ELECTRONIC DISCOVERY: A REFRESHER

By:
Stephen Tucker
Garth W. Aubert

The essential ubiquity of computers in the workplace and the proliferation of electronic communications has had a profound impact on the manner in which discovery is conducted during litigation. Though litigants often avoided the issue in the recent past by producing paper versions of electronic documents, in many instances, this approach no longer suffices as savvy plaintiff and defense attorneys alike have come to recognize that electronic documents, in their native form, provide a treasure trove of information. This has inevitably resulted from recognition of the statistics. One study revealed that in 1999, 93% of business documents were generated electronically, 70% of which were never printed. Employees were expected to exchange nearly three billion Emails in 2000 and the volume has grown exponentially since then.

Stories of Bill Gates' Email indiscretions are legendary. More common (and pertinent in this context) are the stories of other professionals making damaging admissions while engaged in casual "conversation" via the company Email system. In one instance, an engineer wrote to another, "The [expletive] has hit the fan regarding [product X]." The engineer continued to describe the problems with the product, as it happened, just before it was recalled from the market and numerous lawsuits were filed.

Of course, Bill Gates' problems with Email are nothing new. However, litigants and the courts have been compelled to confront this emerging aspect of the law with increased frequency and there have been a number of significant developments in this area. This article will address some of the recent developments in case law regarding the obligation to produce electronic files; cost sharing in the context of electronic search and retrieval; maintenance, destruction and spoliation of electronic evidence; and advice on how best to prepare to respond to the inevitable request for electronic discovery in the context of litigation.

Electronic Files are Discoverable

Witnesses are often surprised to learn that an opposing attorney is entitled not only to discover the content of the paper in their file cabinet, but also the electronic files on their computers and other electronic devices. The Federal Rules of Civil Procedure have explicitly contemplated the discovery of "documents" including "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form" since 1970. The definition of a "writing" in the California Evidence Code was amended in 2002 to specifically include Email, "and any record thereby created, regardless of the manner in which the record has been stored."[1] One court has stated, "A discovery request aimed at the production of

[1] California Evidence Code § 250.

records retained in some electronic form is no different, in principle, from a request for documents contained in an office file cabinet."[2]

In other words, computers, and the electronic documents stored thereon, are fair game. Courts have held that parties not only have a duty to thoroughly investigate the existence of potentially relevant documents, including those in electronic form, but also to disclose if documents are available in electronic form.[3] In one case, a defendant was ordered to provide a written explanation of the steps taken to locate responsive Email messages.[4] Failure to timely produce electronic information can result in Court imposed sanctions against a party.[5] Courts have also routinely held that the production of printed files does not relieve the producing party of the obligation, upon request, to produce electronic versions of the same information as well.[6] In one case, a defendant was required to create a report of Internet sites accessed with company computers[7] and, in another; a party was given access to the opposition's computers to perform key word searches.[8]

Electronic documents can take many forms. These include: Email, word processing files, data compilations, internet related material, and images. They can generally be categorized as active (currently being used), archival (available for active use), backup (stored as a record), and residual (not intended to be retrieved, but retrievable). These documents can be found in, among other locations, office computers, networked computers, home computers, Email servers, laptops, PDA's, removable disk storage, backup tapes, and off site storage facilities.

Emails are particularly useful to plaintiff's attorneys for a number of reasons. First, they tend to contain present sense impressions that are often tentative, unguarded and casual. Second, they are viewed as ephemeral and private by the sender – neither of which is generally true. Third, writers often vent, brag, flame and joke and the context is later often difficult to reconstruct. And fourth, Emails are useful for showing who was in the loop regarding a particular issue.

One of the richest sources of information that tends to show intent is residual data. This is information that the creator believed to be deleted. Most users do not know that when a document is deleted via keystroke, it usually remains on some storage medium.

---

2 *Linnen v. A.H. Robins Co., Inc.*, 1999 Mass. Super. LEXIS 240, at *16 (Mass. Super. Ct. 1999).

3 *See, e.g., GTFM, Inc. v. Wal-Mart Stores*, 2000 U.S. Dist. LEXIS 16244 (S.D.N.Y. Nov. 8, 2000); *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437 (D.N.J. 2002).

4 *See, In re Livent, Inc. Noteholders Sec. Litig.*, 2002 U.S. Dist. LEXIS 26446 (S.D.N.Y. Dec. 31, 2002).

5 *See, e.g., Metropolitan Opera Ass'n v. Local 100, Hotel Empl. & Rest. Empl. Int'l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003); *Residential Funding Corp. v. DeGeorge Fin. Corp*, 306 F.3d 99 (2nd Cir. 2002).

