead a gross-exaggeration of the other side's real position. They assume *anti-Solomon* attitudes where the baby will be split. For that reason they say 1,000 is their bottom line, whereas in fact the reasonable number, which they well know, is 10 not 1,000. They begin at 1,000 even though they know that 10 is proportional. They do not cooperate. They negotiate. They want to win, and most will do so at all costs without regard to the unnecessary attorney fees thereby incurred.



Unfortunately, in e-discovery most attorneys are still stuck in the non-cooperative win/lose discovery battle. They mistakenly think that it is their job to not only argue the law and application of the law to the given facts, but also to try to change the given facts, to hide and obfuscate facts they think are adverse to their client.

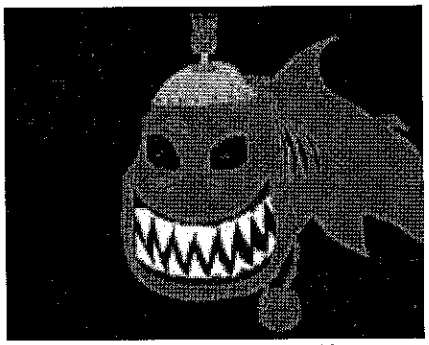
This fundamental difference in attitude towards discovery makes the position of the *cooperator*, here defense counsel, very difficult. The solution is largely one of education of opposing counsel, or failing that, the court.

An objective reasonable discussion should resolve all issues, especially if there is a fair measure of transparency to the process. This must remain the goal of all cooperative counsel in order to protect their clients from excessive costs and disputes.

Next assume that plaintiffs' counsel makes a very broad demand for production of email using the old school, win-lose negotiation methods. Assume they make demand for the relevant emails from 50 custodians, naming everyone and their uncle that might possibly have anything to do with the dispute in question. They also purport to define relevancy very broadly by making 50 category demands on a wide variety of subjects, many with only a nebulous connection to the factual issues of the case. They do so knowing that at most 10 custodians are likely to really know anything, but they are not sure exactly who they are, and for that reason they name the larger group of 50. They are also not sure of the real issues of fact in the case yet, largely because they have never talked with opposing counsel. Since they do not have a clear idea of the issues in the case, they define relevancy very broadly with 50 categories of documents.

The new paradigm attorneys, here defense counsel, quickly realize when they attempt real communication with plaintiffs' counsel on issues of e-discovery, that they are dealing with old school negotiators. It quickly becomes obvious to experienced e-discovery counsel when opposing counsel has little or no personal competence in the area. You cannot hide that, no matter how many experts you may hire to guide you.

Defense counsel quickly realized that no true communications were likely, that they were engaged in a traditional negotiation process with Plaintiff's counsel. But rather than accept and play the game by say offering 3 custodians and 5 issues, hoping to settle for 5 and 7, defense counsel lays out their case for five custodians and seven issues. They play a new game, a cooperative game of reasoned discussion and informed decisions. Defense counsel makes disclosure and explains why they consider the 5/7 offer to be reasonable. They explain why they think the offer that would be beneficial to all parties.



Next assume that plaintiffs' counsel are unpersuaded by defense counsel, that they respond with little or no substance, and instead demand 30/30, instead of 50/50, arguing that they have now made major concessions, and thus suggesting or signaling that they will accept 20 custodians and 20 issues. They assume, incorrectly, that defense counsel is like them, that the 5/7 proposal was just the opening offer in a negotiation dance. They did not really care about the reasons stated by defendants for the proposal, and, truth be told, they did not really understand most of the e-discovery technical talk surrounding the issues. They were hardball trial lawyers; tough advocates doing their job by pounding out as much information from the other side as they could. They thought it would help their clients to make the defendant's case as expensive as possible. They knew e-discovery was a good way to do that, and knew from past experience that this *oppose everything* tactic was a good way to drive up the settlement value of the case. Discovery, especially e-discovery, was just another tool in the battle against the other side.

Next assume defendants continue to refuse to play the negotiation game, and hearing no real *reasons* for them to think their original calculation of 5 custodians and 7 issues is wrong, press forwards in their demands for 5/7. They ask for reasons and calm discussion from plaintiffs' counsel, but instead receive rhetoric and negotiation bluster. Accusatory letters are exchanged, the real purpose of which are not true communications, but mere posturing, mere creation of exhibits for use in motion practice.

The court is then asked to consider cross-motions for relief on a variety of complex e-discovery issues. Both sides claim that they are the true cooperator, and that the opposing party, not them, is to blame for the impasse. What should a judge then do? How do you tell the true cooperator from the mere poser? Both sides claim to be cooperators, and one side did make a major move in custodian and issue count, whereas the other did not. From the negotiation perspective, it looks like plaintiff's counsel is being more cooperative. Whereas we know that they are not cooperating at all, they are not even communicating or attempting to narrow the issues. How is a savvy judge to sort things out?

