

## TWO VIEWS FROM THE DATA MOUNTAIN

By: Steven C. Bennett and  
Thomas M. Niccum, Ph.D.\*

### Introduction

In 1975, when we graduated from high school together, the modern computer age was still in its infancy. Although most major businesses and institutions had some computerized records and operations, the volume of electronic (versus paper) records was still relatively low. The personal computer revolution, desktop networking, the Internet, and e-mail as a common form of business communication all had yet to occur.

These developments, over the last quarter century, for most businesses and institutions have produced a vast mountain of data in electronic form.<sup>1</sup> Many of the most recent developments in computer science and technology, moreover, have made it even easier to store (and, increasingly, to search) this enormous quantity of data.<sup>2</sup>

The ability to create, maintain and use this huge volume of data raises important technical and legal issues.<sup>3</sup> In essence, for most businesses, it is technically possible to keep virtually

---

\* Steven C. Bennett is a partner in the New York City offices of the law firm of Jones, Day, Reavis & Pogue and Chair of the firm's E-Discovery Committee. Thomas M. Niccum, Ph.D., is the President of Lancet Software, Inc. in Minneapolis, and an Adjunct Professor of Computer Science at the University of Minnesota. The views expressed are solely those of the authors and should not be attributed to the authors' firms or their clients. This article will appear in the Creighton Law Review (2003).

<sup>1</sup> See generally Michael R. Overly & Chanley T. Howell, DOCUMENT RETENTION IN THE ELECTRONIC WORKPLACE 1 (2001) ("Only a few years ago, the concept of a 'document' was limited to business information in traditional hardcopy form. Today, when we think of 'documents' we must think in terms of 'electronic documents.'").

<sup>2</sup> See *id.* at 2-5.

<sup>3</sup> See generally Kristin M. Nimsgar, *E-Discovery Adds Complexity to Protecting Clients and Disadvantaging Opponents*, LEGAL TIMES, March 11, 2002, at 28.

every electronic record that comes into existence.<sup>4</sup> Indeed, there are costs<sup>5</sup> and other burdens associated with attempting to eliminate electronic records on a selective basis.<sup>6</sup> In many instances, moreover, there may be legal constraints on attempts to destroy electronic records.<sup>7</sup>

We come at this problem from a common background, but from two different professional perspectives. One of us is a computer science professional who largely views the data mountain from the perspective of the possibilities of improving the efficiency and productivity of business through effective data analysis and storage. The other is a lawyer who largely views the data mountain with trepidation, knowing that what is buried in the mountain may often be the stuff of which litigation nightmares are made.

Can these two views be reconciled? Although there is no one perfect solution to this problem, we believe that businesses and institutions can, with forethought and sufficient effort, master the basic challenge of the data mountain. The final section of this Article is an attempt to outline the most important steps involved in that process.

#### Technical Developments And Issues

The data that corporations and other institutions store is growing exponentially.<sup>8</sup> Most major businesses and institutions have long since passed the tipping point, where the clear

---

<sup>4</sup> See Overly & Howell *supra* note 1 at 2-3. (noting that, in theory, a small business could afford to maintain the text of every book in the Library of Congress.)

<sup>5</sup> William S. Gyves, *Electronic Discovery is a Fact of Life: Coming to Terms with the Nuances and Costs of Discovery in Complex Litigation*, N.J.L.J., April 29, 2002 at S-5. (noting drastic costs associated with e-discovery.)

<sup>6</sup> See *id.* ("[T]he volume of electronically stored information subject to discovery can be nothing short of tsunamiic.").

<sup>7</sup> Jonathan D. Glater, *Companies Rethink What to Shred, and When*, N.Y. TIMES, July 12, 2002 at C5 (surveying examples of strict legal sanctions applied to companies that destroy electronic documentation).

<sup>8</sup> See Shira A. Scheindlin & Jeffrey Rabkin, *Outside Counsel Retaining, Destroying and Producing E-Data: Part 2*, N.Y.L.J., May 9, 2002 at 1 ("Consider, for example e-mail messages saved on a computer hard drive. In

majority of records are now created and stored in electronic form.<sup>9</sup> Even small organizations may have hundreds of gigabytes of data stored and available almost immediately, not to mention the backups archived and locked away in off-site storage.<sup>10</sup> Many office workers and professionals have thousands of e-mails (sometimes sorted into folders and sometimes merely kept as a perpetual inbox), recording nearly every scrap of e-conversation.<sup>11</sup>

As data storage manufacturers continually increase storage capacities and cut costs, our electronic file cabinets are fast approaching a capacity that is effectively infinite.<sup>12</sup> The reasons for this ever-escalating volume of data are many. Nearly every business larger than a paper route

---

(continued...)

1994, Americans collectively sent 100 million e-mails daily, and that number rose to 500 million e-mails per day in 1998. Research indicates that in 2002, Americans will send 1.5 billion e-mail messages every day.").

