BENTLEY
UNIVERSITY

CENTER FOR BUSINESS ETHICS
175 Forest Street, Waltham
Massachusetts 02452-4705

CENTER
FOR
BUSINESS
ETHICS

VERIZON
VISITING PROFESSORSHIP
IN BUSINESS ETHICS AND
INFORMATION TECHNOLOGY

February 11, 2008

YOUR E-MAIL TRAIL: WHERE ETHICS MEETS FORENSICS

Jennifer M. Moore, JD, PhD
Partner, Epstein Becker & Green PC
New York, New York

Center for Business Ethics
Tel: 781.891.2981
Fax: 781.891.2988
E-mail: cbeinfo@bentley.edu
On the Web: *www.bentley.edu/cbe*

BENTLEY
UNIVERSITY

BENTLEY UNIVERSITY is a leader in business education. Centered on teaching and research in business and related professions, Bentley blends the breadth and technological strength of a university with the core values and student focus of a close-knit campus. Our undergraduate curriculum combines business study with a strong foundation in the arts and sciences. The McCallum Graduate School emphasizes the impact of technology on business practice, in offerings that include MBA and Master of Science programs, PhD programs in accountancy and in business, and custom executive education programs. Located minutes from Boston in Waltham, Massachusetts, the school enrolls approximately 4,000 full-time undergraduate, 250 adult part-time undergraduate, 1,400 graduate, and 30 doctoral students. Bentley is accredited by the New England Association of Schools and Colleges; AACSB International – The Association to Advance Collegiate Schools of Business; and the European Quality Improvement System (EQUIS), which benchmarks quality in management and business education.

The Center for Business Ethics at Bentley University is a nonprofit educational and consulting organization whose vision is a world in which all businesses contribute positively to society through their ethically sound and responsible operations. The center's mission is to provide leadership in the creation of organizational cultures that align effective business performance with ethical business conduct. It endeavors to do so by the application of expertise, research, education and a collaborative approach to disseminating best practices. With a vast network of practitioners and scholars and an extensive multimedia library, the center offers an international forum for benchmarking and research in business ethics.

Through educational programming such as the Verizon Visiting Professorship in Business Ethics and Information Technology, the center helps corporations and other organizations to strengthen their ethical culture.

The Verizon Visiting Professorship in Business Ethics and Information Technology epitomizes Bentley's commitment to advancing education and knowledge at the intersection of business and the liberal arts. For more than nine years, Verizon's generous support of this initiative has furthered the work of the Bentley Center for Business Ethics, continuing to engage students, faculty and the corporate community in an important dialogue about the ethical dimension of business—especially at the limits of technological advancement.

It was a pleasure to welcome Jennifer M. Moore, JD, PhD, as our tenth visiting professor in the Verizon series. Dr. Moore is a rare individual who brings together a wealth of experience both in academia and as a practicing lawyer. She has been steeped in the field of business ethics since its early days as a formal discipline. Throughout her career she has been keenly aware of the ethical problems associated with information technologies, and this is reflected in the fact that in 1981 she co-edited with me the book, *Ethics and the Management of Computer Technology: Proceedings of the Fourth National Conference on Business Ethics*. Obviously our human environment is pervaded by technology; what is less obvious is the extent to which over one short decade e-mail has become the standard mode of communication for so much of what we do. Yet, in many respects e-mail is unlike any other form of communications, and consequently, the ethical context is very distinctive. Dr. Moore's talk was a most illuminating reflection on some salient ethical issues that demand our attention.

The Center for Business Ethics will continue to strengthen the business ethics movement through programming such as the Verizon Visiting Professorship in Business Ethics and Information Technology. We are grateful to the Bentley community, to Verizon, to Dr. Moore, and to everyone connected with the center, whose support is indispensable in making these initiatives a success.

W. Michael Hoffman
Executive Director, Center for Business Ethics
and Hieken Professor of Business and Professional Ethics
Bentley University

VERIZON COMMUNICATIONS INC., headquartered in New York, is a leader in delivering broadband and other wireline and wireless communication innovations to mass market, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, serving nearly 69 million customers nationwide. Verizon's Wireline operations include Verizon Business, which delivers innovative and seamless business solutions to customers around the world, and Verizon Telecom, which brings customers the benefits of converged communications, information and entertainment services over the nation's most advanced fiber-optic network. A Dow 30 company, Verizon employs a diverse workforce of more than 228,600 and in 2007 generated consolidated operating revenues of $93.5 billion.