The answer lies in probing the merits of the dispute. This requires the judge to also break out of the old negotiation paradigm, to look beyond the facial numbers. Why are five custodians reasonable and proportional, and twenty custodians too much? Why should relevancy be defined by seven issues, and not twenty? It is not a mere numbers game, as plaintiffs' counsel in this scenario would suggest. The court must do the hard work of examining the merits of the dispute, of determining what is reasonable and proportional for the case, and what is not. The court should refuse to buy into the old paradigm negotiation model, and just split the difference and enter an order allowing 12 custodians and 14 issues. The judge should instead examine the facts in an objective manner, and if 5 custodians and 7 issues are indeed reasonable, should rule accordingly.

This takes time and hard work on the judge's part, and on part of the attorneys who frame the issues and present the case. They need to provide meat for the bone. They need to make disclosures and present facts to support their positions.

In the hypothetical let us further assume that defense counsel realized their quandary and voluntarily made substantial disclosures. Assume they disclosed their own mental impressions, their work product as to why the five custodians they picked would have the most relevant email. Assume they also provided total counts and other metrics of email for the five custodians they proposed. Moreover, assume the defendant also provided counts for the additional fifteen custodians that plaintiffs' proposed.

Assume the defendant make even further disclosures to support their argument of reasonability and proportionality. Assume they presented detailed information concerning the costs of the review and production proposed by plaintiffs, as compared to their proposal. Assume it was not puffed or inflated and was supported by facts, which they offered to backup with further testimony if needed.

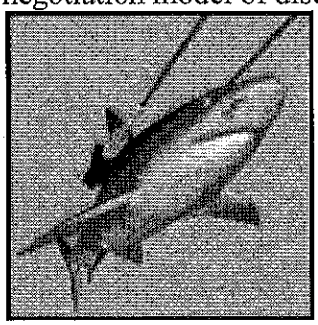
Assume defendants went even further and began to make sample productions from the top five custodians they picked, and that they did so after a strong confidentiality and clawback order was entered by the court. Assume the emails produced showed that most of the other fifteen custodians that plaintiffs wanted to add at great additional cost were copied on most of the relevant documents.

Assume defense counsel even made some random sample productions from all twenty custodians to show that the top five they had selected had the vast majority of the relevant documents, and were the only source of the few highly relevant documents found. Assume they not only

produced the documents they marked relevant, but also made a selective disclosure of documents they marked irrelevant to provide the plaintiffs with an opportunity to review and if need be, to challenge their understanding of relevancy in this case.

Assume that defense counsel was also proposing phased production. That they only insisted their 5/7 approach be for the first phase, and that they did not insist plaintiffs waive their rights to seek additional document productions in follow-up phases. Instead, assume the defendants only sought to clarify that they reserved their rights to object to any future discovery, or not, depending on the circumstances.

With all of these additional facts, these voluntary disclosures, the judge's work becomes much easier. The judge now has the information, the facts, on which to make a ruling. The defendant has made significant disclosures of their client's email systems, and even of their email contents. Now the judge is in a position to determine whose position is reasonable, and who is the true cooperator here. This information provides the substance needed for the judge to go beyond the negotiation model of discovery dispute resolution to a true judicial model.



Of course, in the real world all lawyers come before judges with a history. They have a reputation. This can also help a judge to evaluate "who's on first" and know who is a poser, and who is not. This is especially true where a judge has seen and heard from one or more of the lawyers several times before. That is where the intangible value of an attorney's reputation comes in.

I am happy to say that in my experience when most judges are faced with this situation, and properly advised of the issues, they will do the hard work and make their own determination of reasonability. They will not simply split the baby and order 12 custodians and 14 issues. But this requires proper education of judges on the issues, which in turn requires competent counsel with a good reputation for truth, honesty and fair dealing. If defense counsel in this scenario are competent, and so is the judge, a just and reasoned result will usually be attained, regardless of any overly-clever negotiation tactics of plaintiffs' counsel.

END OF PART ONE.

(1)

Fairfield Inn of Court Oct 9. 2013

MEMBER	PRESENT	EXCUSED ABSENCE	UNEXCUSED ABSENCE	SUBSTITUTE
Hon. Lynn S. Adelman				
Atty. David Asbach	X			
Atty. Michael Ashton	X			
Atty. Tony Scott Baish	X			
Taylor Barnes				
Atty. Melinda A. Bialzik	X			
Atty. Remzy D. Bitar				
Atty. Melissa Blair				
Atty. Rachel M. Blise	X			
Atty. Charles S. Blumenfield	X			
Atty. Sean Bosack				
Atty. James. Boyle	X			
Hon. William W. Brash, III				
Atty. Laura A. Brenner	X			
Atty. Thomas M. Burnett				
Atty. John Arthur Busch	✓			
Hon. Louis B. Butler, Jr.	✓			
Atty. Nathaniel Cade, Jr.	✓			
Hon. William E. Callahan, Jr.				
Atty. Mark Cameli	✓			
Atty. Scott J. Campbell	✓			
Atty. Nicholas D. Castronovo				
Atty. Kelly L. Centofanti				Amy Mastrdy
Hon. Charles Clevert, Jr.				