<sup>9</sup> See Michael R. Arkfeld, *The Wired Lawyer: Electronic Discovery Here to Stay*, 38 *Az. Attorney* 8 (July/August 2002). ("The world has changed. Now, millions of e-mails are sent daily; a typical person receives more than 30 a day. Drafts and redrafts of important business and other word processing documents are viewed and commented upon by many people and stored on computers located in many different locations. Conversations between business associates are occurring in realtime with instant messaging. Many individuals and businesses use individual or joint calendars. Many documents, data and other electronic materials are no longer being converted to paper but are created, revised and stored in electronic format.").

<sup>10</sup> See James A. Snyder & Angela Morelock, *Electronic Data Discovery: Litigation Gold Mine Or Nightmare?*, 59 *J. Mo. B.* 18 (2002). (giving example of staggering effect of electronic communications in a 1,000 person company, with each person writing eight electronic messages a day, producing two million electronic messages a year, not including other electronic documents)

<sup>11</sup> See *id.* ("[I]ncreasingly many employees have access to e-mails. The access to e-mail communications systems opens up a whole new world of communication opportunity for company personnel. Because of the relative ease of delivering an electronic communication, the sheer volume of statements, admissions, conflicting information, and correspondence has increased dramatically over the last five years. This volume increases both the likelihood of a 'smoking gun' type of statement and evidence of mitigating facts to explain the context of a particular communication or statement.").

<sup>12</sup> See Overly & Howell, *supra* note 1, at 2-3. ("One of the primary reasons so many documents are now being stored electronically is that the price of computer storage space has decreased dramatically in recent years. In 1963, one megabyte of hard disk storage cost approximately \$2,000. Today, the same amount of storage costs less than 50 cents. Because storage space has become so inexpensive, many businesses simply choose to never delete any information stored electronically. They prefer simply to keep everything 'online' for ready retrieval in the event something is needed. . . . Affordable terabyte (approximately 500 million text pages) storage is just around the corner.").

uses computers as a normal part of daily operation.<sup>13</sup> Computer systems enable collection of data about sales, inventory, financials and other aspects of business.<sup>14</sup> More and more of this data is retained as firms learn to leverage their investment in information by extracting business trends and customer tendencies from vast warehouses of archived data. This tendency to retain data is accelerated by the decreasing cost of storage.<sup>15</sup> Further, more and more interpersonal and inter-company communication is done electronically by exchanging word processing documents and e-mails.<sup>16</sup> This communication medium is responsible for massive multiplication of documents, as attachments are added to emails, documents are mailed to multiple recipients and long conversations carried out in e-mail "chains" are copied and responded to over time.<sup>17</sup> All of these electronic items are also being retained for long periods as storage capacities climb.<sup>18</sup>

Advances in data creation and storage are not the only reason that businesses are retaining more and more data. Highly efficient search techniques have made it possible to use vast quantities of data effectively.<sup>19</sup> Increasingly, due to technology like the systems that Lancel<sup>20</sup> has built, it is becoming possible to "mine" these enormous quantities of material. In

---

<sup>13</sup> *Id.*

<sup>14</sup> *See* Overly & Howell, *supra* note 1, at v (explaining how, through progress of technology, the term "document" has developed a much broader meaning, such that a "document can mean anything from a word processing file, to a spreadsheet, to e-mail, to digitized audio or video, to the elements of a vast database of information").

<sup>15</sup> *Id.*

<sup>16</sup> *See* Martin Redish, *Electronic Discovery and the Litigation Matrix*, 51 Duke L.J. 561, 588 (2001) (noting that e-mail programs usually store multiple copies of messages on both the sender's and recipient's hard drive even if an attempt to delete the communication has been made).

<sup>17</sup> *See id.* ("E-mail is often used with a lack of appropriate caution, given its near permanence – a fact seldom realized by e-mail users, who think that when they trash a message it is destroyed. Moreover, the distribution of e-mail messages is largely impossible to control because they are so easily copied and forwarded.").

<sup>18</sup> *Id.*

<sup>19</sup> *See id.* at 588-89 (noting internet search techniques and their application to other electronic search problems).

<sup>20</sup> Lancel Software, Inc. is a consultant-owned software development company involved in web-based solutions.

the past, a company might say, in response to a request by business people (internal) or lawyers (outside, in a lawsuit), "this is the best we can do, given cost and time," and the results would be limited. Now (and in the future) with effective data mining, it has become possible to pull a lot of information together for a lot less cost.