(From left) Gregory K. Miles, Director, Ethics and Business Conduct, Verizon Communications, Catherine M. Carney, Executive Director, Compliance, Verizon Telecom, Jennifer M. Moore, JD, PhD, Partner, Epstein Becker & Green PC, Michael Hoffman, founding Executive Director of the Center for Business Ethics and Hieken Professor of Business and Professional Ethics at Bentley University.

JENNIFER M. MOORE, JD, PhD, is partner of the New York City law firm Epstein Becker & Green, P.C., where she focuses on civil and criminal white collar matters, internal investigations, and civil litigation. She also speaks and counsels on business ethics and compliance. Earlier in her career, Moore was federal prosecutor in the Criminal Division of the United States Attorney's Office in Manhattan, where she investigated and prosecuted a range of white collar offenses, from financial institution fraud to health care fraud to money laundering.

Ms. Moore has published widely in matters of laws and ethics, including "Discovery Can Get Tangled Up in 'Strings': It's Not Yet Clear How Privileges Apply to E-mail Exchanges," National *Law Journal*; "Corporate Culpability Under the Federal Sentencing Guidelines," *Arizona Law Review*; "What is Really Unethical About Insider Trading?" *Journal of Business Ethics;* and "Do Executives Face De Facto Strict Liability for Environmental Crimes?", *Business Crimes Bulletin*, 1996. She also co-edited the books *Business Ethics: Readings and Cases in Corporate Morality* (1st and 2nd editions), *Ethics and the Management of Computer Technology*.

As a former prosecutor, Moore is an experienced investigator and trial lawyer who routinely used electronic documents to build and contest cases. She taught white collar criminal law and commercial law at the University of Wisconsin Law School. Prior to becoming a lawyer, she taught business ethics at the University of Delaware, the Wharton School, and Bentley College. Ms. Moore received her JD from *Yale Law School*, where she was executive editor of the *Yale Law Journal*. She graduated magna cum laude from Bowdoin College and holds a PhD from Harvard University.

Your E-mail Trail: Where Ethics Meets Forensics

VERIZON VISITING PROFESSORSHIP
IN BUSINESS ETHICS AND INFORMATION TECHNOLOGY

February 11, 2008

Jennifer M. Moore, JD, PhD

Partner, Epstein Becker & Green PC, New York, New York

It means a great deal for me to be here this week. I started my professional life at Bentley as an adjunct professor in philosophy in the early 1980s, at a time when business ethics had just begun as a field of study. When I told people I taught business ethics, they invariably responded, "Isn't that an oxymoron?" I want to thank Dr. Michael Hoffman for hiring me those many years ago, and for his dedicated work for over three decades that has made business ethics no longer an oxymoron, but a standard part of the education and development of business managers. I would also like to thank Verizon Communications for its generosity in sponsoring this lecture and Visiting Professorship, which bring together academics and practitioners. It is the commitment of companies like Verizon that helps make corporate integrity, responsibility and accountability not just slogans, but operating principles in the conduct of business.

Let me tell you a bit about my background and how it has influenced my thinking about business ethics. I spent the early part of my career as a philosopher and business school professor teaching and writing about issues in corporate ethics. I also read extensively in law journals and judicial opinions. I became interested in the law because I found that judges who were required to resolve real-world cases were struggling with many of the same concepts studied by philosophers working in ethics and social and political philosophy: individual and organizational intent, responsibility, and deliberation, and the relationship between individual and organizational responsibility.

I went to law school and then clerked for a federal judge at the trial court level. As a result of this experience, I decided to become a practicing lawyer. For 10 years I served as a federal prosecutor in Manhattan, where I focused on investigating and prosecuting white-collar criminal cases. Three years ago, I left the government and returned to private practice. I now spend my time representing corporations and individuals that are the subjects of civil and criminal white-col-

lar investigations, conducting internal investigations at the request of organizations, and advising corporations and their leaders on ethics and compliance.

