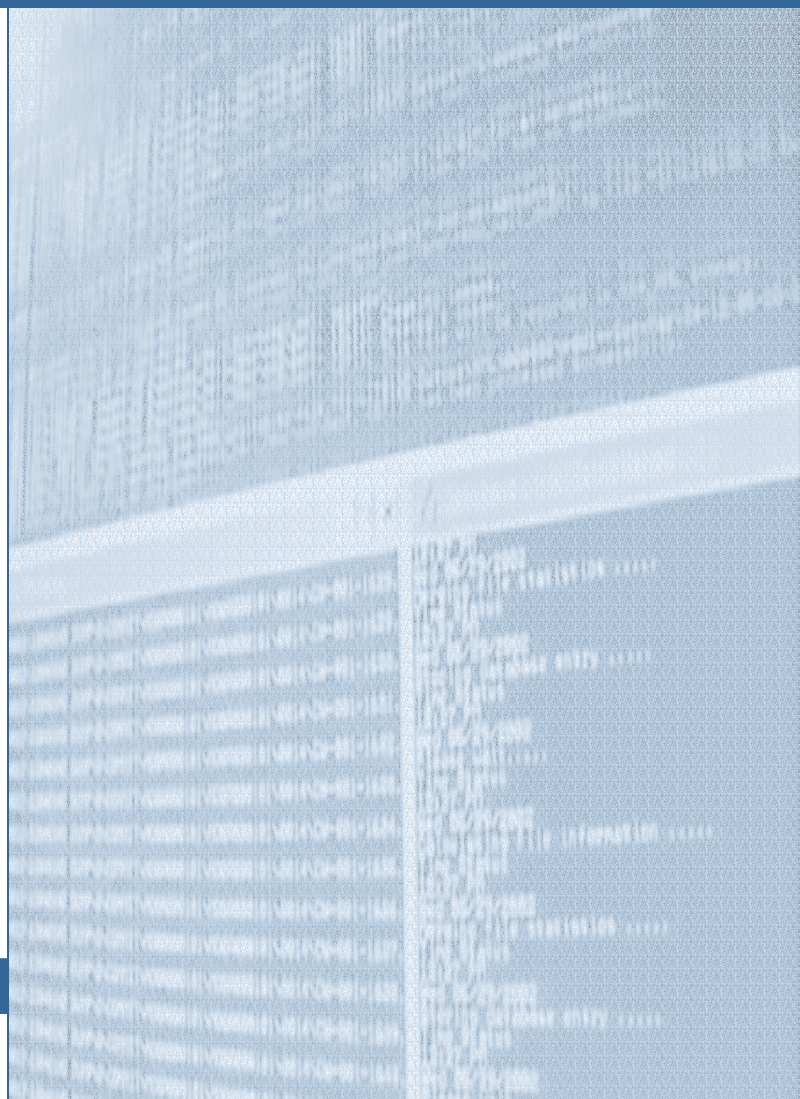


THE *NEW* NEW EVIDENCE

BY PAUL NEALE, JR.



170 Earle Avenue
Lynbrook, New York 11563
tel: 516.823.4000 • fax: 516.823.4400

www.DOAR.com

In the year 2000, office workers in the U.S. exchanged approximately 7 trillion e-mail messages, according to an article in *Wired* magazine. Just about everyone uses e-mail now – from humble cubicles to executive suites, from commuters in rush-hour traffic to business travelers 35,000 feet in the air, and in every corner of the marketplace. And they're all slowly waking up to the realization that nothing they say in their e-mail is private, anything they say in their e-mail is potentially admissible as evidence, and deleting their e-mail won't necessarily destroy it.

The smoking gun of the future consists not of fingerprints and gunpowder residue on metal, but of ones and zeroes.

As corporations rely more and more on computer systems to communicate and manage information, electronic records and files have played a greater role -- sometimes a central role -- in litigation. In addition to e-mail, those records include correspondence, memos, reports, and other plain text files; databases and spreadsheets; digital art and photos; medical records, tax returns, Internet browsing patterns, inventory, proprietary mailing lists, and any other data that is created or stored on a computer or network of computers.

E-mail, however, because of its burgeoning use and the illusion of confidentiality, is perhaps the most damaging sort of electronic evidence of the new millennium. Microsoft Corp., probably one of the most sophisticated e-mail users in the world, has been done in by it more than once:

- As early as 1995, in *Strauss v. Microsoft*, an employee who sued for sexual discrimination was allowed by a federal court to use e-mails from her supervisor to other employees that contained jokes, as evidence of a discriminatory attitude.
- In *Caldera v. Microsoft* (1999), a federal district court ruled that a series of e-mails between staffers provided direct evidence that the company was actively trying to put a competitor out of business.
- The *U.S. v. Microsoft* antitrust trial demonstrated how devastating e-mail evidence could be, when the government introduced a series of e-mails that demonstrated anti-competitive practices, such as improperly using its monopolistic Windows operating system to achieve dominance in the Internet browser market. One internal e-mail message from a Microsoft staffer said: "It seems clear that it will be very hard to increase browser share on the merits of IE4 [Internet Explorer 4.0] alone. It will be more important to leverage OS [operating system] asset to make people use IE instead of Navigator [Netscape's competing software]."