The same techniques that allow a computer user to search the web for a new broccoli recipe that contains garlic can allow huge numbers of documents to be loaded into a database and searched with sophisticated queries. Fuzzy logic and artificial intelligence techniques allow searches to find and rank documents containing words that are near each other, to find documents that contain some words but not others, or to construct a web of linkages between related documents that allow a user to navigate through the pile in a rational manner.<sup>21</sup>

The implications are significant. What would have looked like a daunting, seemingly impossible research task 25 years ago is now quite possible, and will soon become the norm.<sup>22</sup> Computer users are increasingly aware that, with these sophisticated computerized search mechanisms, millions of records can be reviewed and analyzed, and records in disparate

---

<sup>21</sup> Ashby Jones, *Discovery Becomes Electric*, N.Y.L.J., March 11, 2002 at T3. Many companies are promising new, easy approaches to discovery. The procedure generally moves all of a company's electronic documents into an electronic database. An attorney can then search the database using a keyword concept. This technique may be highly efficient. See Michael Bartlett, *Companies Must Prepare For E-Discovery*, Newsbytes News Network, May 23, 2002 at 1 (describing e-mail monitoring programs, which are designed to look for specific words or phrases, taking a conglomerate of information and "reducing it to relationships and trends").

<sup>22</sup> See Jason Krause, *Discovery Channels: Electronic Documents Are Vital to Building a Case, So Don't Get Papered Over*, 88 ABAJ 48 (2002). ("It used to be you'd send young associates out to Brooklyn to some vermin-infested, sweltering warehouse to wade through mountains of paper documents,' says Charles Weeden, chair of 17a-4, a New York City-based company that archives electronic information. 'Now, if you can put your data in a central database with a powerful enough search function, you can type in a keyword and get more information than that poor associate in Brooklyn ever could.'").

locations can be collected and compared.<sup>23</sup> The data mountain is no longer an impossible height to scale, but a vast database to be mined for secrets and insights that were previously unavailable.

Coupled with the vast expansion of electronic data, and the sharp increase in ability to search and use such data, is the fact that, in the modern computer environment, data tends to persist, often well beyond its intended useful life. Even if an institution has a document retention policy (or, more appropriately named, a document deletion policy), and employees apply the policy correctly by doing their housekeeping (deleting old e-mails and ridding disks of documents) making the data truly disappear is not quite that easy. So-called "deleted data" can continue to exist nearly forever in forms that range from immediately available to quite costly to recover, but the data is often recoverable nevertheless.

Discarded data can lurk in a number of spots that the average user may not even know about. Using the ubiquitous personal computer running Microsoft Windows, computer professionals can find data in a wide array of places:

By default, for most computer users, deleting a file does not truly delete it – (the direction to delete simply moves the file into a special folder called the "Recycle Bin."<sup>24</sup> Just as with a real trash can, if you accidentally toss something in the Recycle Bin, you can retrieve it.<sup>25</sup> For

---

<sup>23</sup> Snyder & Morelock, *supra* note 10, at 19 (analyzing sophisticated data mining procedures, and noting: "Once an image copy is obtained, information relevant to a particular litigation is identified through . . . forensic analysis of the data contained on the image copy. Many methods exist for analyzing the data to find relevant information, including searching by keyword, file type, time stamps and other file attributes. More advanced data mining techniques include text and numeric pattern recognition, as well as providing for the analysis of audio, graphics and video files. In addition to locating a file of interest, computerized information is often useful in recreating a timeline of events at issue in litigation.").

<sup>24</sup> Webopedia, *Are Deleted Files Completely Erased?* (2002), at [http://www.webopedia.com/DidYouKnow/Hardware\\_Software/2002/Erasing\\_Deleted\\_Files.html](http://www.webopedia.com/DidYouKnow/Hardware_Software/2002/Erasing_Deleted_Files.html) (defining the "recycle bin" as "an icon on the Windows 95 desktop that represents a directory where deleted files are temporarily stored. This enables you to retrieve files that you may have accidentally deleted.").

<sup>25</sup> *Id.* ("A common misconception when deleting files is that they are completely removed from the hard drive. However, users should be aware that highly sensitive data can still be retrieved from a hard drive even after the

e-mail, there is typically a similar mechanism – deleted items are not deleted, they are just moved into a special folder.<sup>26</sup> Anything in these special folders is recoverable by moving the document back to one of the user's normal folders.<sup>27</sup>

Temporary copies of documents are often created during word processing sessions to archive a document in progress in case the computer crashes.<sup>28</sup> This means that there is a "shadow" version of the document, stored on the computer's hard drive, in a place that the user does not know about – but that document recovery experts DO know about.<sup>29</sup> There are many other places where such "shadow documents" could be hiding, waiting to be recovered by computer forensics experts.<sup>30</sup>

Even when a user "empties" the Recycle Bin, such that the document is no longer easily recoverable by that user, the electronic data persists.<sup>31</sup> A computer, just like a card catalog in a library, keeps track of shelf space, with a map that indicates which slots on the shelves are occupied and which are empty. If we tell a computer to "really" delete a document (rather than

---

(continued...)

files have been deleted because the data is not really gone. Files that are moved to the recycle bin (on PCs) or the trash can (on Macs) stay in those folders until the user empties the recycle bin or trash can.")