I will be speaking to you today about some ethical, legal and philosophical issues that arise from the increasing use of e-mail in the conduct of business. My comments also apply to other forms of instant written communication, such as instant messaging and text messaging. A great deal of ethical discussion related to computers has focused on privacy and confidentiality issues posed by the ability of unauthorized persons (i.e., "hackers" or identity thieves) to get access to electronic information and communications that belong to, and are kept private by, others. Although these issues are of great importance, they are not my main focus today. Rather, I want to focus on the ways in which individual computer users compromise their own or others' privacy or confidentiality by voluntarily creating and sending instant electronic communications that are legitimately accessed by other people. I suggest that the use of e-mail and other instant forms of electronic written communication in business can compromise our ability to control the distribution of certain information about ourselves which was previously private or shared with a limited few.

Some of these compromises result from technological features of e-mail that increase the likelihood that a communication intended for one recipient or group of recipients will be received and read by others for whom it was not intended. They make it more difficult to keep information private and contribute to the larger trend in which maintaining privacy is increasingly a matter, not simply of refraining from disclosure, but also of affirmatively preventing dissemination of information. Simple examples are the "autocomplete" function and the sheer ease and speed of sending e-mail. In part because of these technological factors, preserving confidentiality no longer consists of merely limiting the disclosure of information. Affirmative steps are required to prevent disclosure to inappropriate persons.

Other issues arise from the style and content of many e-mails. Anyone who reads the headlines knows that even at work, e-mail users seem to feel comfortable sharing thoughts, feelings and information that they never would have recorded in writing and disseminated before the advent of e-mail. These e-mails have the potential to disclose to unintended recipients parts of the self that have traditionally been private and not subject to public exposure. Such e-mails can become the basis for inferences made by others about the sender's intent or character, and can result in public embarrassment, loss of reputation, loss of job, or even civil or criminal liability, both for the individual sender and the organization. The results are particularly dramatic in criminal law, where proof of intent is a necessary requirement for liability. It is no surprise that e-mail has become the "smoking gun" of choice in today's white-collar prosecutions. Before the advent of instant electronic communications, the statements in many of these e-mails most likely would have remained internal or been expressed orally to only a trusted few. It is unlikely that the senders would have been held to these statements in a court of law.

The issues raised by these features of e-mail and the way it is used are different in kind, not just in degree, from those raised by more traditional written business communications. To address these issues, we need to ask: What is the impact of the way we use e-mail on our ability to manage our identity, relationships, and roles? What is the scope of the duty of confidentiality in an age of e-mail and electronic data? When is reflecting on or proposing a course of action preliminary or deliberative, and when does it mature into intent? Does the use of e-mail have an effect on the deliberative process of individuals or organizations?

It is clear that although business people are now communicating routinely by e-mail, they frequently approach this form of communication with a casualness that denotes a lack of awareness of the seriousness that should be accorded to it, given its potential longevity and its value as evidence in lawsuits. From this perspective, I would suggest that the "forensic perspective" can provide a useful deliberative and self-assessment tool when considering our e-mail conduct.

How E-mail is Different

Written Records in a Conversational Style

The use of e-mail in business raises new questions because e-mail differs in important ways from letters and memoranda, the traditional forms of written business communication. Written communications may be created for several different reasons: to make a complex matter clear, complete and precise; as an aid to memory for both writer and recipient; to create a record that the communication took place; and to avoid the need to rely on oral testimony should a dispute about the contents ever arise. As a consequence, written communications have a credibility and evidentiary weight that oral communications, which are temporary, fleeting, and vulnerable to memory lapse, do not. United States law recognizes the importance of written communications by requiring certain kinds of agreements to be in writing in order to be enforceable.[1] In arm's-length business dealings, people are assumed to mean what they have said in writing, and are held to what they have written. A written statement is thought to commit

the writer in a way that an oral statement does not. As a result, traditional business letters and memoranda were and are formal, deliberate and precise.

E-mail, in contrast, arose in the personal context as a form of spontaneous, casual, off-the-cuff communication. E-mail is often conversational in style and tone and is frequently used for the same kinds of communications that take place in person or over the telephone. Its main advantage is speed and low cost. Generally written quickly and sent within seconds with the touch of a button, it may not be fully thought out or well articulated. Although it may appear complete, it often does not present the sender's final position on a topic. It may be merely a form of thinking out loud, as in a conversation. Before the advent of e-mail, most people would never have thought to write down these communications. Now they often choose to write them rather than say them.

Although e-mail is conversational, it lacks the interpretive aids of face-to-face conversation, such as tone of voice, body language, and facial expressions. The electronic substitutes – "emoticons" such as smiley faces, or abbreviations meant to indicate tone – are poor substitutes. Nor does e-mail usually include the compositional elements that help the reader determine tone and meaning in more formal writing. Accordingly, e-mail is easily misunderstood by the reader.

