

Digital Discovery: When Litigation Looms

I have come to believe that if anything will bring about the downfall of a company, or maybe even a country, it is blind copies of e-mails that should never have been sent in the first place.

- Michael Eisner, Disney CEO

I. Introduction

For 16 years, Arthur Andersen had provided accounting and consulting services to corporations throughout the world, but few compared to energy trading titan Enron, the 7th largest corporation in the U.S. When Enron retained Andersen for auditing and consulting services, Enron became one of Andersen's largest clients, providing both internal and external work. In its Houston headquarters, Enron even provided Andersen its offices.

An August 15, 2001 memo from an Enron top executive warned Andersen that there may be financial improprieties in Enron's books. By early October 2001, the Securities and Exchange Commission, suspicious of Enron's accounting practices and Andersen's auditing, began an inquiry. On Friday, October 19th, Andersen was alerted to the inquiry. By Tuesday, October 23, Andersen employees began deleting and destroying electronic data and shredding documents pertaining to Enron at their Houston office after being "reminded" by in-house counsel about the firm's document-destruction policy (even though most had not even been aware the company had such a policy). Within months, Andersen and its managers were entrenched in civil and criminal litigation over the evidentiary destruction.

Within a year, corporations such as Global Crossing, WorldCom, Qwest, Adelphia Communications, Merrill Lynch, Salomon Smith Barney, and others found themselves in similar predicaments. One aspect that set the Enron/Andersen debacle apart and captured the public's attention, however, was the intentional destruction of incriminating evidence even in the face of legal action.

As a result of the combination of our litigious culture and a society increasingly reliant on ever-growing amounts of digital data, many businesses and individuals now find themselves in the unenviable position of facing legal action while in the possession of volumes of incriminating documents. Andersen and Enron's example highlight what not to do in such a situation, but knowing what should be done can be a little more difficult. A proper, proactive approach should offer protection from fines, default judgments, or worse.

Of course, the best way to avoid such a quandary is to avoid legal trouble in the first place, though this is not always possible. With the prospect of a legal battle likely,

not having incriminating documents is the next best scenario. As a result, there have been scores of articles written on how to set up and maintain electronic document retention policies, and hundreds of consultants make their living assisting companies in this endeavor. Even with the best preparation, though, there will most likely be some document somewhere that an adversary will take full advantage of. A company or person who is a defendant in civil or criminal action (or even a plaintiff in a civil action), or is even aware that legal action is likely or imminent, must be very careful not to destroy evidence - even that “smoking gun” evidence that can be used against them. Special attention must be paid to electronic evidence, which, while appearing to be the easiest to make disappear, can often be the most tenacious and the most likely to cause serious repercussions. The legal landscape is littered with Defendants who actually believed that pressing the “delete” key made documents disappear.

II. Electronic Evidence is Fully Discoverable

In a given legal action, chances are, electronic data *will* be sought, and most likely will be discoverable. The Federal Rules of Civil Procedure enable parties in litigation to “obtain discovery regarding *any matter*, not privileged, which is relevant to the claim or defense of any party . . .” even if not “admissible at trial, if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.”¹ When the wheels of the discovery machine begin to turn, along with paper documents, a party will need to produce e-mails, databases, spreadsheets, word processing files, and other electronic documents. The Federal Rules of Civil Procedure were amended in 1970 to define the term documents as being “in accord with changing technology” and “applies to electronic data compilations.”² It was soon well established that discovery requests could include electronic data, including, but not limited to, data stored on punch cards, disks, hard drives, recording tapes, and in computer data bases. As the court in Anti-Monopoly, Inc. v. Hasbro, Inc., stated, “today, it is black letter law that computerized data is discoverable if relevant.”³

Over the past several decades there have been numerous disputes over whether (and how much) electronic information must be produced in a response to discovery requests. The answer is that any relevant document, whether in electronic form or on paper, must be produced. While a given discovery request will most likely request documents in both written and electronic form, computerized data is required even if it is

¹Fed. R. Civ. P. 26(b)(1) (emphasis added).

²Fed. R. Civ. P. 34(a)(1) Advisory Committee's Note.

³Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, (S.D.N.Y. Nov 03, 1995).

not specified. In Playboy Enterprises v. Welles⁴, Defendant Terri Welles argued that Plaintiff's request for "documents" did not include electronic data. The court found that by requesting "documents," Plaintiffs were not only requesting paper documents, but were also requesting information stored in electronic form. In fact, the court in Linnen v. A.H Robbins Co., Inc.⁵ stated that "A discovery request aimed at the production of records retained in some electronic form is no different, in principle, from a request for documents contained in an office cabinet."⁶

III. When, How, & What

A. When Preservation Starts

A person or company has an affirmative obligation to preserve any data or documents likely to be relevant to pending or future litigation.⁷ But at what point does this duty attach? Must a potential party to a lawsuit always assume that legal action is imminent and preserve everything, or can the party merrily delete and destroy documents without any repercussions until served with a complaint? The answer lies somewhere in between, using a reasonable person standard. The court in Kippenhan v. Chaulk Services, Inc., et al.⁸ applied such a standard and stated, "[s]anctions may be appropriate for the spoliation of evidence that occurs even before an action has been commenced, if a litigant or its expert knows or reasonably should know that the evidence might be relevant to a possible action." The court went on to qualify this obligation stating that "[t]he threat of a lawsuit must be sufficiently apparent, however, that a reasonable person . . . would realize . . . the possible importance of the evidence to the resolution of the potential dispute." Of course, various courts define "a reasonable person" differently. While some courts impose a duty to preserve only to litigation that is pending or likely,⁹ other impose this duty to any matter in which it is "reasonably foreseeable" that litigation would arise.¹⁰

⁴Playboy Enterprises v. Welles, 60 F.Supp 1050 (S.D. Cal. 1999).

⁵Linnen v. A.H Robbins Co., Inc., 1999 WL 462015 (Mass. Super. 1999).

⁶ *Id.* at 6.

⁷William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984), Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90, 101 (D.Colo.1996), Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y.1991).

⁸Kippenhan v. Chaulk Services, Inc., et al., 697 N.E.2d 527 (Mass. 1998).

⁹ Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998). See also Mathias v. Jacobs, 197 F.R.D. 29, 39 (S.D.N.Y. July 28, 2000).

A party can be put on notice that litigation has arisen or is about to arise in a variety of ways. Of course, there can be no doubt once a complaint has been served. Likewise, the plaintiff in an action is certainly on notice that all relevant documents should be preserved, as Proctor and Gamble found out in Proctor and Gamble v. Haugen.¹¹ In this action, Plaintiff Proctor & Gamble (P & G) sued an independent Amway representative and requested massive amounts of data from the e-mail system of third party Amway. When Amway objected to the request and filed for a protective order, P & G opposed the order, calling it “a naked request for judicially sanctioned spoliation on a grand scale.” After P & G joined Amway as a defendant, however, Amway requested the same types of e-mails from the five P & G employees P & G had already identified as having relevant information. In complete disregard of the ongoing litigation, P & G had deleted the same types of data it had fought to obtain from Amway. The court found that “P & G’s own identification of these individuals belies any possible claim that P & G was not on notice that their e-mail communications would not be relevant” and responded by imposing monetary sanctions against P & G.

