E-mail and Other Electronic Data: Treasure Troves of Evidence

Larry Johnson
Director of Electronic Discovery Services
Fios
and Joan Fledman
Computer Forensics Inc.

Many of us spend more time each day in front of our monitors than we do with family members. It thus may come as a surprise to you that this efficient machine, quietly doing your bidding every working day, never complaining about the hour or day, has the potential of betraying you, your friends, and your co-workers. Indeed, your faithful machine can destroy the company you work for.

How so?

Because most computer users tend to keep everything they have ever created on their hard drives. Unlike paper clutter, which at some point demands to be archived or thrown away, hard drives with gigabytes of space simply fill up invisibly. Thus the modern world is awash in trillions of magnetically stored bytes of what often is so much useless electronic junk. The "junk", however, could someday become important evidence in a lawsuit involving you or your employer.

Also, most computer users forget the equipment they're using at work is not theirs and can be accessed by others; therefore whatever resides on their hard disks is not private, though they may think otherwise.

Think about it: what if I could just take your computer from you right now and copy and print out whatever I wanted, or post it for the world to see on the Internet? How would you like that?

I know I wouldn't like it. And yet that very thing occurs daily, and recently to none other than the Grand Wizard of computer software, Bill Gates. In the anti-trust lawsuit currently underway against Microsoft brought by the U.S. Justice Department, a number of Bill's e-mails are being used against him as evidence of alleged illegal activity. And though these e-mails were imbedded in what must have been billions of bytes on his hard disk and within Microsoft's network, they were easily found with text-search software that lawyers use as bloodhounds to sniff out Mr. Gates' evidence.

Lawyers world-wide are coming to the awareness that pre-trial discovery tools can be used to obtain electronic information.

E-mail: the Mother Lode

Not only are electronic data easily searched and cataloged, each and every file kept on computers is stamped with a date and time. E-mail and programs generating faxes from computers keep logs of dates of transmission and receipt. It is therefore a simple, routine task to match computer activity chronologically to significant dates in a lawsuit: who knew what, where and when. Cases are often made or broken with such evidence.

Electronic evidence may often by the *only* evidence a litigator will find in support of his or her case. It has been estimated that fully a third of all documents kept in the ordinary course of business in the U.S. exist only in electronic form -- there never was a need for a hard copy of the document. This is particularly true of e-mail, where software has made it extremely easy to reply to a sender with a sentence or two, then press a key to have the response sent back, not only to the sender, but potentially to a whole "broadcast" list of recipients.

An Australian lawyer has written that by now over 90% of Australian businesses use e-mail (David Gillespie, "E-Mail - The Clayton's Deletion," published by LawNet online at http://www.lawnet.com.au/). In the context of litigation, getting that information from one computer to another for analysis, without disrupting or corrupting the original source of the electronic data, calls for some legal sophistication and understanding of computers. Lawyers and judges need to be educated that transfer of electronic data in a secure manner, with due consideration for the protection of the confidentiality of that information, can be a simple (although sometimes expensive) task. The cost comes in doing the job professionally, with sufficient equipment and personnel. As consultants become more and more expert in dealing with electronic data, new opportunities arise:

> "The business world is desperate for consulting help. Running leaner than ever, most organizations lack the technical, strategic and project management skills to handle the benumbing rate of technological and market change. Happy to oblige, the consulting industry is splitting at its seams to accommodate the demand. Big consulting firms are inhaling new employees, gulping up smaller firms and merging with peers. Small firms, or 'boutiques,' are sprouting up everywhere." (Jennifer Bresnahan, "The Latest in Suits - CONSULTING TRENDS - Enterprise, Enterprise Magazine October 15, 1998, www.cio.com/archive/enterprise/101598_trends.html)

Still, Australians are just now gearing up for mining electronic data in ways long extant in America: "In the United States, specialist firms practice electronic sleuthing with the principal aim being to find that 'smoking gun' in old E-Mail. It won't be long before the trend develops in Australia." (Gillespie, ibid.)

With respect to e-mail and other electronic data, regardless of the issues and interests at sake, the following points should be kept in mind:

1. "Deleted" files are seldom that.

More often than not, when you "delete" a file you do not destroy its contents on the storage medium. Computers maintain a FAT or "file allocation table" which is like a table of contents, where each "live" file is kept intact and kept from being overwritten by newly generated files. When you "delete" a file only its name is removed from the FAT, but otherwise for a period of time -- which can be a long time -- part or all of the file's content remains reconstructable. That is why there is a DOS command called UNDELETE which can restore a file if it has been only recently deleted. And even if over time the bytes of information that once were part of a "live" file are overwritten, other portions of it may be strewn about your hard disk at various locations, capable of total or partial reconstruction. Finding and "undeleting" deleted files can provide a rich source of information, particularly if the files were deleted at about the time a party was sued and it tried to hide or destroy sensitive information.

There is software available to completely expunge not only a file's name in the FAT but all of its associated electronic data as well. This tool can help reduce the retention of files, but if -- as is common -- the file exists in other locations, such as on archives, backups or on other computers, the tool is of little value.

2. E-mail policies, if in place and enforced, can reduce the size of the "gold mine."

It is an almost impossible task to control the flow and proliferation of e-mail. Still, an employer can and should implement and post prominently a policy that prohibits private use of e-mail, and to remind employees that all e-mails are like postcards, available for all to read, including the employer. From time to time, employee e-mail should be monitored for compliance. Old e-mail should be routinely deleted and expunged.

Programs, such as MIME*sweeper* by Content Technologies, Inc. (info@mimesweeper.com), can routinely scan all employee e-mail for offensive or illegal e-mail content.

While such policies and tools may seem obtrusive, there is a growing body of case law in the U.S. and elsewhere that can come to haunt employers if they do anything to create -- or acquiesce in -- the impression that an employee has a right of privacy to his or her e-mail or other electronic files.

That notwithstanding, however, laws vary from country to country concerning individual privacy rights to computer data, and they need to be reviewed before e-mail policies can be put into effect. Germany and the U.K. have been particularly sensitive to privacy rights in the context of computer data.

3. Passwords and encryption.

Passwords usually apply only to the user's entry into a computer. Once the computer is up and running, the files created are not ordinarily password-protected. A court can order a person to open up his or her computer, just as it could order a garage or

warehouse unlocked. Further, in many instances it is not that difficult to bypass passwords through software that can "hack" a system.

Encryption software and hardware exist to make files less easily accessible, but again a user can be compelled by court order to decrypt files so that they can be read and used in pre-trial discovery.

Thus, businesses should know that security measures to keep out electronic trespassers do not afford any shield in the context of litigation.

A good resource for helping businesses to limit their liability exposure is Michael R. Overly's *E-policy - How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets*, published by the American Management Association, 1601 Broadway, New York, NY 10019, 1999, ISBN 0-8144-7996-0, www.amanet.org.

Meanwhile, keep in mind that whatever you tell the hairdresser, the publican -- or your computer -- can come back to haunt you!

The topic of Auditing Electronic Evidence is explored in further detail in the February issue of the IT Chapter newsletter. Members wishing to obtain a copy of the newsletter can do so by contacting IT_Chapter@icaa.org.au or on 1800 to subscribe

# # #