E-Mail E-Merging E-Normously in Litigation

By: Kevin Schlosser

The Nassau Lawyer, April 2021

We read the headlines time and again about devastating, "smoking-gun" e-mail uncovered in legal actions. After facing days of grueling depositions at the hands of David Boies, Microsoft's Bill Gates lamented at a news conference: "I had expected Mr. Boies to ask me about competition in the software industry, but he didn't do that." Instead, "he put pieces of paper in front of me and asked about words from e-mails that were three years old."1 As we now know, those "e-mails from three years ago" had a dramatic impact upon the Government's antitrust case against Microsoft, leading a reporter to comment on the front page of *The New York Times:* "Never mind monopoly power in the marketplace; the real lesson corporate America is taking away from the Microsoft antitrust trial is that old e-mail can be a minefield of legal liability, not to mention a source of public embarrassment."2

Notwithstanding Microsoft's own blunders, it too has taken advantage of an adversary's ill-advised e-mail. Bristol Technology, a small company attempting to survive against Microsoft's dominance, found out the hard way that e-mail can derail a case with so much as one sentence. Even though Bristol reportedly presented overwhelming evidence of Microsoft's monopolization of the market, a jury rejected its case because of a critical e-mail sent by one of Bristol's directors coining the company's litigation strategy as the "We sue Microsoft for money business plan."3 Indeed, e-mail has haunted even the top chief executive in the nation, who had to endure massive publicity about notorious e-mails from Monica Lewinsky to Linda Tripp detailing her affair with the President; in one such e-mail Lewinsky complains that the "Big Creep didn't even try to call me on [Valentine's]-Day."

Industry experts estimate that e-mail traffic will grow from 2.1 billion – that's right, billion–messages a day in 1998 to 7.9 billion in 2002.4 In North America alone, a study has found that on average there are currently 3.4 billion business e-mail messages and 2.7 billion personal messages sent each day.5 These staggering statistics and horror stories present a daunting task for owners of businesses of all shapes and sizes – and especially for the lawyers who are engaged to protect them in current or anticipated litigation. E-mail is indeed one of richest sources of discovery and trial evidence because it is uniquely suited for the most candid, unguarded, and oft-times unflattering communications. It is often shot out of the computer without a second of reflection and with an apparent mentality that it somehow has a different impact than a formal company memorandum or letter. As the above war stories show, although e-mail may feel like nothing more than water cooler banter, it

takes on a more formal recorded form of medium, with its memo-like "To:, From:, Time:, Re:" format. As such, e-mail is emerging as one of the most important aspects of modern litigation.

Obviously, businesses and litigators must devise strategies to mitigate the potential disastrous effects of uninhibited e-mail. One answer that is clearly not the cure is simply to advise clients to adopt a policy that requires employees to delete their e-mail within a certain time after it is sent. To begin with, e-mail once sent out takes on a life of its own. It can easily be copied in whole or in part, "forwarded" to others, stored in other computers and so on. There is simply no fail-safe way to control distribution of e-mail once sent. Thus, simply deleting your own e-mail does not control the content of the e-mail any more than destroying letters or other hard documents that have been sent. It is also dangerous to think that internal e-mail can be restricted to in-house distribution.

In addition, it is now common knowledge that the "delete" key most certainly does not mean the e-mail has been eradicated forever. E-mail is often backed-up automatically on individual computer hard drives and/or on network servers. The delete key merely sends it to a marked file for overwriting if disk space is needed – which is not terribly often considering the larger storage capacity of computers today. Even more frightening, once a "deleted" e-mail is retrieved, a wealth of identifying "history" can frequently be uncovered, such as who created it, when, on what computer and changes made.6 An emerging field of computer consultants has been tapped to uncover and decipher "deleted" e-mail.7

