

Electronic Discovery:

From Novelty to Common Target



ELECTRONIC DISCOVERY: From Novelty to Common Target

Written By Randolph A. Kahn, ESQ. & Barclay T. Blair¹

Imagine that your organization is involved in litigation, and the opposing party wants to search through backup tapes containing email for your 14,000 employees, using dozens of different search terms.² Or, the court wants you to search 30 million pages of email for the names of particular individuals.³ Or, perhaps the court forces you to create a special software application that will aid in the production of digital evidence.⁴ How will you comply? How much will it cost you?

Or, imagine that you are being sued because one of your products is purportedly making people sick, and the opposing party finds a message in your email system that reads, [I don't want to spend the rest of my career] "paying off fat people who are a little afraid of some silly lung problem."⁵ Or maybe your consulting firm is being sued for inadequate performance, and an internal email is unearthed about one of your consultants which states, "[h]e should be taking classes at community college, not charging for this."⁶ What will be the damage to your case, your company and your reputation?

Although it may be tempting to write off these real-life scenarios as little more than rare cases of the system gone awry, it will not serve your organization's interests to take this view. In fact, as this paper explores, it is increasingly likely that your organization will face or has already faced similar challenges. Electronic evidence is no longer a novelty in litigation, audits and investigations. Rather, it is a common target that organizations must address as part of their overall risk management process.

INTRODUCTION: THE ELECTRONIC DISCOVERY PROBLEM

There can be little doubt that information technology is fundamental to the business operations of corporations and government agencies around the globe. Consequently, whether it is recognized or not, the digital data and records generated by information technology systems are fundamental to these organization's ability to promote and protect their business and legal interests. Digital data and records are required for effective decision-making; good customer service; accurate analysis, forecasting and reporting; and a multitude of additional critical functions. And, today, organizations require digital information for discovery – the production of evidence in the context of litigation, audits, investigations, and other formal proceedings.

Electronic discovery is no longer a novelty. In fact, according to the courts, "[c]omputers have become so commonplace that most court battles now involve discovery of some type of computer-stored information."⁷ Despite this reality, a recent survey found that less than 20% of surveyed companies have a policy on how they would handle electronic discovery requests.⁸ Litigators often take advantage of this lack of preparation by making digital information, especially email, a key target of discovery.

The impact of being unprepared can be disastrous – resulting in thousands of hours of lost employee labor, and millions of dollars in consulting and legal fees. In some cases, litigants have been forced to search, copy and produce millions of email messages at their own cost. In other cases, litigants have been required to create special computer programs to find and extract discoverable data and files believed to have been deleted.

It is clear that organizations need to act now to prepare for the e-discovery challenge. This paper examines the importance of developing and enforcing e-discovery policies and practices, investing in supporting technology, and educating employees. It also explores the consequences of failing to prepare for e-discovery. Finally, it provides an overview of an approach that can help organizations prepare for ediscovery.

ELECTRONIC DISCOVERY TODAY

All parties in litigation must disclose “a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses . . .”⁹

Organizations involved in litigation, audits, investigations, and other formal proceedings have a need to find, collect and produce records, documents and other evidence relevant to the proceeding. Generally speaking, the term “discovery” refers to the process by which a litigant, court or regulatory agency requests or orders the production of such information. Federal and state rules of evidence and rules of civil procedure are the primary source of rules regulating the production of evidence in litigation, including electronic information.¹⁰

WHAT IS DISCOVERABLE?

*A CEO of a public company is arrested and later indicted by a U.S. federal grand jury for obstruction of justice because he “directed another individual to . . . delete certain computer files . . . containing phone messages he received” although he “well knew that at the time that he directed the destruction of documents . . . such documents were material to the SEC’s investigation” regarding insider trading.*¹¹

Rules of evidence and civil procedure have supported the discovery of electronic information for many years. For example, in 1970 the Federal Rules of Civil Procedure (F.R.Civ.P.) were amended so that discovery principles applying to paper-based records would apply equally to electronic records. The amended language of the F.R.Civ.P., and related case law, make clear that electronic evidence is discoverable in federal courts.¹²

The F.R.Civ.P. define a discoverable “document” as including, “writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form”[emphasis added].¹³ State rules relating to discovery contain similar language. Clearly, the definition of discoverable information is very broad and could be applied to nearly any type of electronic information.