Written notification, or even serious oral notice, threatening legal action may serve to attach a duty to preserve potential evidence. Notice may also be inferred in situations that could foreseeably develop into litigation - even absent formal notification of any of pending or potential litigation. In Lewy v. Remington Arms Co., Inc.,¹² the Defendant, a gun manufacturer, was sued in a products liability action when one of its guns accidentally discharged, injuring the Plaintiff. Several relevant documents, including consumer complaints and gun examination reports on the model at issue, had been destroyed pursuant to Defendant’s document retention and destruction policy, which was to destroy documents after three years. The court, noting the nature of the documents, observed “. . . if the corporation knew or should have known that the documents would become material at some point in the future then such documents should have been preserved. Thus, a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.”¹³ See also, Telecom Int’l Amer., Ltd. v. AT&T Corp.¹⁴

B. What to preserve?

¹⁰ West v. Goodyear Tire & Rubber Co., 167 F.3d 776 (2nd Cir. 1999).

¹¹ Proctor and Gamble v. Haugen. 179 F.R.D. 622 (D. Utah 1998), aff’d in part and rev’d in part, 222 F.3d 1262 (10th Cir. Utah 2000).

¹² Lewy v. Remington Arms Co., Inc., 836 F.2d 1104 (1988).

¹³ Lewy at 1112, quoting Gumbs v. International Harvester, Inc., 718 F.2d 88 (CA.3 1983).

¹⁴ Telecom Int’l Amer., Ltd. v. AT&T Corp., 189 F.R.D. 76 (S.D.NY 1999).

Must all data be retained indefinitely under the specter of some unknown future potential litigation? Surely, storing, indexing, and preserving every e-mail, document, and scrap of data would create a logistical, technological, and financial nightmare. In short, a party or potential party has a duty to preserve only any data or documents relevant to a current or reasonably anticipated action. More specifically, “[a] litigant has a duty to preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested in discovery and/or is the subject of a pending discovery request.”¹⁵

Generally, any data or documents relevant - or even potentially relevant - to the action at hand must be preserved. This includes but is not limited to all data including document files, e-mails, databases, spreadsheets, graphics files, digitally stored voice mails, internet browser records, calendar data, records, and backup files. The data can be stored on individual computers, floppy disks, CD-Roms, document servers, backup tapes, personal digital assistants, flash memory devices, voice mail systems, e-mail servers, recordable DVD’s, and other devices too numerous to list. And as technology proliferates, the data and its sources will only increase.

C. How?

Rule 34(b) requires the respondent to produce data as “kept in the usual course of business or . . . organized and label them to correspond with the categories of the request.”¹⁶ The courts have therefore ruled that data and documents must be presented in a format readable to the requesting party.¹⁷ Mere backup tapes, readable only to the respondent, will not suffice. In Sattar v. Motorola, Inc.,¹⁸ when Plaintiff Sattar requested some 210,000 e-mails, Defendant Motorola produced the requested data in the form of their proprietary 4-inch tapes. Unfortunately, as the tapes were not in an easily accessible format, they were unreadable to the plaintiff who lacked the proper hardware and software. Instead the court ordered that Motorola make the already produced data usable by copying the data onto more conventional media, loaning the Plaintiff the necessary software, or offering the Plaintiff on-site access to its own systems.

¹⁵Wm. T. Thompson Co. v. General Nutrition Corp., Inc., 593 F.Supp. 1443-45 (C.D. Cal. 1984).

¹⁶Fed. R. Civ. P. 34(b).

¹⁷Bd. of Educ. Of Evanston Township Hight School v. Admiral Heating & Ventilating, Inc., 104 F.R.D. 23 (N.D. Ill. 1984).

¹⁸Sattar v. Motorola, Inc., 138 F.3d 1164 (7th Cir. 1997).

While parties may choose to store the data in a proprietary format, difficulty producing the data will not act as an excuse for not producing it. In Kaufman v. Kinko's Inc.,¹⁹ when defendant Kinko's argued that the burdens of the retrieval process outweighed the evidentiary benefit of the data, the court replied that:

[u]pon installing a data storage system, it must be assumed that at some point in the future, one may need to retrieve the information previously stored. That there may be deficiencies in the retrieval system . . . cannot be sufficient to defeat an otherwise good faith request to examine relevant information.

In Toledo Fair Housing Ctr. v. Nationwide Mut. Ins. Co.,²⁰ the Defendant insurance company argued that the \$112,500 cost to plan, devise, and execute the computer programs necessary to make data from four databases readable by a layperson would be overly burdensome. Again, the court answered that a party cannot avoid discovery merely because its own computer system makes discovery burdensome, and that "[i]f a party chooses to store information in a manner that tends to conceal rather than reveal, that party bears the burden of putting the information in a format usable by others." And in In re Brand Name Prescription Drugs Antitrust Litig., the Court held the Defendant responsible for the cost of compiling, formatting, searching and retrieving from more than 300 million pages of e-mail stored on backup tapes, stating that Plaintiffs should not have to bear the costs of producing "the defendant's record-keeping scheme over which the Plaintiffs have no control."²¹

In fact, even if paper copies have been produced, the majority view holds that electronic source documents in a source readable by a layperson must be produced as well, if requested by a party. The Court in Armstrong v. Executive Office of the President²² held that "hard copy printouts...may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt."²³ Providing mere paper printouts deprived the recipient of important meta-data, or non-screen data with the data, and essentially does not satisfy a requirement to provide all the data. In Anti-Monopoly, Inc.

¹⁹Kaufman v. Kinko's Inc., Civ. Action No. 18894-NC (Del Ch. Apr. 16, 2002).

²⁰Toledo Fair Housing. Ctr. V. Nationwide Mut. Ins. Co., 703 N.E.2d 340 (Ohio C.P. 1996).

²¹In re Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526 (N.D. Ill. 1995).

²²Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993).

²³*Id* at 1274.

v. Hasbro, Inc.,²⁴ the court stated "The law is clear that data in computerized form is discoverable even if paper 'hard copies' of information have been produced. . . ." This is especially so where the paper copies are exceedingly "complicated and voluminous"²⁵ or so poorly organized as to be useless.²⁶ Many courts are holding it is reasonable to produce the data in digital form, even where paper copies have been specifically requested, as was the case in Storch v. IPCO Safety Prods. Co.²⁷ "This court finds that in this age of high-technology where much of our information is transmitted by computer and computer disks, it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff."²⁸ On the other hand, there are courts that hold a contrary view. In Williams v. Owens-Illinois, Inc.,²⁹ the court allowed appellee to produce paper wage cards over the appellant's objection, finding that although using the cards was "may be more time consuming, difficult and expensive," the appellants were not deprived of any data.

Even data that has previously been deleted is not immune from discovery. When the Plaintiff in Simon Property Group v. mySimon, Inc.,³⁰ brought a motion to compel in this case alleging a trademark breach, the court ordered that the Defendant make its computers available to the Plaintiff's expert in an attempt to recover deleted computer files. The expert "mirrored" or made exact copies of the Defendant's hard drives, deleted files and all. The court ordered protective measures taken, however, including appointing Plaintiff's expert as an officer of the court to ensure confidentiality, and requiring the expert to first turn over the recovered data to Defendant's counsel to review for confidentiality and privilege, before releasing it to the Plaintiff.

IV. The Courts and Electronic Data

A. Sanctions for Deleting or Destroying Data

Rule 37 of the Federal Rules of Civil Procedure and the court's "inherent power

²⁴Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995).

²⁵Timkin v. U.S., 659 F.Supp. 239 (Ct. Int'l Trade 1987).

²⁶Tulip Computers Int'l v. Dell Computer Corp., 2002 WL 818061 (D. Del. Apr. 30, 2002).