Sent in Haste, Repented at Leisure

Traditional forms of written communication, like letters, take time to compose, revise and send. During this time the writer has several opportunities to reflect on the letter's form and content, and the advisability of sending a letter at all. E-mail, however, is usually composed quickly, often without editing, proofreading or reflection, and can be sent instantaneously with the touch of a button. Normally, within minutes of its being sent, an e-mail appears in the inbox of the recipient. Despite the "recall" function on many e-mail programs, there is no reliable way to retract an e-mail before it is seen by the recipient.

E-mail is also easily misaddressed. Both electronic address books, which may hold addresses of several people with the same name, and the "autocomplete" function, which recognizes a name from the first few letters typed in the "to" field, are culprits here. In one well-known case, the *New York Times* reported that an attorney for Eli Lilly mistakenly sent a confidential e-mail about a settlement in a government investigation to a reporter for the *Times*, rather than to the intended recipient, another lawyer involved in the case with the same last name as the reporter.[2] Most e-mail users have had the experience of sending an e-mail to the wrong person. "Snail mail" is far more difficult to misaddress.

The following e-mail was sent by Jonas Blank, a summer associate at top New York City law firm, Skadden Arps. Summer associates are second-year law school students who are hired for the summer so that the law firms can evaluate whether to offer the student a full-time job after graduation. Blank wrote this e-mail to a friend – but also mistakenly e-mailed it to 40 other people in the firm, including 20 partners.[3]

> I'm busy doing jack s***. Went to a nice 2hr sushi lunch today at Sushi Zen. Nice place. Spent the rest of the day typing e-mails and bulls***ing with people. Unfortunately, I actually have work to do — I'm on some corp finance deal, under the global head of corp finance, which means I should really peruse these materials and not be a f***...
>
> So yeah, Corporate Love hasn't worn off yet... But just give me time...
>
> JLB

Blank's e-mail was opened almost immediately by the recipients, some of whom immediately forwarded it to Human Resources, as well as to friends outside the firm. Within a day or two virtually every New York lawyer had received a copy directly or read about it in the news.

Below is Blank's follow-up e-mail:

> I am writing you in regard to an e-mail you received from me earlier today. As I am aware that you opened the message, you probably saw that it was a personal communication that was inadvertently forwarded to the underwriting mailing list. Before it was retracted, it was received by approximately 40 people inside the Firm, about half of whom are partners.
>
> I am thoroughly and utterly ashamed and embarrassed not only by my behavior, but by the implicit reflection such behavior could have on the Firm.
>
> The addressing of the e-mail was obviously an honest mistake. The content of the e-mail was inappropriate, showed a total lack of discretion, responsibility and judgment, and undoubtedly did my reputation and my future here no favors. It showed disregard for the Firm's policies and procedures and for the very explicit speech that all summer associates were given about personal responsibility and using good judgment at the start of their training.
>
> The appropriate parties, including Hiring Partner Howard Ellin and Hiring Director Carol Sprague, are aware of the incident and working with me to deal with it appropriately.

> Although I cannot change what you and the other recipients saw, I do reiterate my sincerest apologies. I do and will take full responsibility for my actions in this incident, and I will do everything I possibly can to correct my mistakes and, more importantly, ensure that this and things like it will not happen again.
>
> With sincere regret,
> Jonas L. Blank[4]

You may have little sympathy for Blank because his embarrassment was largely due to his own carelessness. The incident does not pose a traditional "privacy" issue in the sense of protecting confidential information from assault from the outside. Nevertheless, the Blank e-mails illustrate an important aspect of privacy. One of the most striking things about these two e-mails is the difference in their style, tone and composition. The second one is recognizable as a formal business communication; the first is not. Which e-mail represents the "real" Jonas Blank? Cynics may suggest the first one, but the more likely answer is both. Blank's partners were simply never intended to see the face he showed his friend. Absent the e-mail, they were not entitled to see it, and almost certainly would never have done so.

As Sissela Bok noted in her book *Secrets*, privacy plays an important role in the definition and regulation of a person's relationships with others.[5] What you communicate to friends is not necessarily something you would choose to communicate to your employer. Moreover, this is not necessarily because you have something to hide, but because maintaining a zone of privacy gives you a degree of control over your role, relationship and identity that you would not have if everyone were aware of all available information about you.[6] The choice is part of what makes it possible to be intimate with your friend and professional with your employer.[7] Blank's misdirected e-mail caused a spillover of his personal life into his professional identity. Privacy also protects thoughts, inclinations, intentions, which protection in turn fosters autonomy and provides some protection against manipulation and control by other people.