Because of the scope of allowable electronic discovery, organizations need to think beyond typical definitions of an “electronic record” or “document,” and consider the entire range of digital information that may be subject to discovery. While the need to produce word processing and spreadsheet documents may be obvious to most organizations, email, instant messages, and other “casual” or “hidden” types of evidence may not be.

OBVIOUS FORMS

“The law is clear that data in computerized form is discoverable even if paper ‘hard copies’ of the information have been produced...”¹⁴

Certain forms of discoverable digital information may be more “obvious” to organizations, both in terms of the need to retain and manage them, and their inclusion in discovery requests. However, even the most obvious piece of evidence, such as a word processing document in electronic form, may present unique challenges. Such documents may in fact contain metadata (i.e., “data about data”) that reveals important information. For example, the Wall Street Journal recently reported a story about a political candidate who was able to determine the origin of a smear campaign by accessing the metadata of a word processing document.¹⁵ This unique quality of digital information – that certain parts of it may be invisible unless viewed using the appropriate software and techniques, adds to the challenges of managing data that one day may be produced in the context of a lawsuit.

Similarly, electronic documents such as spreadsheets may contain information that is only “viewable” with the related software application. For example, a spreadsheet calculation may be fundamental to understanding it as evidence, yet would likely be absent if the spreadsheet were printed. Courts have responded to this reality by requiring that electronic versions of evidence be produced in discovery, even though printed copies were available.¹⁶

HIDDEN FORMS

The scope of discoverable digital information does not end with electronic documents and other clearly identifiable “packages of bits.” In fact, there is an entire realm of potentially discoverable evidence that many organizations may not even be aware of.

Newer communications technologies and techniques may in fact offer a goldmine of unmanaged information to a litigant. Email, instant messages, wireless PDA data, and chat room or discussion database conversations are often not captured and properly managed by organizations, because they fail to apply information management and retention policies across the board. Also, such technologies may not easily lend themselves to management, as they are typically used in a casual, distributed and personalized manner.

There have been many cases where email or instant messages were admitted as evidence, and regulators such as the SEC and NASD require such information to be managed like any other record.¹⁷ An August 2, 2002 Wall Street Journal article entitled “Wall Street Has E-Mail Problems” makes clear the brokerage firms are not complying with regulations to manage email and are paying a heavy price for their failure. Other novel forms of electronic evidence, such as that stored on a personal digital assistant (PDA) have also been admitted into evidence.¹⁸

ELECTRONIC EVIDENCE, PARTICULARLY EMAIL, IS A TARGET

Not only are “non-typical” forms of electronic evidence, such as email and instant messages allowable under discovery rules and case law,¹⁹ they are in fact a target in discovery. There are several reasons why such evidence may offer a “treasure trove” of information that would not otherwise be found in more obvious documents.

Lack of management. “Databases frequently turn into information dumps, teeming with poorly classified or outdated information.”²⁰

Good litigators know that organizations commonly fail to apply the same rigorous records management processes to email and other forms of electronic evidence that they do to paper records and more obvious forms of electronic evidence. This lack of management increases the likelihood that useful information will be found in the servers, network, desktop computers, PDAs, backup tapes and other sources long after it should have been disposed of in the ordinary course of business.

The burden. “They lavished huge sums of time and money on an issue that did not remotely justify the expenditure, and which would have been more profitably spent focusing on the merits of this case.”²¹

Litigators have used electronic discovery as a tool to delay or discourage opposing parties by requesting time-consuming and expensive searches through volumes of digital information. In one case, a shareholder class action suit, after months of disputes over allegations of intentional destruction of electronic and hard copy evidence, the court found that “. . . neither the plaintiffs nor defendants have full command over what documents they possessed,” despite having collectively spent more than \$1.5 on the discovery-related dispute – an amount adjudged by the court to be “nothing short of shocking,” and “wholly disproportionate to what the evidence has disclosed.” The final result of these expenditures ultimately bore little bearing on the outcome of the case.²²

Complying with broad electronic discovery requests may be extremely costly for an organization. Even so, the courts may only be sympathetic if discovery is found to be “unduly burdensome” – a standard that can vary widely. For example, the courts have found that creating special programs to search digital information at the producing party’s expense,²³ and providing copies of hard drives so they can be searched for deleted email²⁴ was not unduly burdensome. Courts have also dealt with discovery requests that involved reproducing backup tapes (at an estimated cost upwards of \$1.75 million in one case,²⁵ and \$235,015 per month of backup tapes in another²⁶), searching email backups for 14,000 employees,²⁷ and other activities that could only be undertaken at create expense and inconvenience.