6 *See, e.g., Zhou v. Pittsburgh State University*, 2003 U.S. Dist. LEXIS 6398 (D.Kan. Feb. 5, 2003); *Cobell v. Norton*, 206 F.R.D. 27 (D.D.C. 2002); *Storch v. IPCO Safety Prods.*, 1997 U.S. Dist. LEXIS 10118 (E.D. Pa. July 15, 1997); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 U.S. Dist. LEXIS 16355 (S.D.N.Y. Nov. 3, 1995).

7 *See, Giardina v. Lockheed Martin Corp.*, 2003 U.S. Dist. LEXIS 4160 (E.D.La. Feb. 26, 2003).

8 *See, Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998).

All that happens when the delete command is executed is that a notation is made on a computer's storage medium. This notation indicates that the area where the document resides is now available for storing future documents - if the space is needed. If the space is not needed (and it often is not with today's large hard disks) a document, or its fragmentary pieces, can continue to exist for years. Other locations of residual data include temporary procedure related files created by Windows to ease computer usability, cache files (which speed up computer operation by making frequently used information readily available), meta data (discussed below), and the user recycle bin (for undeletion of material later needed by the user).

Meta data, sometimes referred to as embedded data, is simply data about data. Meta data is the unseen information about an electronic document, such as when and how it was created, modified and transmitted, and by whom. Meta data also provides the links between Email messages and the attachments, revealing information about which version of a document was attached and where it was stored. Meta data even reveals information about who received a message and when it was actually opened. It is easy to imagine any number of circumstances in which this type of information could be highly relevant to a case. But when a document is printed and produced in paper form, all of this information is lost since, by definition, none of it actually appears on the face of the document. For this reason, parties are requesting, and obtaining with the assistance of the Court when necessary, discovery in electronic form.

The production of documents in electronic format offers another distinct advantage: searchability. When documents are produced in paper form, they cannot be searched unless a vendor is employed to "code" the documents, the time consuming and expensive task of extracting information such as names and dates from a document and inputting them into a searchable database. Electronic documents, together with the corresponding meta data, not only reveal more information about a document, but also permit the parties to execute automated searches for relevant persons, dates or issues.

The potential relevance of residual data and meta data in litigation has created a whole new type of forensic expert. These experts "mine" for data by first creating a mirror image of a particular storage medium. An expert of this type is subject to *Daubert/Kumho* safeguards in terms of the methodology used by the expert to retrieve the data. Great care must be taken in this area of expertise to not destroy residual data in the process of retrieving it. The situation is not unlike an archeological dig – amateurs can spoil the dig if not using the utmost care in uncovering the object of exploration.

It is not uncommon for courts to order a defendant to make its computers, and in particular the hard drives, available for inspection by mutually agreed or court appointed forensic experts.[9] One of the leading cases on electronic discovery of hard drives is *Playboy v. Welles*. There, the court approved a discovery plan wherein a court appointed expert created a mirror image of a hard drive in an effort to uncover evidence concerning

---

[9] *See, e.g., Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002); *Superior Consultant Co. v. Bailey*, 2000 U.S. Dist. LEXIS 13051 (E.D. Mich. Aug. 22, 2000); *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D. Cal. 1999)

the use of the bunny icon by a former playmate on a web page unrelated to the well known magazine.

Allocation of Costs

However, the benefits of electronic discovery do not come without costs, both financial and in terms of the burdens it can impose upon a responding party. Electronic data is most frequently maintained not only on desktop computers, but also on networks and in archives. In many instances, archives are maintained in an outdated format, no longer compatible with systems currently in use. Forensic experts can usually retrieve this information – at a cost, which can easily run into six figures.

Traditionally, the presumption has generally been that the responding party must bear the expense of complying with the discovery requests. However, in this context, some courts have chosen to apply a balancing test in extraordinary cases where the cost of electronic discovery will impose an undue burden or expense upon the responding party. One recent, leading case identified the following factors to be considered: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.[10] At least one other court has applied a "marginal utility test" which considers not only cost, but also the likelihood that the requested material will contain relevant information.[11]

Destruction vs. Spoliation

The fluid nature of electronic documents, resulting from routine access to or deletion of electronic files on the computer, raises important questions regarding the obligation to preserve evidence which may be relevant to litigation.