<sup>26</sup> Michael Bartlett, *supra* note 21, at 1 (demonstrating how much greater focus is given to e-mails today, because information that was once thought to be deleted is likely to be retrievable).

<sup>27</sup> *See id.* ("People are candid with e-mail, but this is true in Word documents, also . . . when a computer is on a network, with many redundancies built in, even if someone deletes an e-mail or a document from his hard drive, and then from the recycle bin, it's still not gone.")

<sup>28</sup> *See e.g.*, Microsoft Product Support Services, *WD97: How Word for Windows Uses Temporary Files* (2000), available at <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q89247&>. (explaining that the purposes of temporary files are twofold: 1) Copying information into temporary files allows Word to access, save, or scroll through the file at more rapid speed; 2) Copying a document into a temporary file provides a fail-safe against system errors or a power failure of some sort).

<sup>29</sup> *See id.* (giving example of how temporary files interact with multiple files of which the user is most likely unaware).

<sup>30</sup> *See id.*

merely to move it to the Recycle Bin), the computer's map of shelf space is updated to indicate that a spot on the shelves is available for another document. But the document is allowed to sit on the shelf (i.e., in the computer's memory) until another document is added to the library and the spot is needed.<sup>32</sup> With the large amounts of space on today's computers, it could be a long time before that spot is needed. Also, the catalog "card" used to index the document is not fully destroyed, but just marked as "gone."<sup>33</sup> The ability to identify documents that are marked for deletion (by reviewing descriptive document names) may make it possible for a computer expert to reconstruct other information about the document (such as the date it was created and the last time it was modified).<sup>34</sup> This kind of information could be enough to tell an expert where to begin looking on backup tapes and other places for copies of the documents.

Most organizations perform periodic backup of their data.<sup>35</sup> Many organizations employ cyclical backups where data may be backed up every night, to different media.<sup>36</sup> The media are

---

(continued...)

<sup>31</sup> See Microsoft Product Support Services *supra* note 28.

<sup>32</sup> *Id.* (demonstrating what happens to a file after one attempts to delete it: "[w]hen you delete a file in Windows Explorer or My Computer, the file appears in the Recycle Bin. The file remains in the Recycle Bin until you empty the Recycle Bin or restore the file. . . . Older files are also removed from the Recycle Bin when newer files are deleted and the Recycle Bin exceeds the maximum size allocated in Recycle Bin properties. . . . Each hard disk contains a hidden folder named Recycled. This folder contains files deleted in Windows Explorer or My Computer, or in Windows- based programs. When you delete a file, the complete path and file name is stored in a hidden file called Info or Info2 (Windows 98) in the Recycled folder. The deleted file is renamed.").

<sup>33</sup> Webopedia, *supra* note 24 ("Any time that a file is deleted from a hard drive, it is not erased. What is erased is the bit of information that points to the location of the file on the hard drive. The operating system uses these pointers to build the directory tree structure (the file allocation table), which consists of the pointers for every other file on the hard drive. When the pointer is erased, the file essentially becomes invisible to the operating system. The file still exists; the operating system just doesn't know how to find it. It is, however, relatively easy to retrieve deleted files with the right software.")

<sup>34</sup> See *id.*

<sup>35</sup> MYOB, *Backup Principles*, at <http://support.myob.com.au/snote.cfm?iSNID=1300>. ("Backup is the copying of your computer generated data file(s) to disk, magnetic tape or some other form of storage device, separate from your computer system. Backups are necessary as they provide a working copy of your data that can be reloaded into your machine in case the original copy stored on your computer becomes damaged or corrupted. Data

often cycled in some pattern, such as on a weekly, monthly, quarterly and annual cycle.

Sensitive documents may also be stored on these same backups. Thus, deleting a document from a computer server may really do nothing, as the document could be on dozens of backup tapes, especially if the document has existed for a substantial period.<sup>37</sup>

The problem grows worse because of the often rapid and uncontrolled dissemination of electronic data. Even if one user is diligent in deleting copies of a document, everyone on a "cc" list must do likewise or the document will not be safely deleted.

The implications are clear: even if computer users fully comply with corporate document retention policies, it is almost always possible to retrieve some of the data that has been "deleted" with various available recovery methods. The completeness of recovery will generally depend on the resources and time dedicated to the effort.

Electronic "shredding" of documents, like shredding of paper, can make reconstruction of records very difficult, but they cannot entirely eliminate the possibility of reconstruction.<sup>38</sup>

There are several commercially available tools that can help with the "shredding" of electronic documents.<sup>39</sup> "Disk shredders" typically attempt to address the persistence of supposedly deleted

---

(continued...)

corruption can occur in numerous ways; viruses, power failures, power spikes (these are sometimes not even noticeable), system crashes, external damage such as fire or theft, or simply user error.")