Casual, contextual smoking guns. Communications technologies such as email and instant messaging have replaced the water cooler as the forum for casual conversation among employees (Even though email use today is not confined to casual chat. Substantive business is now transacted everyday in most companies using email and IM). However, unlike the water cooler, email and instant messaging memorialize these conversations. As a result, many litigators are eager to find the so-called “smoking gun” email that will reveal thoughts and conversations that may not have been formally recorded in other business records. There have been many widely reported cases where this has occurred, including a recent \$100 million settlement in the securities industry prompted in part by email messages that revealed conflicts of interest.²⁸ In another recent case, an employee adding the comment, “Yikes, Pls note the rail screwed up . . .” to a forwarded email provided an important piece of evidence in a dispute over a shipment of spoiled produce.²⁹

“If you want to make someone look bad, it’s easy to take words on a page intended sarcastically out of context. Often email produces guns that shouldn’t be smoking but appear as though they are.”³⁰

Email and instant messages also provide a unique management challenge because their contents are often contextual – that is, their meaning relies on related messages in the “chain” of conversation, the reasons for the conversation, the relationships among the parties, and other factors. Despite this, litigators may be able to bolster their case by isolating individual messages and emphasizing their contents.

An organization that is unable to separate and produce only email that is relevant during discovery may be subject to embarrassment and reputation damage – and therefore may decide to forgo litigation altogether. Although many people wrongly perceive email to be private, an organization unable to cost-effectively filter discoverable email may inadvertently enter evidence of sexual affairs, internal squabbling, irrelevant confidential information and other embarrassing activities into the public record.

The “viral effect”. Digital information, particularly that found in email messages, has the ability to be widely disseminated in a short time (i.e., like a virus), which makes it difficult to identify and properly manage all the copies of an email message (and attachments) that may exist. For example, a single email and its attachments may exist on the creator’s computer; multiple email servers; the desktop, laptop and handheld computers of each recipient; in printed copies; and in a multitude of additional locations. Clearly, ensuring that each copy of an email is properly managed and disposed of pursuant to a retention schedule is difficult – which can be taken advantage of by discovering parties.

FAILING TO PLAN AND INVEST IS NOT AN OPTION

“If 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 useable by others.”³¹

Failing to be proactive in developing and enforcing management policies that account for ediscovery can have disastrous consequences. Reacting to a discovery request when the required information has not been properly managed ahead of time can be a major drain on company resources, and can distract an organization from its core operations.

One of the reasons that the cost of e-discovery can take companies by surprise is the state of the law. Although related rules and case law have clearly established that nearly any form of electronic information is discoverable, the courts have not taken a consistent approach in determining what is “unduly burdensome” and to assigning costs associated with e-discovery. As such, it may be difficult to predict the costs associated with any particular case.³² Therefore, as this section will discuss, e-discovery can be very burdensome, and especially when organizations have failed to plan and invest in advance.

Search and retrieval costs. In some cases the courts have placed the burden on the producing party to weed through massive volumes of email to find relevant messages. In one such case, a discovering party (plaintiff) wished to search “³⁰ million pages” of email stored on the producing party’s (defendant’s) backup tapes for the names of particular individuals.

The producing party argued that the discovering party should pay the cost of compiling, formatting, searching, eliminating duplicates, and retrieving the requested email. However, the court found that the request was not “unduly burdensome” because the difficulty and cost of the effort was largely due to the limitations of the producing party’s software, and ordered them to undertake the retrieval at their own expense.³³

Creating or buying software. “[I]f a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk.”³⁴

“...the producing party can be required to design a computer program to extract the data from its computerized business records, subject to the Court's discretion as to the allocation of the costs of designing such a computer program.”³⁵

An organization required to produce electronic evidence may be required to buy special software or even develop their own software that will allow the data to be searched, compiled, copied, and/or converted into a different format. This is more likely to be the case if the organization maintains its data in a disorganized, complex or proprietary manner that the discovering party cannot easily replicate on their own. In one case, an employee discrimination lawsuit, the discovering party (plaintiff) sought 210,000 hard copy pages of email. The producing party (defendant) instead delivered 4-inch tape media, which the discovering party did not have the technology to access and review. The court subsequently required the defendants to copy the email onto a hard drive and provide it to the discovering party.³⁶

Having software that centrally manages and indexes messages and eliminates duplicates may help streamline the discovery process by enabling the search for relevant messages. There may be upfront costs associated with buying or building an application, however it is likely less expensive than manually searching for responsive messages under tight time constraints and may generally promote access to needed email for normal business purposes.