Luckily for Blank, his personal e-mail resulted in embarrassment for him, but no harm to his law firm. But the e-mails of individuals in a business may represent more than their own personal thoughts and statements. Organizations are legal fictions that can act and speak only through their employees. Under corporate criminal law, acts of a corporation's agents or employees, done in the course of their employment, for the benefit of the corporation,[8] are imputed to the corporation for purposes of criminal liability. Employees do not have to be high-level executives for their statements or conduct to bind the corporation.

An e-mail itself may constitute an act attributable to the corporation. In a well-publicized case in 1995, for example, female employees at Chevron brought a sexual harassment suit against the company. One of the principal pieces of evidence was a "personal" e-mail circulated among 25 men at the company listing "25 reasons why beer is better than women." Chevron ultimately paid $2.2 million to settle the lawsuit. The plaintiffs claimed that Chevron created, or failed to prevent, a hostile working environment for women.

E-mail and the Scope of the Duty of Confidentiality

Not only is e-mail easily misdirected, it also proliferates more rapidly and widely than traditional, hard-copy written communications. Once an e-mail is received by a recipient, it is a freestanding document and the user has no control over its ultimate destination. It can be forwarded easily and at almost no cost; it can be posted to a blog or message board and become available to the public. E-mail, then, makes it much more difficult for both individuals and corporations to maintain privacy and confidentiality.

Confidentiality is vital in business for many different reasons. Professionals such as doctors, lawyers, accountants and psychiatrists have legal and ethical duties to preserve the confidentiality of client confidences in order to encourage the candor that is necessary for them to provide their professional services. Employees generally have ethical and legal duties of confidentiality and loyalty to their employers that require them to maintain the confidentiality of information belonging to their employer, such as patented inventions, trade secrets, non-public financial information, customer lists, business strategy, and marketing information, among others. Organizations must be able to maintain the confidentiality of this information if they are to compete economically and profit from the sale of their products and services.

Corporations also have legal duties to safeguard the confidentiality of certain types of customer information. For example, the Gramm-Leach-Bliley Act[9] contains provisions restricting the sharing of customers' personal financial information and requires covered financial institutions to have systems in place that safeguard that information. The privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) establish regulations for the use and disclosure of protected health information, that is, information about the health

status, provision of health care, or payment to health care that can be linked to an individual.[10]

Before the advent of electronic data storage and electronic communications, the duty of confidentiality was primarily the negative one of refraining from disclosure. Information was known to a limited group unless affirmative, sometimes costly steps were taken to publicize the information. Advances in the capture and storage of electronic data, and the ability to transmit it rapidly using e-mail and other forms of electronic communication, have changed the scope of the duty of confidentiality. Increasingly, confidential information is becoming public, and preventing dissemination has become the affirmative and more difficult task.

Certain habits of e-mail users increase the likelihood that e-mail will be forwarded to individuals who were never intended to be recipients. For example, use of the "Reply to All" function sends messages to everyone who was copied on the original message, often unnecessarily. In addition, in order to avoid looking up e-mail addresses, many users often start a new e-mail exchange by replying to an earlier e-mail from the recipient. These practices result in long e-mail "chains" that distribute information widely to employees who are not authorized to have the information or for whom it is not relevant or important. This can have significant legal consequences.

In a recent case, forwarding an e-mail chain outside the circle of employees for whom it was relevant resulted in the loss of the corporation's attorney-client privilege. As you may know, confidential communications between a client and an attorney, for the purpose of giving or receiving legal advice, are legally protected from disclosure unless the client consents to the disclosure or certain exceptions apply. Corporate clients are also protected by the attorney-client privilege just as individuals are. For a corporate client to receive the protection of the privilege, however, many jurisdictions require the corporation to restrict privileged communications to the small group of employees who need to review it in order for the corporation to be effectively represented (such employees are referred to as being "within the scope of the privilege"). In *Muro v. Target Corp.*, 2007 WL 1630407 (N.D. Ill. Nov. 28, 2006), an e-mail addressed by counsel to Target personnel within the scope of privilege was later forwarded via an e-mail chain to a non-lawyer outside the privilege's scope. The e-mail was marked "Confidential. Attorney-client privileged communication. Do not forward without author's consent," but the court held that forwarding the e-mail outside the privileged circle defeated the privilege. It ordered Target to disclose the document to its opponent in the litigation.[11] In law, lack of care in protecting privacy may waive the right to have the information later treated as confidential.