<sup>36</sup> *See id.* ("How often you backup depends largely on the value you place on the information to your business' viability, and the cost of replacing and/or recreating it in the event of loss.")

<sup>37</sup> *See id.* The backup of files is performed regularly by most businesses to save time and money in case a document is destroyed. Most businesses consider this to be an integral part of its operations and most businesses are thus likely to have multiple copies of their files.

<sup>38</sup> *See, e.g.,* Associated Press, *This Article will Self-Destruct in Three Days*, USA Today, Feb. 16, 2002, available at <http://www.usatoday.com/life/cyber/tech/2002/02/18/self-shredding-e-mail.htm>.

<sup>39</sup> These tools are compared at the web-site: [http://www.fortunecity.com/skyscraper/true/882/Comparison\\_Shredders.htm](http://www.fortunecity.com/skyscraper/true/882/Comparison_Shredders.htm).

data by "overwriting."<sup>40</sup> Thus, swap file residue, deleted files and file names (any of which may contain all or part of deleted documents) are overwritten with random data.

Unfortunately, use of disk shredding software bears various costs and offers no absolute guarantee of permanent deletion.<sup>41</sup> With the large disk drives in use today, the disk shredding process can be exceptionally time-consuming.<sup>42</sup> The more overwrites, the longer the process. Depending on the shredding software used, it could take anywhere from 30 minutes to 10 hours to shred data on a typical hard drive. During that time, the computer cannot be used.<sup>43</sup>

Even overwriting data may not be enough. Experts have shown that magnetic traces may be recoverable (like "whiting out" a typewritten page and holding it up to the light to see the faint images still on the paper).<sup>44</sup> It may be effectively impossible to sanitize storage locations by simply overwriting them, no matter how many overwrite passes are made or what data patterns are written.

---

<sup>40</sup> "Overwriting," generally speaking, is the process of replacing data with meaningless data in such a way that meaningful data cannot be recovered from a hard drive. The Department of Defense states that overwriting "consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) or zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased."  
<http://hermetic.magnet.ch/dd/dd.htm>.

<sup>41</sup> See Associated Press, *supra* note 38.

<sup>42</sup> See, e.g., PC Magazine, *Shred Deleted Files* (2002), at <http://pcmag.com/article2/0,4149,258,00.asp> ("Shredding large amounts of free space can take a very long time.").

<sup>43</sup> See *id.* note 42 ("Because there will be no free space available on the selected drive while it is being shredded, you must save any open documents and close any running programs that may need to write to that drive. Any attempt to allocate additional space on that drive will fail, so it's best to have other programs shut down and your work saved before you start.").

<sup>44</sup> See, e.g., Australia's Defence Signals Directorates, *Australian Communications-Electronic Security Instruction 33 (ACSI 33)*, at <http://www.dsd.gov.au/infosec/asci33/HB6p.pdf> ("In general there is no known method short of total destruction which will completely remove all traces of the information borne by memory devices . . . or magnetic media.").

For the total elimination of data, most computer professionals would advise following the practices of the United States Military. When classified information stored on any magnetic media must be disposed of, the physical media are destroyed (usually by melting down the data-carrying media).<sup>45</sup>

### Legal Developments And Issues

Lawyers recognize that it is impossible to stop the accumulation of electronic records. Indeed, to a large degree, lawyers have embraced computer technology in their own operations. Electronic word processing, record storage and data sharing with clients all are generally seen by lawyers as a means to improve productivity and efficiency. Lawyers have also adopted electronic record search techniques as a major part of the way that legal research is performed. Law schools teach every law student the fundamentals of such research, and virtually every lawyer's office has access to, and relies upon, electronic research capabilities.<sup>46</sup> Many lawyers, moreover, have begun using sophisticated Internet and private networks and research databases as a means to harness and extend their data processing and analysis capabilities.<sup>47</sup>

Lawyers have also extended the reach of electronic commerce. Lawyers, for example, have lobbied for the passage of electronic signature laws at the federal and state levels.<sup>48</sup> These laws aim at making it possible to do business using purely electronic exchanges of contracts and

---

<sup>45</sup> See, e.g., United States European Command, *Directive 25-1, Headquarters United States European Command Security Standard Operating Procedure (SOP) (1998)*, at <http://www.eucom.mil/Directorates/ECJ1/Publications/ED/20-25/ED25-1.pdf> (discussing military protocol on destroying certain magnetic media).

<sup>46</sup> See, e.g., Harvard Law School, *First Year Lawyering*, at <http://www.law.harvard.edu/academics/fyl/description.html> (Harvard Law School's First Year Lawyering Program familiarizes students with electronic research).