Penalties for destruction of evidence. “A party is obligated to retain evidence that it knows or reasonably should know may be relevant to pending or future litigation . . . Obviously service of a discovery demand places a party on notice to preserve the materials explicitly requested, but the duty to preserve arises whenever a party has been served with a complaint or anticipates litigation.”³⁷

An organization without a formal approach and mechanism for retention runs a greater risk of being penalized from improper destruction of evidence. As the quote above illustrates, the duty to retain all relevant information may begin when a party anticipates litigation – even before a formal discovery process has begun. Clearly, without a mechanism for informing employees of the need to retain information that might otherwise be destroyed in the ordinary course of business, and for finding and preserving information related to the case, an organization has little chance of fulfilling this duty.

The courts take such destruction of evidence (often referred to as “spoliation”), willfully or inadvertent, seriously. Willful destruction of email and other evidence can rise to the level of a felony. Courts have the ability to dismiss claims outright in cases of spoliation, and to mete out sanctions designed to “serve prophylactic, punitive, and remedial purposes.”³⁸ In one case, a smoker suing a tobacco company was awarded \$700,000 in damages because the company had destroyed email messages and evidence in a “deliberate attempt to subvert court processes.”³⁹ In another case, a former CEO was found to be personally responsible for “failing to exercise any ongoing oversight to ensure” that evidence related to a shareholder lawsuit was preserved, and was subsequently fined.⁴⁰ In yet other case, a company was sanctioned for purging electronic records according to their retention schedule during the courts of litigation.⁴¹ Case after case clearly demonstrates that the courts will not tolerate a failure to preserve electronic evidence.

Additional hard and soft costs. Even basic operations, such as searching backup tapes of email, can be costly and labor intensive. In once case, experts estimated that it would take 600 hours to review email contained on twelve monthly backup sessions, at a cost of \$99,000.⁴² Other e-discovery related costs may include:

- **Employee time lost** to participating in e-discovery efforts. This “soft cost” can in fact be the source of greatest expense, as dozens of IT and other staff are tied up in the discovery effort.
-

- **Forensic experts** for data recovery and testimony
- **Technology experts** for custom coding
- **Computers**, servers and networks taken offline, or made unavailable
- **Software** to collect, search and store relevant information

E-DISCOVERY PLANNING

Increased reliance on information technology, and the increased targeting of electronic evidence by litigators, regulators, and investigators means that most organizations are likely to face the challenge of ediscovery. Therefore, an organization's best interests can only be served by preparing for those challenges today. There are few alternatives to the development and enforcement of information management policies and practices that include an e-discovery plan. Further, aside from e-discovery, proper management of electronic information has clear benefits such as improved customer service and more efficient operations. In any case, such policies and practices should consider the following issues:

1. **Assign clear responsibility** for e-discovery. As mentioned earlier, the courts have found that executives with day-to-day management obligations share responsibility for ensuring that ediscovery duties are observed. The judge in one such case even chided the board of directors for not taking a more active oversight role. The organization should clearly define who is ultimately responsible for policy development, enforcement, training, notification and other duties.⁴³
 2. **Create a clear notification mechanism.** In the event of a discovery request or anticipated litigation, everyone in your organization who may have control of potentially relevant information should be notified of the requirement to retain information to prevent inadvertent spoliation. For example, email that would normally be disposed of in the ordinary course of business pursuant to a retention schedule may need to be retained in anticipation of litigation.
 3. **Training and education.** Every employee in your organizations should be aware of the duty to manage records and other information in accordance with written policies generally, and should also understand their obligations in the face of audits, investigation and litigation. Employees should also be educated about acceptable use and their conduct should be evaluated against these policies.
 4. **Make "wheat and chaff" decisions.** The volume of digital data that organizations must manage is overwhelming. Organizations should ensure that they are spending their resources managing the information that has the most value. In addition, the ongoing elimination of duplicate email, drafts, and so on, in accordance with a written policy, can reduce the burden of e-discovery.
 5. **Technology investments.** A key reason that e-discovery turns out to be burdensome for organizations is the lack of appropriate management technology and searching tools. For example, the ability to search email messages by name, dates, subject lines, routing information, keywords, and other criteria can turn a long and expensive discovery process into a routine operation. Greater flexibility in indexing and retrieval tools can lead to significantly lower soft and hard costs for e-discovery. In addition, the ability to quickly locate and produce information across your organization support a host of business goals, such as improved customer service, and more timely and accurate forecasting and reporting.
 6. **Manage in electronic form.** Courts may require information that was generated in electronic form to be produced in electronic form, even if paper copies are available. Courts may look negatively upon litigants who attempt to thwart the discovery process by failing to provide evidence in its native format. In one complex case, the producing party attempted to comply with a discovery order for records that were stored in a database by directing the discovering party to dozens of warehouses around the world where hard copy records were stored. The Court ruled that this approach did not satisfy their obligation pursuant to F.R.Civ.P.
-