Many people do not realize that the threat to confidentiality is increased when electronic communications are used to transmit files such as word processing files or spreadsheets. Many electronic documents contain hidden data that reveals more information than meets the eye. This data – called "metadata," or data about data – reveals information that is not evident from the face of the document, such as the author, date of creation, and changes made during the life of the document. Sophisticated recipients can use forensic software to unlock the secrets of metadata, gaining access to information that was never meant to be transmitted, unless steps are taken to eliminate or conceal the metadata, which can be done through various software programs.

Organizations: Managing the Risk

Not surprisingly, most organizations have taken steps to reduce the risks of e-mail by adopting comprehensive electronic communications policies, which are designed to protect the organization's control over its own identity and reputation, prevent the loss of trade secrets and confidential information, prevent breach of organizational duties to stakeholders, and to detect and prevent unlawful conduct by employees. Because organizations act only through their employees, these measures involve greater or lesser restrictions on the privacy of individual employees. Electronic communications policies usually include one or more of the following:

- Restrictions limiting the personal use of e-mail and the Internet
- Policies forbidding harassing, offensive, threatening and other illegal communications, such as those that violate privacy law or copyright law
- Monitoring of e-mail and Internet use
- Blocked access to personal web-based e-mail
- Blocked access to external blogs and certain Internet sites (e.g., pornographic, sexist or racist, personal networking, gambling, or shopping sites)
- Monitoring is generally conducted using a combination of automation and manual review. Software programs are available to flag risky e-mails, which can then be viewed by investigators or compliance professionals. According to the American Management Association's (AMA) 2007 Electronic

Monitoring and Surveillance Survey, 43% of companies retain and review e-mails. Another 43% track the content, keystrokes, and time spent by employees at the keyboard.[12]

Because the U.S. Constitution protects individual privacy only against intrusions by the federal government, not private parties, employees of non-governmental employers do not have a constitutional right to privacy against their employers. Some privacy protections are provided by statute, such as the Electronic Communications Privacy Act of 1986. However, these protections are generally not available when the employer provides employees with e-mail service through a company-owned system, or when the employee consents to monitoring by using the company-owned system after having been clearly informed of e-mail monitoring. According to the AMA, 80% of organizations do notify their employees that monitoring is taking place.[13] Some do so through employee handbooks; others provide a notice that appears on the company's computer screen pop-up box informing employees that the monitoring is a condition of use of the company's computer system.

Employees, then, have no reasonable expectation of privacy in their e-mail or records of their web traffic to the extent it takes place at the workplace, through servers belonging to their employer. This is true even if the company system is used to access the employee's personal ISP in order to check his or her e-mail.

Because organizations act through individuals, and have both legal and ethical responsibilities, there are strong arguments in favor of a degree of transparency and control over the business communications of managers and employees. These e-mails are the communications of the organization. On the other hand, monitoring reduces employee privacy and exposes the writer's thoughts, emotions and intentions in an unprecedented way. The monitoring of personal e-mail is also controversial. These issues are currently the subject of vigorous debate by both lawyers and academicians. Monitoring employee e-mail has the capacity to significantly change the relationship between employer and employees.

Currently the law resolves the tension in favor of employer monitoring, in part on the ground that the employee has consented to it. Provided they are informed that monitoring is taking place, courts reason, employees can minimize the disclosure of personal information. E-mail is not the only means of communication in the workplace. Employees can pick up the telephone for personal matters.[14] The consent argument becomes less persuasive the more employers choose to monitor, and the more indispensable e-mail becomes as a form of business communication. However, employees can also preserve a level of privacy by writing e-mail more judiciously, with the awareness that e-mail may be treated with the same seriousness as a more formal written business communication and may be widely disseminated. Arguably, employees have an obligation to their organization to write e-mails that are professional and well-written.

Increasingly, employers have access to technological solutions such as software that flags high-risk e-mail for review, encryption software that can be used to protect confidential communications or data transmissions, and "scrubbers" that determine when an e-mail or attachment poses a high risk of transmitting metadata that could reveal confidential information. These solutions could be used to reduce the need for company monitoring. However, each of these options reduces the speed and efficiency of e-mail, and increases its cost.