²⁷Storch v. IPCO Safety Prods. Co., 1997 WL 401589 (E.D. Pa. July 16, 1997).

²⁸Storch at 4.

²⁹Williams v. Owens-Illinois, Inc., 665 F.2d 918 (9th Cir. 1982).

³⁰Simon Property Group v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000).

to regulate litigation, preserve and protect the integrity of proceedings before it, and sanction the parties for abusive practices”³¹ vests the court with the authority to impose sanctions for the destruction of evidence, and gives the court “a broad canvas upon which to paint in determining sanctions.”³² The purposes for which the court imposes sanctions are threefold. First, sanctions serve to punish the wrongdoer for his unacceptable behavior. The sanctions also serve to compensate the prejudiced party in an attempt to put right that which was made wrong by the sanctioned party. Finally, the court will tailor sanctions most likely to discourage future similar behavior.

Courts generally first determine whether behavior is sanctionable by examining: (1) whether the conduct was part of a pattern of wrongdoing; (2) whether the conduct was willful; (3) whether the opposing party was prejudiced; (4) whether the administration of justice was hindered, and; (5) whether there were any other mitigating factors. If the conduct is found to meet the above criteria, the courts then attempt to find less severe alternatives than sanctions. If none exist, then sanctions are imposed.³³ Once conduct is found to be sanctionable, and sanctions are found to be warranted, the court has myriad options from which to choose.

Order to Correct

The most forgiving sanction the court can order is an order to correct, allowing the non-complying party an opportunity to remedy the discovery non-compliance. This was the approach taken by the Court in Liafail, Inc. V. Learning 2000, Inc.³⁴ Here, the Plaintiff had given conflicting accounts of data stored on two of its laptops, first stating that the data had been destroyed, then testifying that the same data had already been provided to the Defendant. Due to the confusion over what had already been produced, the court declined to immediately punish the Plaintiff, instead ordering the Plaintiff to produce the Bates numbers of the documents allegedly produced. If the Plaintiff failed to comply, the court indicated it would order sanctions in the form of adverse jury instructions.

Adverse Inference Jury Instruction

The adverse inference is probably the most frequently used sanction, simply allowing the fact finder to presume that any evidence lost or destroyed would have been

³¹Capellupo v. FMC Corporation, 126 F.R.D. 545, 551 (1989).

³² *Id.* at 551.

³³Republic of Philippines v. Westinghouse Electric Corp., 43 F.3d 65, 74 (3d Cir. 1995).

³⁴Liafail, Inc. V. Learning 2000, Inc. 2002 US Dist. LEXIS 24803 (D. Del., Dec. 23, 2002).

unfavorable to the party responsible for its loss. Devitt and Blackmar's Federal Jury Practice and Instructions³⁵ offers the following proposed jury instruction: "If a party fails to produce evidence which is under his control and reasonably available to him and not reasonably available to the adverse party, you may infer that the evidence is unfavorable to the party who could have produced it and did not."

In Lewy,³⁶ the court enumerated three factors in determining whether an adverse jury instruction was appropriate. First, the court stated, a determination should be made regarding whether the "record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents." In the instant case, the court found that the Defendant's three year retention policy might be warranted for documents such as appointment books and telephone logs, but not documents of greater importance, such as consumer complaints and gun test results. Next, the court should consider whether and how many lawsuits have been filed concerning the same or similar complaints, and should take into account the magnitude of the complaints. Here, the court noted numerous gun examination reports, customer complaints, and even testimony of other customers who had complained of the same defect. Finally, the court should determine whether the retention policy was instituted in bad faith. The Lewy court found that a document retention policy instituted in order to limit damaging evidence available to potential plaintiffs may lead to such a finding. Routine destruction of documents pursuant to company policy and without fraudulent intent, however, should give rise to a presumption of good faith.

In In re the Prudential Insurance Corporation of America Sales Practices Litigation,³⁷ the court issued a pre-trial scheduling order that specifically addressed the preservation of evidence. While the Defendants' in-house counsel and top executives issued an e-mail to their field offices that documents were to be preserved, there was little or no follow-through, and individual agents in field offices either ignored or did not receive the instructions. As a result, the court found that:

haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute. Because the destroyed records . . . are permanently lost, the Court will draw the inference that the destroyed materials are relevant and if available would lead to the proof of a claim.

³⁵E. Devitt, C. Blackmar & M. Wolff, Federal Jury Practice and Instructions, §72.16 (4th ed. 1987).

³⁶Lewy at 1112.

³⁷In re the Prudential Insurance Corporation of America Sales Practices Litigation, 169 F.R.D. 598 (D.N.J. 1996).

Financial Sanctions

Another frequently used form of sanctions is the financial sanction. A compensatory sanction may be imposed to compensate the court, the adversarial party(s), or both for their time and expenses. Compensation may also be in order for experts, computer forensics, and other necessary costs to prove that the destruction occurred. In more extreme cases, the court may issue punitive sanctions intended to penalize for past contumacious behavior and to deter such future behavior.

In addition to the adverse inference imposed in In re Prudential Ins. Co.,³⁸ the court levied a \$1,000,000 fine upon the Defendant recognizing “the unnecessary consumption of the court’s time and resources to the issue of document destruction” and preserving and protecting the jurisdiction and integrity of the court in the face of repeated incidents of document destruction. In this assessment, the court also took into account the Defendant’s financial worth and minimal impact on Defendant’s financial stability. Additionally, Prudential was ordered to reimburse plaintiff’s counsel for all fees and costs associated with the sanctions motion, show cause order, depositions and discovery leading thereto, and for preparation and distribution of the plaintiff’s Report of Investigation to the court and counsel.

After the Defendant was found to have intentionally destroyed incriminating documents in Capellupo v. FMC Corporation,³⁹ the court awarded the Plaintiff twice the cost of all attorney fees and costs of investigating, researching, preparing, and arguing issues regarding the destruction. Additionally, the Defendant was ordered to pay the court for its time and costs. After determining that the Defendant’s willful destruction more than warranted sanctions, the Court reasoned that since the Plaintiffs still had additional evidence against the Defendant, the purposes of justice could still be adequately served by less severe sanctions than a default judgment.

Dismissal or Default Judgment

Perhaps the most severe sanction, and one the court reserves only for the most egregious of circumstances and the most recalcitrant conduct, is exposure to dismissal or default judgment. This ultimate civil sanction is only to be applied when it is “proportional to the discovery failure. The courts will presume proportionality when there are willful or bad faith violations of discovery orders. The same presumption applies when there is a pattern of contumacious conduct or dilatory tactics or the failure

³⁸In re Prudential Ins. Co., supra. at 60.