<sup>47</sup> See, e.g., web-based legal research providers *LexisNexis* ([www.lexis.com](http://www.lexis.com)) and *Westlaw* ([www.westlaw.com](http://www.westlaw.com)).

<sup>48</sup> See, e.g., Robert L. McCurley, Jr., *Legislative Wrap-Up*, 62 Ala. Law. 18 (2001)(discussing the American Law Institute's support for the Uniform Electronic Transaction Act).

other transaction documents.<sup>49</sup> Lawyers have also obtained ethics opinions in many jurisdictions holding that electronic exchanges between attorney and client can preserve privilege (thus fostering such discussions).<sup>50</sup> Far from holding back the creation of electronic records or insisting that only paper records have legitimacy, lawyers are generally in step with the modern electronic records based economy.

Lawyers, moreover, have long been aware that computer technology could have a profound impact on their dispute resolution practices. Rules of civil procedure, for example, have recognized since the 1970s that electronic records are "documents" that may be produced in litigation.<sup>51</sup> Despite those rules, however, until recently, discovery in most litigation focused mostly on paper records. The reasons for this retarded development of electronic discovery are several.

First, even though many disputes involve businesses and institutions with extensive electronic records, many such disputes really turn on a relatively small number of documents. A commercial dispute of modest size, for example, may involve a contract, some background information leading up to the formation of the contract, and some correspondence and internal memoranda regarding the performance of the contract. For disputes of this size, perhaps one or two dozen documents are really key to understanding and resolving the dispute. These

---

<sup>49</sup> *Id.*

<sup>50</sup> *See, e.g.*, ABA Commission on Ethics and Professional Responsibility, Formal Opinion 99-413 (1999) (listing state bar ethics opinions that preserve attorney/client privilege when e-mail communications are utilized).

<sup>51</sup> *See*, Advisory Committee Notes on the 1970 Amendment to Rule 34 of the Federal Rules of Civil Procedure:

The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made useable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into useable form.

*See also Sanders v. Levy*, 588 F.3d 636, 648 (2d Cir. 1976).

documents are generally easy to identify and retrieve (indeed, paper copies of the documents will often be stored as conventional paper records in conventional files). Thus, sophisticated, detailed research into electronic records never becomes an issue.<sup>52</sup>

Second, even though lawyers (and their clients) may be aware of the possibility that electronic records in their adversary's hands could be important to a dispute, there is often a deep foreboding about the possibility of having to search one's own electronic records for responsive materials. A kind of "mutually assured destruction" mentality develops, in which both sides of a dispute are deterred from pressing for review of all electronic evidence.

Finally, discovery of electronic records often involves substantial work and cost for both sides of the litigation.<sup>53</sup> In the first instance, if a requesting party wishes to obtain specific electronic records, standard discovery forms may need to be modified to reflect such a request. If an adversary fails to produce electronic records, the requesting party will have to follow up, demanding information about what records exist and what searches were performed. If an adversary still resists production (or indicates that records no longer exist), the requesting party may need to get a court order to compel production of records, or to compel the adversary to give the requesting party's expert access to electronic records, for purposes of reconstructing and retrieving necessary information.<sup>54</sup> And, when records are finally made available, they must be

---

<sup>52</sup> See, e.g., *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1<sup>st</sup> Cir. 1996) (balancing costs of recovering electronic media with likelihood of discovering relevant material); *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001). (same).

<sup>53</sup> See Redish, *supra* note 16 at 590 (noting example of defendant who incurred electronic discovery costs in excess of three million dollars); see also *Rowe Entertainment Inc., et al. v. The William Morris Agency, Inc., et al.*, 205 F.R.D. 421 (S.D.N.Y. 2002) (where plaintiffs were to bear the costs of production, approximately \$850,000, and defendants were to bear the costs of any review of privileged and confidential material (approximately \$367,000)).

<sup>54</sup> See, e.g., *GTFM, Inc. v. Wal Mart Stores*, 2000 U.S. Dist. LEXIS 3804 (S.D.N.Y. 2000) (plaintiffs moved for an order to compel on-site inspection of computer records; court granted plaintiffs' expert access to computer systems).

reviewed, analyzed and collated in a coherent form. At each step, cost, burden and time are involved. Unless the potential value of the records is high, the effort may not be justified.