To deal with the problem of uncontrolled e-mail, high-tech entrepreneurs have entered the fray of the cat and mouse game of hiding and finding e-mail. Software designed to reduce the exposure of electronic discovery is spreading fast, with mixed reviews. For example, "self-deleting" e-mail programs are available to control the manner in which e-mail is maintained. Some critics note, however, that these "'self-deleting' e-mail programs share a fatal technical flaw: they don't actually delete the messages at all. They encrypt the message, and perhaps avoid the network server in sending the message, but the messages still exist on the senders', recipients', and perhaps others' computers. … A skilled computer forensics technician will be able to recover such messages using no more sophisticated methods than are used to recover other 'deleted' files."8 These critics also aptly note that once these purportedly deleted files are found, with the identifying information, they can be even more powerful in the hands of opposing counsel, "as the sender and recipient will have to explain, in a deposition or under court order, what the message was and why it needed to be handled in this fashion."9

Another drawback of playing this "hide the e-mail" game is that it could cost your client the tremendous expense of retrieving buried e-mail now requested to be produced in discovery. Some courts have imposed the cost of finding and assembling the e-mail on the party who has been requested to produce it – rather than the party requesting the discovery.10 Moreover, under the spoliation doctrine, adverse inferences can be imposed against companies that allow e-mail to be eradicated or hidden during pending cases or even in anticipation of likely litigation

.

Nor is simply advising clients to avoid using any e-mail the answer. Whether we want to accept it or not, as the above statistics make clear, e-mail is a well-entrenched form of communication in individual and business life. It is here to stay. Any business owner who believes that it can bar the use of any e-mail is simply ignoring the hard reality. Indeed, even company policies banning the use of e-mail for any personal use would be more likely to be breached than followed. Does anyone expect office workers to refrain from ever communicating by e-mail with their family or friends during office hours? Does anyone think that the office telephone is never used to call home?

For business owners and their lawyers it is more important to implement realistic policies that govern e-mail use and remind employees of the potentially devastating impact and effect that their written words could have in pending or future as yet unknown litigation. An excellent new publication, Digital Discovery & e-Evidence,11 provides a wealth of information and suggestions for dealing with e-mail and implementing protective procedures. It is a matter of being sensitized to these important issues and vigilant in continuing to educate employees to avoid the ill-conceived, sensitive or otherwise negative communication. Although few e-mails would ever pass this test, some have suggested that if you wouldn't want it plastered on the front page of The New York Times, you shouldn't send it.

At a minimum, e-mail policies should address (1) the company's right to monitor e-mail and consent of employees; (2) what type of communication is prohibited, limited or otherwise restricted; (3) an effective notice to everyone in the organization to protect the company from potential liability and exposure in litigation; and (4) an e-mail retention policy.12 Once in litigation, counsel must immediately get full and frank information from the client regarding its e-mail policies, advise the client of its obligation to preserve evidence and determine the extent of potential e-mail discovery and what damaging evidence might be lurking out there. Although there is probably nothing that can eliminate the risk of damaging e-mail, it is critical for the company and counsel to be sensitive to this important emerging issue both before and during litigation.

1. J. Heilemann, Pride Before the Fall: The Trials of Bill Gates and the End of the Microsoft Era, (HarperCollins Publishing 2001), p.159.

2. A. Harmon, "Corporate Delete Keys Busy as E-mail Turns Up in Court," The New York Times, Nov. 11, 1998, p.1.

3. The case is commented upon in K. Liebman & R. Kahnke, "It's 2 AM: Do You Know Where Your E-Mail Is?" http://www.faegre.com/articles/article_ 328.asp

4. Source: IDC; see http://www.IDC.com

5. S. McGrane, "A Little E-mail (Or a Lot of It) Eases the Workday," The New York Times, March 8, 2001, p. G8, citing an IDC study.

6. See T. Loomis, "Company E-Mail: Electronic Messages Can Become Damaging Evidence," NYLJ, Feb. 8, 2001.

7. Id.

8. K. Withers, "'Self-Deleting' E-mail: A Self Delusion?" http://www.kenwithers.com/articles/ email.html

9. Id.

10. See in re Prescription Drugs Antitrust Litigation, 1995 U.S. Dist. LEXIS 8281 (N.D. Ill. June 13, 1995).

11. Digital Discovery & e-Evidence, Vol. 1, No. 1, December 2000 (Pike & Fischer, Inc., a subsidiary of BNA, Publisher).

12. A helpful summary of some of the important considerations in drafting an e-mail policy can be found at http://www.asanet.org/newsletters/display/0, 1901,249,00.html, a site maintained by the American Society of Association Executives.