³⁹Capellupo v. FMC Corporation, 126 F.R.D. 545,126 FRD 545 (D MN 1989).

of less drastic sanctions.’⁴⁰

The behavior of the Defendant in Carlucci v. Piper Aircraft,⁴¹ provides a powerful example of the kind of repeated, deliberate, and willful disregard of the court's orders and of opposing party's rights that can lead to the ultimate civil sanction of default judgment. Here, the court explains that:

[w]hen a party has consistently disobeyed orders, obstructed discovery, delayed proceedings and made misrepresentations to the court, an extreme sanction is warranted. When a party engaging in such conduct has previously been sanctioned by the court and yet continues the same pattern of conduct, the ultimate sanction is warranted.⁴²

The court goes on to illustrate the process of arriving at a default sanction:

[f]irst, dismissal is to be sparingly used and only in situations where its deterrent value cannot be substantially achieved by use of less drastic sanctions. Whether the other party's preparation for trial was substantially prejudiced is a consideration. Dismissal is generally inappropriate and lesser sanctions are favored where neglect is plainly attributable to an attorney rather than to his blameless client.⁴³ Nor does a party's simple negligence, grounded in confusion or sincere misunderstanding of the Court's orders, warrant dismissal. Finally, the Rule 'should not be construed to authorize dismissal when it has been established that failure to comply has been due to inability to comply.'⁴⁴

Like the defendant in Carlucci, the defendant in Telectron v. Overhead Door Corp.,⁴⁵ also engaged in willful and flagrant destruction of documents which might have substantiated Plaintiff's case. The Telectron court established three criteria to be satisfied before the ultimate sanction of dismissal or default was to be imposed. First, the court

⁴⁰Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993).

⁴¹Carlucci v. Piper Aircraft, 102 F.R.D. 472, 481, 486(S.D.Fla.1984).

⁴²Carlucci at 488.

⁴³Carlucci at 488, quoting National Hockey League v. Metropolitan Hockey Club, 429 U.S. 874 (1976).

⁴⁴Id.

⁴⁵Telectron v. Overhead Door Corp., 116 F.R.D. 107 (SD Fla. 1987).

was required to find the party acted willfully or in bad faith. The destruction of evidence here cannot be a mere accident or negligence, but must exhibit “flagrant bad faith”⁴⁶ and “callous disregard to discovery rules.”⁴⁷ Such bad faith evidence destruction also gives rise to the “adverse inference rule,” holding that “bad faith destruction of a document relevant to proof of an issue at trial gives rise to a strong inference that production of the document would have been unfavorable to the party responsible for its destruction.”⁴⁸

The next requirement under Telectron⁴⁹ before the imposition of an entry of default, is that there must be a finding of prejudice; that the discovery abuse must “materially affect the substantial rights of the adverse party” and be “prejudicial to the presentation of his case.”⁵⁰ In addition to placing otherwise discoverable, relevant evidence forever out of the reach of the opposing party, the party that destroys evidence may also prejudice his opposition in other ways, such as causing his opponent to devote extra time, money, and resources into proving the destruction of evidence, in addition to causing inordinate delays.

Finally, before the court can impose the ultimate sanction, it must find lesser sanctions inadequate. To determine whether or not lesser sanctions are adequate, the court would examine each sanction in turn to ascertain whether it fulfilled the treble objectives of: compensating the aggrieved party for the prejudice worked upon it; punishing the party at fault for its contumacious conduct, and; deterring future similar acts of disregard for the court and its discovery rules. Only after finding that all lesser sanctions failed at least one of the three aims may the court assess dismissal or default.

Criminal Charges

In extreme circumstances, criminal contempt and obstruction of justice charges may be brought against one who chooses to “alter, destroy, mutilate, or conceal an object with intent to impair the object’s integrity or availability for use in an official proceeding.”⁵¹ This was vividly illustrated recently when the United States Justice

⁴⁶National Hockey League v. Metropolitan Hockey Club, 427 U.S. 639 (1976).

⁴⁷Id.

⁴⁸Coates v. Johnson & Johnson, 756 F.2d 524, 551 (7th Cir. 1985).

⁴⁹Telectron at 132.

⁵⁰Telectron, quoting Wilson v. Volkswagen of America, Inc., 561 F.2d 494, 503 (4th Cir. 1977), cert. denied, 434 U.S. 1020, 54 L. Ed. 2d 768, 98 S. Ct. 744 (1978).

⁵¹18 U.S.C. §1512(b)(2)(B).

Department brought charges against executives and key employees at Enron, and its auditor Arthur Andersen. Though infrequently used in civil litigation, it is still a tool available to the court.

The new Sarbanes-Oxley Act⁵² was signed into law in July of 2002 as a direct response to the Andersen/Enron scandal. In an attempt to curtail accounting fraud and restore investor confidence in the stock market, it imposes criminal penalties on anyone who destroys, alters, or falsifies data or documents with the intent to impede a Federal investigation or bankruptcy. The act creates the Public Company Accounting Oversight Board to oversee publicly traded companies, and imposes the requirement that auditors maintain work papers for seven years, with prison terms of up to 10 years for violators.

Other

In addition to the standard sanctions listed above, the courts frequently exercise their power to impose a wide range of orders designed to curtail, limit, punish, compensate for, and/or rectify discovery abuses.

The Prudential⁵³ appeals court issued, in addition to the sanctions listed above (adverse inference jury instructions, \$1,000,000 fine, and costs), an order that required to defendant to: (1) copy every employee with the court's order and explain the civil and criminal sanctions implicit in evidence destruction; (2) write a document retention policy manual with clear guidelines and plans to distribute to every employee; (3) set up an anonymous hotline for employees to report violations of the newly-implemented retention policy; and (4) establish a certification process wherein each manager must certify that her/his office is in compliance with the retention policy and is not destroying documents contrary to it. Additionally, the appeals court authorized the trial court to impose any additional sanctions the trial court saw "fair and appropriate to remedy unknown harm to individual party opponents caused by document destruction."

Any Combination

As shown in Prudential, a court is not limited to a particular sanction, but can impose any combination of sanctions it feels is a necessary and appropriate response to discovery abuse. If the court feels a particular sanction fails to satisfy the three objectives of sanctions, but also feels a default or dismissal is not warranted, they may craft a remedy consisting of any combination of lesser sanctions.

⁵²PL 107-204, July 30, 2002, 116 Stat 745, United States Public Laws 107th Congress – Second Session Convening January 2002 (H.R. 3763)(S.2673).

⁵³Prudential, supra.

Tort for Spoliation of Evidence

After the court has imposed whatever sanctions it feels are appropriate, in some jurisdictions the parties can initiate a separate tort action for spoliation of evidence. Spoliation, from the Latin *spolium* meaning “a thing violently or unlawfully taken from another,” is defined by Black’s Law Dictionary⁵⁴ as “the intentional destruction of evidence or the significant and meaningful alteration of a document or instrument.”

Spoliation as a separate tort is a relatively recent legal concept, initially formulated about two decades ago as “intentional spoliation of evidence” but now expanded to include negligent spoliation as well. The spoliation tort was first applied in Smith v. Superior Court,⁵⁵ where the Plaintiff was injured when the wheel and tire from a car came through her windshield. When the car was towed to the dealer who originally sold the car, the plaintiff notified the dealer that the car was evidence and needed to be examined by Plaintiff’s expert. When the dealer agreed but later lost or destroyed the vehicle, the Plaintiff sued the dealer, among others, alleging that the dealer had interfered with her cause of action. Although Plaintiff’s claim was disallowed by the trial court, the appeals court held that Plaintiff’s civil action was a thing of value and was impaired by Defendant’s intentional destruction of evidence.

More recently, however, the Court in Cedars-Sinai Medical Center v. Superior Court,⁵⁶ has limited intentional spoliation claims to exclude parties to the underlying litigation. In Cedars, the Plaintiff in a malpractice claim sought to amend their complaint to add an intentional spoliation claim against the Defendant hospital when the Defendant failed to preserve relevant medical records. The court ruled that since adequate and effective remedies were available to parties in the original malpractice action, it is preferable to rely on the non-tort remedies.