These prevailing attitudes toward electronic discovery, however, are likely to change as lawyers and their clients come to realize that electronic records can dramatically affect the outcome of a case. There have been several recent, headline-grabbing lawsuits where electronic records (especially, e-mails) have served as vital evidence for one side or another.<sup>55</sup> Awareness of the power of electronic discovery is likely to grow for several reasons:

- Electronic discovery offers the power to impose disproportionate burdens on parties in certain forms of litigation. Individual shareholders or consumers suing a corporation, for example, are likely to have no electronic records of their own, but they (and their lawyers) may be able to gain access to thousands (perhaps millions) of records in the corporation's files, with relatively little effort.<sup>56</sup> The burden on the corporation of having to respond to such requests may be a powerful incentive for corporations to settle such suits, even if they have dubious merit.
- The risk of being charged with "spoliation" of evidence is increased in an electronic records environment. Spoliation, in most jurisdictions, generally means destruction of records where a party knows that the records may be important in litigation.<sup>57</sup> Where a court

---

<sup>55</sup> See, e.g., Jason Krause, *Discovery Channels: Electronic Documents are Vital to Building a Case, so Don't Get Papered Over*, A.B.A.J., July 2002 (explaining how e-mails impacted the Microsoft antitrust litigation and the Clinton impeachment trial).

<sup>56</sup> See, e.g., *Linnen v. A.H. Robins Co.*, 1999 Mass. Super. LEXIS 240 (Mass. Super. June 16, 1999) (co-administrators of decedent's estate requested an order to compel production of e-mail messages retained by defendants; defendants, in opposition to the request, stated that they had already produced volumes of such messages; although the costs of producing the e-mails was high, the court granted plaintiffs' motion to compel, and ordered that defendants bear all costs associated with the production).

<sup>57</sup> See, e.g., *Willard v. Caterpillar, Inc.*, 40 Cal. App. 4<sup>th</sup> 892, 907 (Ct. App. 1995); *Aldrich v. Roche Laboratories, Inc.*, 737 So.2d 1124, 1125 (Fla. 5<sup>th</sup> DCA 1999); *Federated Mutual Insurance Co. v. Litchfield Precision Components, Inc.*, 456 N.W.2d 434, 436 (Minn. 1990); *Trigon Insurance Co. v. U.S.*, 2001 U.S. Dist. LEXIS

concludes that a party has spoliated evidence, various sanctions may be imposed, ranging from imposition of the costs required to reconstruct needed information, to an "adverse inference" (basically, a ruling as a matter of law that the missing records may be presumed to have been supportive of the requesting party's position),<sup>58</sup> to an outright judgment in favor of the requesting party.<sup>59</sup> In some instances, even criminal sanctions may accompany the destruction of records.<sup>60</sup> Again, especially for a party with relatively few records of its own, demands for electronic documents may hold the prospect of either uncovering beneficial information, or at least making life very uncomfortable for the other side.<sup>61</sup>

- Vendors are actively marketing technology to deal with electronic records, especially to lawyers.<sup>62</sup> As with the recent Y2K crisis, a small army of experts and consultants is forming to exploit this market.<sup>63</sup> Seminars on the subject are given throughout the country on a regular basis.<sup>64</sup> Unlike Y2K, however, which resolved itself with a whimper rather than a bang,

---

(continued...)

18824 (E.D. Va. 2001). *See also Black's Law Dictionary* (7<sup>th</sup> Ed.) (defining "spoliation" as the intentional destruction, mutilation, alteration, or concealment of evidence, usually a document).

<sup>58</sup> *See, e.g., Linnen, supra* note 62 (The court allowed an adverse inference where defendant failed to reveal the existence of back up tapes, which were not removed from recycling until four months after the commencement of the litigation, until months after requests had been made).

<sup>59</sup> *See, e.g., Patton v. Newmar Corp.*, 538 N.W.2d 116 (Minn. 1995) (plaintiffs unable to maintain a prima facie case after losing key piece of evidence); *Mudge, Rose, Guthrie, Alexander & Ferdon v. Penguin Air Conditioning Corp.*, 221 A.D.2d 243 (1<sup>st</sup> Dep't 1995) (dismissal warranted because of "plaintiff's negligent loss of a key piece of evidence that defendants never had an opportunity to examine."); *Shepherd v. American Broadcasting Co.*, 62 F.3d 1469 (D.C. Cir. 1995).

<sup>60</sup> *See, e.g., Temple Community Hospital v. Superior Court*, 976 P.2d 223, 227 (Cal. 1999).

<sup>61</sup> *See Krause, supra* note 61 and accompanying text.

<sup>62</sup> *See Jones, supra* note 21 at T3 (listing companies that market software to deal with electronic documents discovery).

<sup>63</sup> *See id.*

<sup>64</sup> *See, e.g., Debra Baker, Electronic Future is Now: Courtroom Innovations, Lawyer Tips at TECHSHOW 98*, 84 A.B.A.J. 93.; Law.com, *Internet Do's & Don't's: Beware of the Newest Risks*, Corporate Legal Times

this "crisis du jour" is more than just a short-term economic opportunity for some get-rich-quick consultants. These consultants and experts are educating lawyers for new rounds of escalating conflict over electronic discovery, and there is no natural stopping point for such conflict.