It is clear that the obligation to preserve evidence arises no later than the time a defendant is served with a complaint.[12] However, courts have held that the obligation may arise substantially earlier than that, such as when lawyers and experts examined a vehicle in anticipation of litigation.[13] Another case determined that the duty to preserve evidence arose when the party "knew or should have known that it was reasonably foreseeable that the [evidence] would be relevant to future litigation."[14] Importantly, destruction of documents pursuant to a document retention policy does not absolve a party of responsibility, or protect it from sanctions, if the party took no steps to preserve

---

10 *Zublake v. UBS Warburg, LLC*, 2003 U.S. Dist. LEXIS 7939, at *21 (S.D.N.Y. May 13, 2003).

11 *See, McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001).

12 *See, e.g., Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F.Supp. 1443 (C.D.Cal. 1984).

13 *See, Silvestri v. General Motors Corp.*, 271 F.3d 583 (4th Cir. 2001).

14 *Barsoum v. NYC Housing Auth.*, 202 F.R.D. 396, 400 (S.D.N.Y. 2001).

evidence that it knew, or should have known, was subject to disclosure in the litigation.[15] These principles have been applied to the preservation of corporate Email communications.[16]

Indeed, courts have historically imposed monetary sanctions against parties for failing to maintain electronic files in the face of litigation. In one extreme case, the court dismissed the plaintiff's case and ordered him to pay defendant's attorneys' fees and costs where the plaintiff had used a software deletion program, "Evidence Eliminator", to delete files from his computer the night before an inspection was scheduled by the defendants.[17]

Few cases are that egregious of course. However, courts will impose sanctions not only for the intentional destruction of evidence, but also for failing to prevent the destruction of evidence.[18] Courts will consider whether the destruction was accomplished in bad faith and whether the opposing party was substantially prejudiced as a result. *A valid, consistently enforced document retention policy is critical in this context*. In certain circumstances, courts have also ordered defendants to preserve all existing backups and to refrain from deleting files from servers and desktop computers.[19]

Documents destroyed prior to knowledge of potential litigation pursuant to a valid, consistently enforced document retention policy may protect a party from sanctions resulting from alleged spoliation if the document retention policy is reasonable. One court, faced with the inability of a fire arms manufacturer's inability to produce documents regarding customer complaints, articulated a three part standard for determining the reasonableness of a document retention policy: (1) the policy must be reasonable considering the facts and circumstances surrounding the relevant documents (i.e. a consideration of the type of documents); (2) whether lawsuits concerning the complaints or related complaints had been filed, as well as the frequency and magnitude of such complaints; and (3) whether the document retention policy was instituted in bad faith.[20] Even so, the court noted that a corporation may not blindly destroy documents pursuant to a retention policy and expect to be shielded from sanctions in all instances.[21]

Recommendations for ABC Assureds

Many of the pitfalls associated with electronic discovery can be avoided with advance planning and preparation. The following recommendations are considered essential for

---

15 *See, Trigon Insur. Co. v. United States*, 204 F.R.D. 277 (E.D.Va. 2001).

16 *See, Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998).

17 *See, Kucala Enterprises v. Auto Wax Co.*, 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. May 23, 2003).

18 *See, Liafail, Inc. v. Learning 2000, Inc.*, 2002 U.S. Dist. LEXIS 24803 (D. Del. Dec. 23, 2002); *Pennar Software Corp. v. Fortune 500 Sys.*, 2001 U.S. Dist. LEXIS 18432 (N.D. Cal. Oct. 25, 2001) (defendant sanctioned for altering relevant portion of web site while motion was pending); *Danis v. USN Communications*, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 20, 2000).

19 *See, e.g., Positive Software Solutions, Inc. v. New Century Mortg. Corp.*, 259 F.Supp.2d 561 (N.D. Tex. 2003); *Dodge, Warren & Peters Ins. Svcs., Inc. v. Riley*, 105 Cal.App.4th 1414 (2003).

20 *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988).

21 *Id*.

an organization to work towards a successful defense when it comes to electronic document control:

1. Top management support for electronic document control;
2. Maintenance of an accurate record of hardware and software used;
3. Documentation of all electronic interfaces with the outside world;
4. An electronic document retention policy which is created and enforced;
5. Insofar as individual litigated cases are concerned, creation of a litigation support team including the following representatives: legal counsel, HR personnel, product or service managers, and IS staff - to insure proper procedures are followed;
6. Ensure software set up which achieves full deletion of file fragments and meta data;
7. Emphasize the fact that laptops, home computers and PDA's are subject to discovery;
8. Assume every document you compose will eventually appear on the cover of the New York Times.

Electronic documents have created a rich source of evidence of intent. In order to safeguard your organization, it is essential that close attention be paid to following the above guidelines insofar as the written word is concerned. Mendes & Mount is available to assist ABC assureds with these issues.