MEMBER	PRESENT	EXCUSED ABSENCE	UNEXCUSED ABSENCE	SUBSTITUTE
Atty. Rebecca M. Coffee	X			
Atty. Michael Cohen				MC
Hon. Pedro A. Colon	X			
Atty. Jacques C. Condon	X			
Hon. Jeffrey Conen	X			
Atty. Daniel Conley				
Hon. Charles H. Constantine				
Atty. Joshua B. Cronin	X			
Hon. Patricia Curley	X			
Hon. Rebecca F. Dallet				
Atty. Donald Daugherty, Jr.				
Atty. William Duffin	✓			
Atty. Laurence J. Dupuis	✓			
Vanessa Eisenmann	X			
Atty. Matthew R. Falk	✓			
Atty. Jessica Farley	✓			
Atty. Andrew Frank				
Atty. Heather K. Gatewood	✓			
Atty. Robert L. Gegios	RLG			
Atty. Kate Gehl	✓			
Atty. Derek H. Goodman	✓			
Hon. Patricia J. Gorence				
Hon. Lindsey Grady				
Hon. Michael Goulee	✓			
Atty. Laurence C. Hammond, Jr.				

MEMBER	PRESENT	EXCUSED ABSENCE	UNEXCUSED ABSENCE	SUBSTITUTE
Atty. Scott W. Hansen	✓			
Atty. Andrew N. Herbach				
Atty. Thomas Hruz	✓			
Atty. Grant Huebner	✓GH			
Atty. James L. Huston				
Atty. Michelle Jacobs	✓			
Hon. Nancy Joseph	✓			
Dean Joseph D. Kearney				
Hon. Joan Kessler	X			
Margo S. Kirchner	X			
Atty. Matthew D. Krueger	X			
Hon. Mary Kuhnmuench	✓			
Atty. Lisa M. Lawless				
Atty. Jeremy Levinson	✓			
Atty. Susan E. Lovern	✓			
Atty. Kevin J. Lyons				
Atty. Jacob Manian				
Atty. Jonathan H. Margolies				Patricia Jenness
Atty. Lynn S. McCreary				
Hon. Margaret McGarity	✓			
Atty. James T. McKeown				Jacob McGee
Nancy Morris	MSM			
Atty. William J. Mulligan				
Atty. Elizabeth a. Odian	✓			
Atty. Aaron Olejniczak				Chris Liro

MEMBER	PRESENT	EXCUSED ABSENCE	UNEXCUSED ABSENCE	SUBSTITUTE
Atty. Matthew W. O'Neill	✓			
Atty. Richard T. Orton	✓			
Atty. Wendy A. Patrickus				
Atty. David G. Peterson	✓			
Atty. Mark A. Peterson		✓		Daniel Peterson
Atty. Nelson W. Phillips, III				
Hon. William Pocan	✓			
Atty. Benjamin W. Proctor	✓			
Atty. Janet Protasiewicz	✓			
Atty. Thomas H. Reed	✓			
Atty. John A. Rothstein				
Hon. Richard Sankovitz				
Atty. James L. Santelle	✓			
Atty. Jane C. Schlicht	✓			
Prof. Ryan Scoville				
Atty. Nancy J. Sennett	✓			
Atty. William L. Shenkenberg	✓			
Atty. Sheryl A. St. Ores	✓			
Hon. J.P. Stadtmueller	✓			
Atty. William R. Steinmetz	✓			
Atty. Karen Louise Tidwall	✓			
Hon. Paul Van Grunsven				
Atty. Eric J. Van Schydle	✓			
Atty. Christopher R. Walker	✓			
Atty. Joseph Wall				

(5)

MEMBER	PRESENT	EXCUSED ABSENCE	UNEXCUSED ABSENCE	SUBSTITUTE
Atty. Johanna Wilbert	✓			
Zachary R. Willenbrink	✓			
Atty. Julie P. Wilson	✓			
Hon. Timothy M. Witkowiak				
Atty. Matthew M. Wuest	✓			
Atty. Kaivon Yazdani	✓			
Erika D Olson	X			
Greg Helding	X			
Taylor Gumbleton	X			
Jamie Yu	X			
Bill Harbeck	Here			