- Increasingly, judges, even those raised before the dawn of the modern computer era, are becoming comfortable with the technology and the size of electronic discovery. Where once it might be sufficient to tell a judge that a request involved potentially millions of pages of records, a lawyer cannot assume that a judge will deny a request for discovery on volume alone.<sup>65</sup> More and more, judges are becoming aware that it may, in fact, often be possible to review masses of records at costs and on time frames that in the past would simply have been prohibitive.

The law in this area is still developing. Although the basic practice of discovery is familiar to most lawyers, practical solutions to many issues that can arise in electronic document production have yet to become standardized into any neat set of rules to govern most cases. Instead, rules for electronic discovery are largely developing on a case-by-case basis with each judge attempting to reconcile the needs and interests of the parties as they appear in the individual matter.<sup>66</sup>

What seems certain, however, is that the issue of electronic discovery will not go away. Just as the trend in the data processing industry is toward creation of ever greater volumes of

---

(continued...)

SuperConference, at <http://store.law.com/seminars/seminarPreview.asp?prgid=101> (discussing seminars regarding electronic records).

<sup>65</sup> See, e.g., *Linnen supra* note 25 (where over 33 million e-mail messages were examined).

<sup>66</sup> Compare, e.g., *Linnen, supra* note 62 with *Rowe, supra* note 58 (where costs of discovery were distributed differently).

information,<sup>67</sup> the trend in law is toward ever greater demands for discovery of such information.<sup>68</sup>

Implications for Business  
And Institution Managers

For many business and institution managers (and their lawyers) there is a tendency to fantasize about a magic solution to the electronic records problem. Surely, with our powerful technology, there should be some technical solution to the problem. A business or institution should be able to keep only its "good" records and discard, permanently, records that are harmful or useless. Yet, there is no magic solution to the problem. Most businesses and institutions keep vast and ever-increasing quantities of outdated and useless records, which, if anyone looked closely, include many records that could, in the light of litigation, be viewed as inappropriate, embarrassing or, in some instances, absolutely devastating.

If there is no magical solution to the problem, then are there at least some ways in which the problem can be contained? We suggest here a few basic principles to consider:<sup>69</sup>

- Make records management a priority. As we have seen, the task of containing records is not an easy one. If no constraints are imposed, records tend to proliferate and to hide in many places. Substantial, active resources must be dedicated, if any real controls are to exist.

---

<sup>67</sup> See Overly & Howell, *supra* note 1 and accompanying text.

<sup>68</sup> See Overly & Howell, *supra* note 1 at 29-30 (discussing increased volumes of information that can be requested in various forms of electronic media).

<sup>69</sup> For more detailed information concerning document retention and e-mail policies, see Steven C. Bennett, Dealing With Office E-Mail, N.Y.L.J., May 16, 2002, at 5, col. 1; Steven C. Bennett, Building An E-Document Retention Policy, 3:3 InfoPro 42-45 (2001).

- Clearly identify categories of records that should not be retained. This task may be especially difficult, because of the numerous business incentives to retain records, outlined above. Review of legal constraints on document destruction, moreover, should be an essential part of this task. Failure to identify the target group of records, specifically, however, may result in over-inclusion or under-inclusion in the document disposal process. Employees (both those in information technology and those working in other areas) require clear guidance.

- Take steps to ensure that documents that should be destroyed truly are. In addition to considering technical solutions (electronic shredders and the like) a business may require specific policies and compliance mechanisms to ensure that copies of documents are not maintained in uncontrolled, unaccountable places within the organization. It may be particularly important, in this regard, to identify the "official" location for certain types of records, and to encourage employees to discard all drafts and copies of the records, other than those in the official location.

- Recognize that document destruction practices, once initiated, may be difficult to stop. Routine recycling of back-up media, for example, is an engrained part of the normal information technology function. There must be clear, effective contingency plans that will permit the business to preserve data whenever a dispute arises that may require use of the records, and certainly when a specific demand has been made for records, in a lawsuit, or by a regulatory agency.

- Pay particular attention to concerns about privileged or highly confidential records. Although many of these records will have to be retained, clear identification of such records may make it much easier, if and when document requests are made, to ensure that privileged and confidential records are not produced, without some special consideration.

- Consider document organization and retrieval as a species of document retention.

To a large degree, in today's information environment, the contention that "we do not have any such records" is really a statement that "after reasonable search, we have been unable to retrieve any such records." When a formal document request comes (in litigation, or as part of some regulatory effort) the business will need to be in a position to establish that the search, in fact, was reasonable. If electronic records are well organized, and search capabilities are adequate, it will be much easier to explain (to a court or government agency) why the business should not be required to spend additional time and effort searching for records that might have been missed.

### Conclusion

The view from the data mountain depends on your perspective. Whether you view the growing volume of data as a source of improved efficiency, insight and productivity in business, or a source of burden and pressure in litigation, it seems clear that the trend toward ever-increasing creation and use of electronic records is unstoppable. Electronic records management, therefore, must be a top priority for every major business.