Additionally, there is a split as to which jurisdictions recognize this new cause of action. Courts in Alaska, Florida, Illinois, Kansas, New Jersey, New Mexico, Ohio, and Louisiana have all recognized the separate tort of intentional spoliation of evidence. Idaho, Mississippi and North Carolina, have all discussed the principle and recognized the serious interference to the litigant’s case, but have not explicitly recognized the intentional tort to the extent California has. Finally, a number of states have declined to recognize the tort including Arizona, Arkansas, Georgia, Indiana, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Missouri and New York.

⁵⁴Black’s Law Dictionary 1401 (6th ed.1990).

⁵⁵Smith v. Superior Court, 151 Cal. App. 3d 491, 198 Cal. Rptr. 829 (1984).

⁵⁶Cedars-Sinai Medical Center v. Superior Court, 18 Cal. 4th 1, 74 Cal. Rptr. 2d 248 (1998).

B. Cost / Benefit Analysis - Proportionality

With the explosive growth of the “personal computer,” the 1980's saw exponential growth in the number of computers used, both at home and in commerce. Additionally, as data storage became increasingly less expensive and more available, the amount of data companies retained rapidly grew. As a result, the amount of computerized data being sought in discovery began to become unmanageable, and often became the focus of abusive discovery tactics. Partially as a result, Rule 26(b)(2) was added in 1993 to give the court the discretion to limit discovery “if the burden or expense of the proposed discovery outweighs its likely benefit.” This addition helped to alleviate the growing problem of responding to this discovery onslaught, and gave the court the discretion to limit oppressive discovery, including (but not limited to) computerized discovery and thus became especially relevant in light of the enormous amounts of data generated, stored, and used by parties in their computer systems.

Not only did the rapidly increasing discovery demands begin to increase the burdens placed on parties to the legal action, the amount of data subpoenaed and requested began to overwhelm third-parties and non-parties as well. In a recent case, Braxton v. Farmers Insurance Group,⁵⁷ the Plaintiff subpoenaed e-mails between the Defendant insurance company and third party insurance agents. The court relieved the third party agents from the burden of this discovery, stating that the discovery should more properly come from the Defendant rather than burdening an innocent third party.

Additionally, the courts in recent years have been implementing a host of innovative cost containment measures designed to alleviate the time and expense to parties complying with large discovery requests. One such innovation has been the increased use of neutral third party experts. In Tulip Computers Int'l v. Dell Computer Corp.,⁵⁸ Plaintiff Tulip sued Defendant Dell in a patent infringement action. Dissatisfied with Dell's response in a number of areas, Tulip filed a motion to compel and for sanctions. One issue was Dell's refusal to provide the e-mails of Dell's senior executives “unless Tulip can demonstrate a direct connection to this matter.”⁵⁹ Since Tulip could not easily demonstrate a direct connection without the subject e-mails, they proposed a solution using a third party expert. In response, the court adopted the proposed solution and ordered the Defendant to turn data over to Plaintiff's expert for keyword searching, based on a mutually agreed list of key words. After searching, the expert identified a list of documents to Dell which after reviewing for privilege and confidentiality, they then

⁵⁷Braxton v. Farmers Insurance Group, 209 F.R.D. 651, (N.D.Ala.).

⁵⁸Tulip, *Supra*.

⁵⁹Tulip at 4.

produced to Tulip.

A second approach in dealing with voluminous data requests is a sampling or “marginal utility approach.” Here, a portion of the data is examined for relevance before the court decides whether the entire amount of data is to be produced. This approach was used in McPeek v. Ashcroft⁶⁰ where the Plaintiff sought the complete restoration of the United States Department of Justice’s backup system and a full search for relevant documents. When the Government balked at such an enormous request, the Court ordered a “test run” restoration of a small subset of data, with results and costs documented, before deciding on whether to search all of the data.

C. Cost Allocation

*Too often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter. . . . [D]iscovery expenses frequently escalate when information is stored in electronic form. Rowe Entertainment, Inc. V. William Morris Agency, Inc.*⁶¹

Enterprises now store enormous amounts of data in a wide variety of locations, including document servers, backup tapes, e-mail servers, users’ individual computers, laptop computers, personal digital assistants, zip drives, CD-Roms, and many more. Given the amount of time and money required to locate, retrieve, review, and produce this prodigious amount of digital data, the burden in responding to a discovery request can be significant, especially when costly and time-intensive retrieval from backup tapes is involved. In Linnen,⁶² Defendant A.H Robbins discovered they had been storing over 1,000 old backup tapes. The cost to restore the data contained on the tapes was in excess of \$1,000,000. As the Linnen court stated, “While the court certainly recognizes the significant cost associated with restoring and producing responsive communications from these tapes . . . this is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world.”

Traditionally, “[u]nless the task of producing or answering is unusual, undue or extraordinary, the general rule requires the entity answering or producing the documents to bear that burden.”⁶³ This includes the costs to research, retrieve, review for privilege

⁶⁰McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001).

⁶¹Rowe Entertainment, Inc. V. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y 2002).

⁶²Linnen (Supra.).

and confidentiality, copy, and deliver. But with the huge volumes of electronic data involved in modern litigation, the costs can be extremely high, and the courts have shown some sympathy to burdened parties. The alternative, requiring the requesting party to cover the costs of the production, may increase judicial efficiency since it requires the requesting party to impose a cost-benefit analysis and decide if the production expense is justified. Unfortunately, however, this “market approach” has serious disadvantages. Aside from being unorthodox, such an approach may serve to cause meritorious plaintiffs to abandon their claims out of financial hardship if unable to afford the Defendant’s discovery. As a result, the courts have begun examining the shifting of costs onto the requesting party only under certain narrowly prescribed circumstances.

When the Plaintiffs in Rowe Entertainment, Inc. V. William Morris Agency, Inc.,⁶⁴ issued sweeping discovery demands, the Defendants moved for a protective order relieving them from the burden of producing the responsive e-mails, arguing that the burden and expense (estimated to be over \$1,000,000 for the four Defendants combined) of restoring, producing, and reviewing for privilege and confidentiality would be out of proportion to any possible benefit. In the alternative, the Defendants sought to shift the cost of such extensive - and expensive - discovery onto the Plaintiff.

In response, the court declined to issue the protective order as the Plaintiffs’ requests were generally relevant, but instead developed an eight factor test to determine whether the costs should be shifted to the requesting party. (1) *Specificity of Request(s)* - Broad, less specific requests are more appropriate to shift to the requesting party. “Where a party multiplies litigation costs by seeking expansive rather than targeted discovery, that party should bear the expense.”⁶⁵ (2) *Likelihood of a Successful Search* - The more likely it is that data at issue contains relevant data, the fairer it is that the respondent search and produce at its own expense. (3) *Availability from Other Sources* - Where “data has already been made available, or is accessible in a different format at less expense,”⁶⁶ the costs should be shifted to the party making the request. (4) *Purposes of Retention* - Data stored in connection with current business activities are more properly the responsibility of the producer. Conversely, data that is stored for archival or backup purposes, or data not intentionally stored (i.e. “deleted” items on the users hard-drive that take elaborate computer forensics to uncover) is more appropriately the responsibility of the requesting party. According to the court in Rowe, backup tapes and old archived e-mails fall into the latter category. (5) *Benefit to the Parties* - There is less rationale for shifting the cost to the requesting party when the party responding to discovery reaps

⁶³Continental Illinois Nat’l Bank & Trust Co. v. Caton, 136 F.R.D. 682, 685 (D. Kan. 1991).