34(b) “that documents be made available for inspection at a reasonable place,” and that their response was “patently unreasonable,” and was an “empty gesture ... arguably designed to further frustrate the discovery process.”⁴⁴ Aside from what the courts required in terms of production format, managing information in electronic form improves searchability and access, thereby reducing discovery and other costs for your organization.

7. Remove records from active systems. Broad discovery orders can result in an organization’s workstations, servers and networks being periodically unavailable for business operations while they are searched for relevant information. Regularly moving electronic records and other information off of active systems in and into records management, document management and archival systems can help organizations avoid this eventuality.
8. Involve the IT/IS department. Clearly, as the “owner” of the systems that generate and house digital information, your organization’s IT department has a role to play in the e-discovery process. As such, the IT department should be a part of e-discovery planning. From implementing technology with information management in mind from the outset, to assisting in retrieval and production, to educating executives and attorneys and providing testimony, the IT department plays many roles in the e-discovery process.

CONCLUSION

Electronic discovery is no longer a novelty. Rather, it has become a challenge that every organization is likely to face at some point. Further, electronic evidence – email in particular – has become a favorite target of litigators, regulators and investigators. Unmanaged and unguarded email “conversations” are a veritable goldmine of useful information in the litigation context.

Organizations need to be proactive in addressing this reality. Existing policies, practices, and technology approaches should be viewed in a harsh light that takes into account the millions of dollars, thousands of employee hours and other burdens that organizations have faced in the past for failing to get it right. Even organizations that are facing litigation today can benefit from improvements in technology and policies to streamline the discovery process.

Properly managing information should be a priority within all organizations – not just because of e-discovery, but because it is essential to ongoing business success.

ABOUT THE AUTHOR

Randolph A. Kahn, Esq.

Randolph A. Kahn, Esq., is an attorney and consultant with expertise in the legal, risk and policy issues of digital information, business records and e-business processes. As a principal of Kahn Consulting Inc., Mr. Kahn advises corporate counsels and information technology professionals in both government and corporate institutions on policy issues related to the management of digital information and electronic records.

Mr. Kahn's clients include federal, state, and local agencies; federal and state courts; Fortune 500 corporations; information technology vendors; and other organizations. Specific areas of expertise include electronic records management; electronic filing; enterprise email management strategies; electronic and digital signature legality; and electronic discovery. Mr. Kahn also has vertical expertise in the pharmaceutical and financial services industries.

In addition to teaching at George Washington University, Mr. Kahn conducts more than 30 seminars, lectures, and keynote addresses across the country each year. Mr. Kahn is also a frequent contributor to publications such as *The Business Lawyer* (American Bar Association), *Business Law Today* (American Bar Association), *Digital Discovery and E-Evidence*, *e-doc Magazine*, and *KMWorld*. Mr. Kahn is involved with a number of international industry groups, including the American Bar Association's Electronic Evidence and Information Security Committees; Federal Bar Association; AIIM International; ISO, PDA (Parenteral Drug Association); ARMA International; and others.