Disparagement and profanity

E-mail evidence can be particularly devastating for two reasons. First, it is an informal medium of communication; people say things in e-mail that they wouldn't dream of expressing in print, on the phone, or in a face-to-face conversations. They tend to be less inhibited about making derogatory or disparaging comments, they tend to use more

profanity, and -- because it is a nearly instantaneous medium -- they often hit the "send" button without taking time to consider whether they've revealed more information than they should.

The second factor that makes e-mail evidence so devastating is that many users still have the misapprehension that e-mail is private and secure, as long as it doesn't leave the company's internal communications network -- especially if it gets deleted without ever being printed out. That assumption is dangerous both technically and legally. New technology exists that can recover and restore deleted electronic files from computer hard drives, diskettes, servers, handheld devices, cell phones, voice mail tapes, backup media, etc. If an e-mail or document is sent from one company to another electronically, the audit trail extends to the recipient's communication network as well as third-party service providers and various outposts and ports of call throughout the Internet.

Mining and tracking e-evidence

In fact, electronic audit trails can reveal much more than their paper counterparts. An electronic file leaves its own chronology of creation, modification, and transmission. It may contain a history of drafts, rewrites, edits, and comments between collaborators.

Sophisticated drive imaging, data mining, and tracking software makes all that possible. Experts in the field can use it to retrieve, convert, analyze, search, catalog, and manage electronic files during the discovery phase of litigation, as well as prepare the evidence for presentation at trial.

This software is derived from programs that the U.S. government developed and once considered top-secret. Programmers at discovery services firms have further developed customized applications specifically to process electronic evidence cost-effectively. For example, this software can search through millions of electronic documents and e-mails to retrieve only those files that contain certain key words or text, narrow the search to specific time periods, filter out unrelated types of files such as program and system files, and "de-duplicate" redundant files. After the evidence is collected on a central database, the software keeps track of who reviews the files, on what dates (down to the exact minute), and can even attach codes, annotations and Bates-numbered tags.

Managing digital discovery

Without the technology to narrow the search and organize the output, digital discovery can become massively prohibitive. In a recent case in which a Fortune 500 company was being sued by a former employee for wrongful termination, the company was ordered to turn over all e-mail that mentioned the former employee's name. The company did not have a policy for purging old e-mail files, and so it had to search 20,000 backup tapes for e-mail files containing the person's name. The estimated cost of searching the tapes was \$20,000 -- that's not counting the potential cost of producing e-mail files for the plaintiff.

Costs can be compounded when the hardware and software used to create a series of files are obsolete or outdated -- and these days, it takes only a few years for computer components to become outdated. Sometimes it is necessary to restore the old system

before you can search or produce old files. A lawyer who requests old files may be able to shift such costs to the producing party, but there is no guarantee of that.

Since most law firms do not have the expertise on staff to apply the technology, electronic evidence service providers (EESP) are available to handle the job. When choosing an EESP, make sure the project managers who are assigned to your case are familiar with the particular type of litigation and discovery procedures that are involved, so they can help you analyze discovery needs. For best results, choose a firm that delivers integrated litigation support services, so that they can coordinate digital discovery with all other evidence production, organization, and presentation.

Also make sure the EESP has the experience and capabilities necessary to help you accomplish the following:

- Develop and implement a strategic plan for cost-effectively managing the digital discovery process (see below)
- Collect and handle evidence carefully to insure its authenticity and accuracy -- and be prepared to testify about it
- Preserve the chain of custody to insure admissibility.
- Work with the legal team in a professional manner, and be able to explain the technology in plain English
- Adhere to the highest legal and professional standards

Strategic Planning

More lawyers routinely request electronic evidence, especially e-mail, early in their discovery efforts. It's important to take a long-term view of the digital discovery process to ensure that the evidence is (and remains) authentic and admissible. Strategic planning typically involves the following steps:

- Send a preservation-of-evidence letter and, if necessary, obtain a protective order to preserve electronic files. An electronic file can be revised, moved, or corrupted any time work is done on a computer, whether the work involves that particular file or not.
- Notify the other party as early as possible that you intend to request electronic records, and specify the kinds of information and where the files may be located (whether on an individual's hard drive, the organization's network, backup media, an old computer stored in the warehouse basement, an executive's home laptop, etc.).
- Refine your requests by specifying, for example, key words, particular users, or relevant time periods to search for. In a large database, you may request only certain fields that relate to your case. Narrowing down the kinds of information you ask for accomplishes two things. First, it forces the other party to organize the information and limits the magnitude of materials that you will have to review. Second, it ensures that your request will not be denied because it is considered too broad.
- Request information about the party's information technology (IT) structure. How many offices does the company have, how many servers does it use, what application software does the company use, how often do they back up their data and in what

format? How likely is it that multiple copies of the files you need reside across the entire network? Also, ask all company employees whom you depose about their computer usage, to get a picture of how they create, revise, save, store, and purge files.

- When you receive electronic evidence for review, first write-protect and virus-check it to maintain its integrity (and avoid contaminating your system). If you detect a virus, do not try to clean it up -- contact the party that produced it. Make working copies of all evidence to avoid altering the originals.
- Work with your EESP to review the electronic files in the most cost-effective way, avoiding duplication and irrelevancy. As you perform your review, classify and code the files you might want to use as evidence. Your EESP should help you produce a coding manual, based on the key legal and logistic issues in the case.

As electronic evidence processing becomes more routine in litigation, law firms will undoubtedly develop greater in-house expertise for retrieving, analyzing, and managing electronic evidence. Meanwhile, be very selective about the outside experts you hire to help you with the process.

###