⁶⁴Rowe Entertainment, Inc. V. William Morris Agency, Inc., supra.

⁶⁵Rowe at 430.

⁶⁶Id.

some tangible benefit from the production, such as being able to later use a computer search program or a litigation benefit from the extra data. (6) *Total Cost* - As the magnitude of the cost increases to the producer of the data, so does the reasonable expectation that the requesting party contribute to its production. (7) *Ability to Control Costs* - Where there is some discretion as to the scope of the discovery, “[I]t is more efficient to place the burden on the party that will decide how expansive the discovery will be.”⁶⁷ (8) *The Parties’ Resources* - The relative financial strength of the parties may be an appropriate consideration as well. Discovery costs that outstrip the respondent’s financial resources justify a cost shifting to the propounder of the discovery. The ultimate decision of the Rowe court was to require the Plaintiff to bear the costs of production for its requests, but require the Defendant to pay for its own privilege and confidentiality review.

The court in Rowe explained the break with the traditional “producer pays” model:

even if this principle is unassailable in the context of paper records, it does not translate well into the realm of electronic data. The underlying assumption is that the party retaining information does so because that information is useful to it, as demonstrated by the fact that it is willing to bear the costs of retention. That party may therefore be expected to locate specific data, whether for its own needs or in response to a discovery request. With electronic media, however, the syllogism breaks down because the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it. And, even if data is retained for limited purposes, it is not necessarily amenable to discovery.⁶⁸

The Rowe eight factor test was later used in Murphy Oil v. Fluor Daniel, Inc.,⁶⁹ but with a slight twist. The Murphy court required the producing party to elect one of two proposed protocols. The first protocol shifted the costs to the requesting party, but allowed the requesting party to see the evidence first. The second protocol allowed the producing party to first have the opportunity to review the evidence but required them to pay the cost of culling the data.

⁶⁷Rowe at 431.

⁶⁸Rowe at 429.

⁶⁹Murphy Oil v. Fluor Daniel, Inc., No 2002 WL 246439, 52 Fed.R.Serv.3d 168, E.D.La. (Feb 19, 2002).

D. Limitations on Discovery

While electronic documents, e-mail, and other electronic data are as a general rule discoverable, there are certain circumstances in which requests for electronic information are held improper. In addition to the traditional limitations, some additional protections have been carved out for the requests of electronic evidence.

Work Product

In 1946, the U.S Supreme Court established the privilege against discovery of attorney work product in Hickman v. Taylor.⁷⁰ In Hickman, the Supreme Court acknowledged the privacy of an attorney's materials prepared in reasonable anticipation of litigation, noting that such privacy is an essential component to the orderly function of the legal system.⁷¹ The Court noted a qualified immunity for what has come to be known as ordinary or fact work product. The court will justify production of documents as witness statements when the “party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means.”⁷² They further established absolute immunity for attorney opinion work product, an attorney's subjective thoughts, mental impressions, legal theories, conclusions and opinions. The work product doctrine, later codified as Federal Rule 26(b)(3), “can be defined as the result of an attorney’s activities when those activities have been conducted with a view to pending or anticipated litigation. The attorney’s work must have formed an essential step in the procurement of the data which the opponent seeks, and the attorney must have performed duties normally attended to by attorneys.”⁷³ With the greatly increased use of the computer as a tool to prepare for litigation and the advent of computerized litigation systems, this protection applies to litigation databases and digital work product as well.⁷⁴

This distinction between opinion work product and ordinary work product has been extended to cover computerized litigation support systems and databases. When the Plaintiff in Scovish v. Upjohn,⁷⁵ sought defendant Upjohn’s document database and

⁷⁰Hickman v. Taylor, 329 U.S. 495 (1947).

⁷¹*Id.* at 512.

⁷²Conn. Practice Book §219 (2003 ed.).

⁷³Stanley Works v. New Britain Redevelopment Agency, 155 Conn. 85, 95, 230 A2d. 9 (1967).

⁷⁴Hines v. Widnall, 183 F.R.D. 596, 598-600 (N.D. Fla. 1998).

⁷⁵Scovish v. Upjohn, 1995 WL 731755 (Conn. Super.).

index to their document retrieval system, Upjohn objected, claiming the material was protected as attorney opinion work product. The court found that, although the data was prepared in anticipation of litigation, it was not opinion work product but merely ordinary work product as it failed to reveal the “thoughts, opinions and the strategies of defense attorneys.” Because the defendant’s index and database consisted of more than one hundred thousand pages of documents, “it is highly unlikely that Upjohn’s mental impressions would be exposed by production of such an index or database.”

But what about work that serves more than one purpose? What if an attorney is hired to consult on a business decision that will likely lead to litigation? Such was the situation in United States v. Aldman,⁷⁶ Defendant Aldman was evaluating whether to follow through on a merger that would result in a large loss, but generate a substantial tax refund. Knowing that the IRS would likely challenge the refund, Aldman commissioned a report by an attorney/accountant on the risks of litigation. In the ensuing litigation over the tax refund, the IRS sought the report in discovery. While the traditional rule is that such a report is not covered by the work product exception if it was created primarily to assist in a business decision, the Second Circuit held differently. Here, the court held that the fact that the report was created primarily to assist in a business decision was not relevant. The relevant question to ask is whether the report was created in anticipation of litigation, noting that FRCP 26(b)(3) requires courts to guard against disclosing an attorney’s “mental impressions, conclusions, opinions or legal theories.” Other Circuits, however, have yet to adopt this rule.

Attorney-Client Privilege

Closely related to the attorney work product exception, attorney-client privilege also limits the discoverability of data. Designed to protect communications intended to be confidential between a party and counsel where the dominant purpose is legal advice, Rule 26(b)(3) applies the attorney-client privilege to both electronic and paper documents equally.

The plaintiff in Allendale Mutual Ins. Co. v. Bull Data Systems, Inc.,⁷⁷ sued insured Bull Data Systems (BDS) to prove that a policy did not cover the insured’s loss. Allendale’s coverage of BDS was in turn re-insured by two third parties. When BDS sought in discovery to obtain communications between Allendale and the re-insurers, Allendale claimed the communications were not discoverable as they were attorney-client communications and/or attorney work product. The court enumerated the following elements: (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made

⁷⁶United States v. Aldman, 134 F.3d 1194, 1202 (2d Cir. 1998).

⁷⁷Allendale Mutual Ins. Co. v. Bull Data Systems, Inc., 152 F.R.D. 132 (N.D. Ill. 1993).

in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.⁷⁸ Here, the court found the communications were primarily business communications and, as such, were not entitled to protection.

Whether on paper or in digital form, to protect attorney-client privilege, a party must generally demonstrate that appropriate care has been taken to safeguard confidential communications with counsel, including e-mail. Disclosure of the communications with a third party can serve to destroy attorney-client privilege. As such, like their paper counterparts, data and electronic documents should clearly be marked as confidential attorney-client communications to avoid being discoverable.

Of recent concern with the burgeoning use of e-mail as a means of communication is the destruction of attorney-client privilege through interception of e-mail by third parties. To prevent losing the attorney-client privilege, the parties must take reasonable precautions to prevent disclosure. But what constitutes reasonable precautions? Does sending an ordinary e-mail, which is fairly easily intercepted, provide enough protection to be considered a reasonable precaution?