- 1 This White Paper was drafted by Randolph Kahn, ESQ. & Barclay Blair of Kahn Consulting, Inc., at the request of Legato Systems. Question and comments can be directed to Mr. Kahn at 847-266-0722 or info@KahnConsultingInc.com. The White Paper or any information contained in it should not be considered a legal opinion or professional advice. It is advisable for an organization with any specific questions or concerns to consult with legal counsel.
- 2 Proctor & Gamble Co. v. Haugen, 179 F.R.D. 622 (D. Utah 1998).
- 3 In re Brand Name Prescription Drugs Antitrust Litigation 1995 WL 360526, N.D.III., 1995. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html> (date accessed: July 25, 2002).
- 4 Sanders v. Levy, 558 F. 2d 636; U.S. App. Lexis 12778.
- 5 3 Schmidt, Richard B., "The Cyber Suit: How Computers Aided Lawyers In Diet-Pill Case", The Wall Street Journal, October 8, 1999.
- 6 Johnson, Gregory S., "A Practitioner's Overview of Digital Discovery", GONZAGA LAW REVIEW (Vol. 33:2 1997/98).
- 7 Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985).
- 8 Source: PricewaterhouseCoopers/Section of Litigation of the American Bar Association Pulse Survey, May 2000.
- 9 FED. RUL. CIV. PROC. 26(a)(1)(B). Available online at: <http://www.law.cornell.edu/rules/frcp/overview.htm> (date accessed: July 25, 2002).
- 10 "The Federal Rules of Civil Procedure: The Impact of Digital Discovery," published online by The Berkman Center for Internet and Society at Harvard Law School, October 10, 200. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library.html> (date accessed: July 25, 2002).
- 11 United States of America v. Samuel Waksal, Available online at: <http://news.findlaw.com/wsj/docs/imclone/usvwaksal080702ind.pdf> (date accessed: August 8, 2002).
- 12 "Digital Discovery: State of the Law," published online by The Berkman Center for Internet and Society at Harvard Law School, October 10, 200. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library.html> (date accessed: July 25, 2002).
- 13 FED. RUL. CIV. PROC. 34(a).
- 14 Anti-Monopoly, Inc. v. Hasbro, Inc. 1995 WL 649934, 1995 U.S. Dist. LEXIS 16355, S.D.N.Y., 1995. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/process/antimonopoly.html> (date accessed: July 25, 2002).
- 15 Wall Street Journal, October 20th, 2000
- 16 See, for example, Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995); and American Brass v. U.S., 699 F. Supp. 934 (Ct. Int'l Trade 1988).
- 17 For example, according to the guidance provided by the NASD to the brokerage companies, Conduct Rule 3110 dealing with books and records "requires that correspondence with public customers, both written and electronic, be maintained in compliance with NASD rules and the SEC Rules 17 a-3 and 17 a-4."
- 18 Mathias v. Jacobs 197 F.R.D. 29, S.D.N.Y., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/mathias.html> (date accessed: July 25, 2002).
- 19 See, U.S. v. Siddiqui, 2000 WL 1843447 (11th Cir.); Pope v. State, 2000 WL 1877798 (Ind.App. 2000); Sola v. Illinois Human Rights Com'n, 736 N.E.2d 1150 (Ill.App. 2000).
- 20 "Growth at McKinsey Hindered Use of Data," Wall Street Journal May 20, 2002.
- 21 Danis v. USN Communications, Inc. 2000 WL 1694325, N.D.III., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/danis.html> (date accessed: July 25, 2002).
- 22 Ibid.
- 23 Sanders v. Levy, 558 F. 2d 636; U.S. App. Lexis 12778
- 24 Playboy Enterprises, Inc. v. Terri Welles, 60 F. Supp. 2d 1050; 1999 U.S. Dist. Lexis 12895; 45 Fed. R. Serv. 3d 981
- 25 Thomas F. Linnen et al. v. A.H. Robins Company, Inc., et al., 1999 Mass. Super. Lexis 240
- 26 Alexander v. FBI, 188 F.R.D. 111; 1998 U.S. Dist. Lexis 22562
- 27 Proctor & Gamble Co. v. Haugen, 179 F.R.D. 622 (D. Utah 1998).
- 28 "Subpoenaed Enron E-Mail Causes Headaches," Washtech (Washington Post), May 22, 2002.
- 29 Sea-Land Service, Inc. v Lozen International, LLC, Ct. (9th Cir., April 3, 2002).
- 30 "Subpoenaed Enron E-Mail Causes Headaches," Washtech (Washington Post), May 22, 2002.
- 31 Toledo Fair Hous. Ctr. v. Nationwide Mut. Ins. Co. 703 N.E.2d 340, Ohio Com.Pl., 1996.
