# **Understanding Electronic Discovery in Civil Litigation**

by Steven Nudelman, Esq.

Watch those e-mails. Here are two from recent lawsuits. "Oops! I haven't beaten anyone so bad in a long time," and "Do we have a clear plan on what we want Apple to do to undermine Sun?" These examples of ordinary e-mail messages were offered as evidence in recent high profile trials. The first message was sent by a Los Angeles police officer about the 1991 Rodney King case. The second message was written by Bill Gates to Microsoft executives in 1997. Both messages illustrate why electronic evidence, such as e-mail, documents, and other computer-generated data, has been called the "smoking gun of the future."

One of the largest sources of electronic evidence is e-mail, which presents its own set of peculiar problems. People tend to treat e-mail

informally, often writing things they would otherwise neither write on paper nor say to another person in a conversation. In addition, e-mail can easily be forwarded to countless people (with or without the original sender's knowledge or approval). E-Mail can also be forged since most correspondents lack the ability to either encrypt and/or digitally sign messages. Finally, e-mail has a long shelf life, with backup copies of messages often available on computer networks and backup tapes. As one commentator stated, "In the litigation environment, it is often electronic mail that contains the most damning admissions." What can you do to avoid or minimize the possibility of staring down the barrel of a "smoking gun" e-mail? Understanding electronic evidence, particularly as it relates to the litigation discovery process, is an excellent starting point.

The rules of discovery in civil litigation allow a party to learn (with some limitations) all relevant facts about its case (from the perspective of adversaries, experts and others) so the party can fully prepare for trial. Parties learn these facts through discovery techniques such as depositions, interrogatories, requests for admissions, and demands for documents and other things. This last discovery device, "demands for documents and other things" is what often results in the type of "smoking gun" electronic evidence that is becoming more prevalent in today's world of commercial litigation.

In examining a party's obligations to produce electronic discovery, courts have focused on three broad concepts: location, volume and cost.

### The Rules

The Federal Rules of Civil Procedure and New Jersey Court Rules require a party to produce non-privileged documents, including writings, drawings, graphs, charts, photographs, phone records, and other "data compilations" from which information can be obtained and translated, if necessary, through electronic devices into reasonably usable form, that are relevant to the claim or defense of any party. As one court explained, "A discovery request aimed at the production of records retained in some electronic form is no different, in principle, from a request for documents contained in an office file cabinet. While the reality of the situation may require a different approach and more sophisticated equipment than a photocopier, there is nothing about the technological aspects involved which renders documents stored in an electronic media 'undiscoverable.'"

Courts have interpreted "documents" and "data compilations" broadly to include a host of electronic sources, such as e-mail messages and files, deleted e-mail, voice mail messages and files (including back-ups), program files, data files (from word processors, databases, spreadsheets, graphics programs), temporary files, embedded data (such as metatags and other hidden



messages that reveal when files are revised), chatroom transcripts, internet browser cache, web site information (stored in textual, graphical or audio format), web site log files, cookies, local hard drives, tape backups, deleted files, and even entire computers.

#### Costs

As one can imagine, the quantum of electronic discovery and the costs of locating, producing and duplicating this discovery can be staggering. Approximately 31 billion e-mail messages were sent each day in 2002. Experts project this number to rise to 60 billion by the year 2006. The costs involved in producing e-mail alone in discovery can be astronomical. As one court noted, "Too often, discovery is not

just about uncovering the truth, but also about how much of the truth the parties can afford to disinter." In a recent case, one party estimated that it would cost \$9,750,000.00 to retrieve all of its relevant e-mail messages on backup tapes. Who should pay for the cost of producing and/or retrieving such electronic discovery?

Under the discovery rules, there is a presumption that the responding party must bear the expense of complying with discovery demands. However, a court can limit discovery if the burden or expense of the proposed discovery outweighs its likely benefit. If the burden of a request outweighs the likely benefit, courts generally shift all or part of the cost of production to the discovering party. Most courts have applied cost shifting automatically whenever electronic evidence is involved. However, in a recent employment discrimination case involving UBS Warburg LLC, a New York federal court held that cost shifting should not be automatic; rather, it should depend "primarily on whether [the requested discovery] is kept in an accessible or inaccessible format." The Court identified the following possible formats, from most accessible to least: hard drives, optical disks, off-site backup tapes and deleted/damaged files:

Prior to the *UBS Warburg* case, most courts applied the following eight-factor balancing test to determine how to allocate the costs of electronic discovery: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with the production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party.

Although the Court in *UBS Warburg* described the above test as the "gold standard," it modified it slightly by adding two additional factors: the amount in controversy and the importance of the issues at stake in the litigation. The Court also noted that the fourth factor is "typically unimportant." Applying these factors in a subsequent decision, the Court shifted the \$166,000 cost of restoring and searching 77 backup tapes to the requesting party. However, the Court required the producing party to absorb the \$108,000 cost of producing e-mails restored from backup tapes.

## Penalties

If the parties cannot agree on a discovery protocol, including cost allocation and procedures, a court will apply the above factors to establish the parameters for electronic discovery. It will then be up to the parties to comply with the court's direction or face the consequences. These consequences range from a stern

(Electronic Discovery, continued from page 5) warning or second chance (e.g., produce the discovery by a particular date or face a penalty), to a preliminary injunction (e.g., enjoining a party from destroying electronic discovery), to monetary sanctions (e.g., requiring a party to pay a fine and/or their adversary's attorneys' fees), to an adverse inference jury instruction (e.g., informing the jury that it may infer that a party destroyed unfavorable electronic evidence), to preclusion of testimony, to the ultimate sanction — judgment as to liability. This last sanction, administered by a New York federal judge in a recent fifty-page decision, was the culmination of egregious discovery practices by lawyers and clients who repeatedly lied in open court, failed to search for and produce documents and blatantly destroyed evidence, "all to the ultimate prejudice of the truth-seeking process."

## Be Proactive

Rather than worry about these consequences, it is best for clients to take a pro-active approach. As attorneys, we can help you understand the nature of e-mail, including the legal consequences resulting from its misuse. Specifically, we can help you develop an appropriate workplace e-mail and internet use policy for your employees. We can also assist you by preparing a formal electronic document retention policy. We can help you identify potential sources of electronic discovery in your workplace and address the legal and cost-shifting issues regarding its production in litigation. By taking the above pro-active measures, you will be able minimize the possibility of staring down the barrel of a "smoking gun" in electronic discovery.

Steven Nudelman is an associate at the law firm of Greenbaum, Rowe, Smith, Ravin, Davis & Himmel LLP with offices in Woodbridge and Roseland, New Jersey. He is a member of the firm's Litigation Department and Construction Practice Group. He can be reached at (732) 549-5600, ext. 5662 or by e-mail at snudelman@greenbaumlaw.com. Reprinted with permission. ©2003 Greenbaum, Rowe, Smith, Ravin, Davis & Himmel LLP.