While there is little case law on the subject, the ABA Standing Committee on Ethics and Professional Responsibility has concluded, "A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."⁷⁹ Supporting this view is the fact that unauthorized interception of an e-mail is a federal crime under the Electronic Communications Privacy Act, which also provides that "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." The South Carolina Bar, however, states that the ability of system operators and others to view e-mail in transit may implicate ethical rules regarding confidentiality.⁸⁰ In either view, however, highly sensitive matters require enhanced security, such as encrypting the contents.

Inter-company e-mails are also becoming a serious problem. As more individuals, especially those removed from the legal framework of the case, access the e-mail, its purpose begins to shift from attorney-client communications seeking legal advice to ordinary non-legal business purposes. In N.C. Electric Membership Corp. v. CP&L

⁷⁸id at 137, quoting United States v. White, 950 F.2d 426, 430 (7th. Cir. 1991).

⁷⁹ 45ABA Committee on Professional Ethics and Grievances, Formal Op. 99-413 (1999).

⁸⁰South Carolina Bar Ethics Opinion 94-27, South Carolina Legal Ethics C-168 (Jan. 1995).

Co.,⁸¹ the court refused to protect, under the attorney-client privilege, a number of documents that were “addressed to a number of individuals, only one or more of whom were in-house counsel for the Defendant.”

Accidental production, often the result of poor indexing, generally destroys attorney-client privilege as well. In United States v. Keystone Sanitation,⁸² the Defendant was found to have waived privilege by inadvertently producing copies of billing statements that had not been reviewed and redacted. And in Ciba-Geigy Corp. v. Sandoz, Ltd.,⁸³ the Defendants produced all documents from a database without first conducting a privilege review. When they moved for a protective order requiring Plaintiff to return the privileged documents, the court held that such careless production amounted to gross negligence and served to waive privilege. In doing so, the court enumerated five factors to consider in deciding waiver of privilege: (1) whether reasonable precautions were taken to prevent inadvertent disclosure in light of extent of production; (2) the number of such disclosures; (3) the extent of the disclosure; (4) the measures taken to remedy the disclosure and any delay, and; (5) whether any other overriding factors would serve justice in relieving the producing party of the results of its error.

Relevance, Overly Broad and Unduly Burdensome, Trade Secrets

The purpose of discovery is to make all the relevant information available to all the parties. Therefore, this purpose is corrupted when a party attempts to use discovery as a weapon or for “fishing expeditions” rather than as a tool to reveal the facts. The 1983 amendments to the Rules were a conscious response to the ever-increasing requirements in complying with discovery and the increasing use of discovery as a weapon. In an attempted to combat “excessively costly and time-consuming activities that are disproportionate to the nature of the case, the amount involved, or the issues or values at stake,” the amendments gave “the court authority to reduce the amount of discovery that may be directed to matters that are otherwise proper subjects of inquiry.”⁸⁴ A decade later, further amendments were made, creating Rule 26(b)(2)(i)-(iii). This change was necessary as “the information explosion of recent decades has greatly increased both the potential cost of wide-ranging discovery and the potential for

⁸¹N.C. Electric Membership Corp. v. CP&L Co. 110 F.R.D. 511, 517 (M.D.N.C. 1986).

⁸²United States v. Keystone Sanitation, 885 F.Supp. 672 (M.D. Pa. 1994).

⁸³Ciba-Geigy Corp. v. Sandoz, Ltd., 916 F.Supp. 404 (D.N.J. 1995).

⁸⁴FED. R. CIV. P. 26(b)(3) (notes of Advisory Committee on 1993 Amendments to Rules).

discovery to be used as an instrument of delay or oppression.”⁸⁵

A proper response to a broad, unfocused discovery request would be an objection based on relevance, or an objection to overly broad or unduly burdensome discovery. See Belcher v. Bassett Furniture Indus., Inc.⁸⁶ Additionally, Rule 26 allows the court a measure of discretion to protect parties by limiting and/or allocating expenses as discussed previously, where the burden outweighs the benefit.

When a party requests all computer hard drives, all backup tapes, all computer disks, etc., they are likely over-reaching and hoping to find relevant data along with the irrelevant. Such was the case in In re Grand Jury Subpoena Deces Tecum dated November 15, 1983,⁸⁷ where the grand jury issued a subpoena seeking entire computers, including their hard drives and floppy diskettes. The court held that by requesting the media itself instead of specific categories of data, the subpoena requested irrelevant and personal documents along with potentially relevant ones. It was not enough that relevant data would probably be found somewhere on the drive. The subpoena was therefore quashed.

Likewise, the court is generally loathe to allow the disclosure of a party’s proprietary information. When the Plaintiff in Symantec Corp. v. McAfee Assoc., Inc.,⁸⁸ sought extensive proprietary data from the Defendant, the court responded, “Symantec seeks to obtain the entire source code for *all* of McAfee’s products dating back to 1995, as well as copies of all hard drives . . . Production of this magnitude would be unduly burdensome to McAfee . . . in terms of the proprietary nature of the information sought” and denied Plaintiff’s request.

V. What To Do When Litigation Looms

First, it must be made clear that compliance with electronic document retention obligations is a top-down corporate imperative ; it is solely the responsibility of the senior management to institute and implement data and document preservation requirements. “When senior management fails to establish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of field office actions. The obligation to preserve documents that are potentially discoverable materials is an

⁸⁵*id.*

⁸⁶Belcher v. Bassett Furniture Indus., Inc., 588 F.2d 904, 906-907 (4th Cir. 1978).

⁸⁷In re Grand Jury Subpoena Deces Tecum dated November 15, 1983, 846 F.Supp. 11 (S.D.N.Y. 1994).

⁸⁸In Symantec Corp. v. McAfee Assoc., Inc., 1998 WL 740807 (N.D. Cal. Aug. 14, 1998).

affirmative one that rests squarely on the shoulders of senior corporate officers.”⁸⁹ The Prudential court held that the Defendant violated the court order to preserve documents when its senior management failed to effectively notify the field offices of the pendency of litigation and the court order to preserve documents. The court described the management’s efforts as “a haphazard response to a serious problem of judicial administration.”

The steps necessary to safeguard digital data need to be much more proactive than steps required to preserve paper documents. Generally with paper documents, upon notice of potential litigation, the cessation of intentional document destruction and discarding adequately prevents claims of spoliation. With electronic data, however, data is lost everyday through a variety of activities. Counsel must work closely with the company’s IT department to ensure that no relevant data is deleted, and to locate and safeguard all sources of discoverable information.

If large amounts of data are significant to a case, the services of a third party expert may be advised. A computer forensics firm that specializes in electronic evidence will help to streamline the process of securing, searching, preserving, collecting, extracting, and producing the data. Though their services may be costly, the services of an expert may cost less than a sanction or even an adverse judgment.

Create an Inventory

With the help of their IT department or hired expert, a party on notice of litigation should assess their computer system and get to know its layout and structure, as well as the locations, sources, and format of data contained. In case of a future dispute over the adequacy of the response, search efforts should be documented, as disclosure may later be required to detail what steps were taken to search for, preserve, extract, and collect relevant data. This inventory should include the numbers, types, and locations of all computers, in addition to the numbers, types, and locations of all computers no longer in use, but relevant to the case. Each such entry should include the operating systems and software applications contained on each machine, the network information for each machine, any backup information specific to that machine, and of course information on the users of each machine. Server logs, internet history use files, and access records should be included.