- 32 "In the existing discovery system, judges have nearly total discretion to order and then to limit discovery. Over the past 2-plus decades, judges' discovery orders have spanned the spectrum, including the total turnover of digital material at the expense of the producing party, cost-sharing plans, limited discovery, and other creative solutions." Comes from "Digital Discovery: State of the Law," published online by The Berkman Center for Internet and Society at Harvard Law School, October 10, 200. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library.html> (date accessed: July 25, 2002).
- 33 In re Brand Name Prescription Drugs Antitrust Litigation 1995 WL 360526, N.D.III., 1995. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html> (date accessed: July 25, 2002).
- 34 In re Brand Name Prescription Drugs Antitrust Litigation 1995 WL 360526, N.D.III., 1995. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html> (date accessed: July 25, 2002).
- 35 Anti-Monopoly, Inc. v. Hasbro, Inc. 1995 WL 649934, 1995 U.S. Dist. LEXIS 16355, S.D.N.Y., 1995. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/process/antimonopoly.html> (date accessed: July 25, 2002).
- 36 Sattar v. Motorola 138 F.3d 1164 (7th Cir.1997). Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/process/sattar.html> (date accessed: July 25, 2002).
- 37 Mathias v. Jacobs 197 F.R.D. 29, S.D.N.Y., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/mathias.html> (date accessed: July 25, 2002).
- 38 Mathias v. Jacobs 197 F.R.D. 29, S.D.N.Y., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/mathias.html> (date accessed: July 25, 2002).
- 39 "Smoker awarded \$700,000 because evidence was destroyed," The Age, April 12-13, 2002, available online at: http://www.icij.org/investigate/birnbaauer_042502.html (date accessed: May 1, 2002).
- 40 Danis v. USN Communications, Inc. 2000 WL 1694325, N.D.III., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/danis.html> (date accessed: July 25, 2002).
- 41 Applied Telematics v. Sprint, 1996 US Dist. LEXIS 14053 (D. Pa.).
- 42 Aragon, Lawrence, "E-Mail is Not Beyond the Law," PC Week, October 6, 1997.
- 43 Danis v. USN Communications, Inc. 2000 WL 1694325, N.D.III., 2000 provides an excellent overview of an organizations responsibilities in the face of audits, investigations and litigation. The court enumerated the CEO's failures as follows:
1. The CEO "personally took no affirmative steps to ensure that the [document retention] directive was followed."
 2. He did not direct that the company "implement a written, comprehensive document preservation policy, either in general or with specific reference to the lawsuit"
 3. "he did not instruct that any e-mail or other written communication be sent to staff to ensure that they were aware of the lawsuit and the need to preserve documents"
 4. "and he did not meet with the department heads after this staff meeting to follow up to see what they had done to implement the document preservation directive . . ."
 5. He "exhibited extraordinarily poor judgment" by delegating these responsibilities to an in-house attorney with no litigation experience nor experience in developing a retention program, when he had the option of using the outside law firm, with a deep experience in the area.
 - a. The in-house attorney erred by doing "nothing to ensure that all . . . employees who handled documents that might be discoverable were aware of the lawsuit and the need to preserve documents:
 - b. "he held no meetings with employees below the managerial level,"
 - c. "and he did not issue any written communications to anyone on the subject"
 - d. "[He] did nothing to determine whether the managers who attended the staff meeting followed his direction of communicating to their respective departments the need to preserve documents . . ."
 - e. "[He] did not review the pre-existing practices . . . relating to document preservation for terminated employees and closed offices, to determine whether these practices were still suitable in light of the need to preserve documents as a result of litigation."
- 44 In re Dow Corning Corp. 250 B.R. 298, Bkrtcy.E.D.Mich., 2000. Available online at: <http://cyber.law.harvard.edu/digitaldiscovery/library/process/dowcorning.html> (date accessed: July 25, 2002).



LEGATO Systems, Inc.

2350 West El Camino Real, Mountain View, CA 94040 USA

Tel (650) 210.7000 • (888) 853.4286 | Fax (650) 210.7032 | www.legato.com

For a complete listing of Legato Systems offices worldwide, please visit <http://www.legato.com/offices/>