Also, those who possess relevant information should be ascertained, paying particular attention to the locations in which they store data. In addition to those individuals identified in pleadings and requests, those who may be called as deponents or witnesses should be considered, as well as those who may have had contact with relevant

⁸⁹In re: Prudential at 615.

persons. With the list of key persons in hand, an inventory listing each person's desktop computer, laptop computer, home computer (if used for business purposes), handheld computer devices, personal information managers, network directories and files, etc. should be compiled. If data has been purged from any of the above devices, back up files or devices, backup directories, or backup tapes should be searched.

Secure

In conventional paper-based discovery, the objects sought have been physically stable. In most circumstances, there is little concern about accidental destruction or alteration. Digital discovery, however, brings to life a host of unique difficulties. Information stored in digital form is easily altered, deleted, and overwritten - either unintentionally or intentionally. Every day acts such as booting a computer, copying or moving files, and routine maintenance can make recovery of the data significantly more difficult, expensive, and sometimes impossible.

Before anything else is done, the IT department should be consulted if there is one. If not, the services of an IT professional should be retained at once - preferably one well-versed in electronic discovery. Potential sources of data will need to be mapped out, and a preservation plan should be charted to segregate and preserve necessary data.

Immediately, all data destruction and deletion policies must cease. This may not be, however, as easy as it sounds. The proliferation of organizational data throughout multiple systems and storage areas often contain multiple copies or versions of the same data. An e-mail sent to an employee arrives via a series of servers and arrives on the corporate mail server, each of which makes a copy of the e-mail. The e-mail is then sent to the user's in-box in his mail program, where it is also stored. When he answers the e-mail, there is a copy of the original e-mail in his sent-items folder, and again on the mail server. There likely exist copies of the e-mails in the local machine's cache files. Then, when the mail server(s) is (are) backed up, both the incoming and outgoing e-mails are again copied. And a single word processing document likely exists on network drives, users' backup files, users' cache files, and backup tapes. This is, of course, compounded when the user makes multiple copies or stores multiple versions. And this does not even take into account copies stored on portable media such as floppy disks, CD-Roms, laptops, personal digital assistants, portable drives, and the list goes on. Since the data that needs to be preserved is not only the data that is relevant, but all data that *may* be relevant, the preservation of data becomes a critical concern.

A first step should be the immediate suspension of the rotation of relevant backup tapes.⁹⁰ This doesn't necessarily mean all backup tapes, though. There is no obligation

to preserve backup tapes that have no relevant data. This is why it is important to have an intelligent backup strategy. First, the data most likely to be the subject of discovery must be identified. When the Defendant in Linnen continued to overwrite backup tapes well into pending litigation, the court found this behavior to be “inexcusable conduct” and noted that “the customary recycling of backup tapes . . . should have been suspended.”⁹¹ Also, any deletion of relevant e-mail must cease immediately. This means notifying anyone who might possibly be in the possession of such e-mail. Then, any documents, whether on central file servers or on individual workstations need to be protected.

Even booting a computer can destroy valuable data, as was discussed in Antioch v. Scrapbook Borders, Inc.⁹² Here, the Plaintiff in a copyright infringement action suspected the Defendant of deleting evidence from her computers. The court issued an order that required a third-party computer forensics expert to copy the hard drives of the computers in question at the earliest convenience, as “data from a computer which has been deleted remains on the hard drive, but is constantly being overwritten, irretrievably, by the Defendants’ continued use of that equipment.”

This is also the time to address programs that automatically delete data after a certain amount of time. Many e-mail clients, such as Microsoft Outlook, Eudora, and others contain “janitor” functions that allow for the “removal” of items from the “deleted items” area. Some can even be configured to delete items from the user’s inbox after a configurable time period. Processes such as these can result in the destruction of relevant data without the decision, or even the knowledge, of an individual to do so. These need to be immediately reconfigured so that nothing is deleted on any computer likely to have relevant data.

Preserve

After making sure that no data is being either intentionally or unintentionally deleted, the next step is to preserve currently existing data. The first step is to preserve any relevant data in its current state - take a “snapshot.” This means copying or “mirroring” the data from active network servers, desktop hard drives, laptop hard drives, and other sources onto some other media, whether hard drive, optical disks, tape, or some other form of storage. Next, index of the data will need to be created. This will not only

⁹⁰ Companies often create full backups on a periodic basis, usually weekly, incrementally backing up only changed data on a daily basis. These tapes are then stored for a certain time interval before being recycled or rotated and used again, overwriting the old data.

⁹¹ Linnen, *Supra*, at 10-11.

⁹² Antioch v. Scrapbook Borders, Inc., 2002 WL 31387731 (D. Minn. Apr. 29, 2002).

make it easier for both parties to make sense of the data (and may be ordered by the court), but will greatly facilitate the parties own organization of the data for production and may significantly decrease the chances of unintentionally producing confidential or privileged data.

As soon as practicable after the complaint is served, preparation for disclosure under 26(b)(1) should begin, as it is required even before advent of discovery. Preservation letters should be sent to all parties and non-parties potentially in the possession of relevant data. It may be wise, as soon in the litigation as possible, to file a motion for a protective order and/or a preservation order in order to clearly define the breadth of the parties duties and to establish boundaries to avoid the alteration or destruction of relevant electronic evidence.⁹³ In particularly egregious circumstances, the court may even allow for the search and seizure of computer and data storage media, as was done in Sega Enterprises v. MAPHIA.⁹⁴ Here, the Defendant was ordered to allow Plaintiff to enter its premises, seize computers, copy data and delete pirated software.

Educate

It may be wise to communicate with those employees who have knowledge and/or relevant documents regarding the legal action, as well as the legal obligation and importance of preserving data and documents. This communication should outline the types of data relevant to the action, the types of media sought, and the recommended course of action should they possess or encounter any relevant data. Additionally, the request should state - in no uncertain language - the consequences of failing to preserve the data, to avoid being accused of “uncoordinated and haphazard” discovery response as the Prudential⁹⁵ defendants were.

Collect

As you collect the data, you may need to lay a foundation for authenticating it should you wish to use it as evidence. With this in mind, you should carefully document its sources, methods obtained, and measure to limit access and protect the data.

Produce

Of course, before any information is released, it should be reviewed by counsel for confidentiality and privilege. When it is produced, the data should be in an

⁹³Armstrong, id.

⁹⁴Sega Enterprises Ltd. v. MAPHIA, 948 Supp. 923, 927 (N.D. Cal. 1996).

⁹⁵Prudential, *Supra*.

inalterable form to protect against alteration, accidental or otherwise. Optical media such as CD-Roms or DVD-Roms are ideal.

VI. Conclusion

Rapid technological advances and increasing use of computers both in the home and workplace have fundamentally altered the legal landscape. Because we live in a society increasingly defined by both computers and litigation, disputes over digital data and the role it plays in the court room are only likely to increase. There is, however, no turning back. The digital revolution has begun and the law must catch up with its rapid progress.

While legal action (or even threatened legal action), can be a harrowing experience, a carefully prescribed and deliberate plan can make go much more smoothly. While the complexities of responding to electronic discovery can be daunting, it does have many elements in common with traditional paper based discovery. Like traditional discovery, the interests of justice - and ultimately the interests of the parties themselves - are best served when the parties cooperate and fully exchange information in good faith. Unlike traditional discovery, however, with digital discovery, events occur more quickly and the participants can soon find themselves overwhelmed in a sea of data. Only by prompt and proactive action, can you prevent such devastating results as inadvertent disclosures, sanctions, and even default judgments. However, in the end, you may save time, money, and even the company itself by responding properly to a discovery request. No doubt those at Andersen wished they had.