The Use of E-mail as Proof of Intent

The adoption of e-mail as a means of business communication has led to another recent development: the use of business e-mails as proof of intent in litigation. This trend, which started with white-collar criminal cases, has now spread to civil regulatory enforcement cases and private litigation.

When corporations and their employees are accused of criminal conduct, the key evidence is not typically fingerprints, bloodstains or bullet trajectories. The primary dispute in white-collar criminal cases is often about intent. Criminal liability, like moral responsibility, requires not merely a "bad act," but also a "guilty mind." A statement may be false, for example, but it is not fraudulent unless the speaker knew it was false and intended to defraud the listener of something of value. Intent, knowledge or agreement with others to carry out an illegal act may all be elements of a crime (i.e., things that a prosecutor must prove to the jury beyond a reasonable doubt before the jury can properly convict the accused). When the accused is a corporation, intent is found by imputing the intent of an individual employee or employees to the organization.

Traditionally, intent, knowledge and agreement have been difficult to prove. Other than an admission by the accused, there is no direct evidence of intent. Intent must be inferred from circumstantial evidence, including actions, witness testimony, and formal business documents. Today, prosecutors and other litigants turn to e-mail for spontaneous, uncensored communications that are memorialized in writing and arguably demonstrate intent.

In 2005 and 2006, for example, in the course of an investigation into leaks by the company's Board of Directors, Hewlett-Packard's internal investigators hired an outside private investigation firm to investigate the leaks. The PI firm, in turn, obtained telephone records through "pretexting," a form of fraud in which investigators contact the telephone company and trick employees into providing records by posing as the individuals whose telephone records they are seeking. Kevin Hunsaker, an HP lawyer who was in charge of the investigation, e-mailed one of HP's internal investigators to ask if obtaining the phone records was "above board." He was advised that the PI firm got the phone records "under some ruse" and that the operator who provided the information "is liable in some sense." The investigator described the technique as "on the edge but above board." Hunsaker's reply, *"I shouldn't have asked,"* was key to establishing that he knew or should have known that the practice was fraudulent.[15]

In the WorldCom case, an e-mail from CFO Scott Sullivan to CEO Bernie Ebbers helped prove that Ebbers knew of the massive fraud to conceal losses by WorldCom. Sullivan wrote:

> [WorldCom's monthly revenue reports are] getting worse and worse. [The] copy that you and I have already had accounting fluff in it. . . all one-time stuff or junk."

The e-mail was a significant link in a chain of evidence that led to Ebbers' conviction and his sentencing to 25 years in prison.[16]

The use of e-mail to conduct business results in an enormous increase in the amount of evidence available in legal cases. In some cases, it may appear as if every step of the offense has been documented in e-mail. E-mail can be used to create a timeline of the offense, to identify who knew what, when, and to determine who spoke to whom for purposes of identifying members of a conspiracy. It provides a road map of the case for prosecutors. In some cases, additional evidence may be obtained from e-mail by forensic analysis. The name of the creator, date of creating and editing, names of recipients, and changes made may be recoverable. In one of my cases, forensic analysis showed that a document that seemed to be written solely by Individual A had in fact been edited by Individual B, a fact that proved guilty knowledge on the part of B.

E-mail has significantly changed the landscape of white-collar litigation. It has played a role in almost all of the high-profile white-collar criminal cases of the past 10 years.[17] Investigators and other litigants now often begin an investigation by issuing subpoenas requesting all of the e-mail traffic relevant to the subject under investigation or litigation, as well as more traditional business records. With few exceptions, United States law requires that these materials be produced. The e-mails are then reviewed and culled to identify those that produce the most powerful case.

Electronic discovery law now requires that steps be taken to preserve all documents, including all e-mail and other electronic documents, when the company becomes aware that litigation is "reasonably likely." This involves ensuring that electronic documents are not destroyed by routine procedures that are part of the company's document retention program, which determines when documents are destroyed and sets forth protocols for destruction. Because the costs of responding to requests for documents in litigation and the suspension of a company's document retention program are so high, many companies have begun to retain documents, including e-mail, for longer periods of time, making it more likely that e-mail can be retrieved.

Frequently, individuals or corporations conclude that deleting inculpatory e-mail will protect them against an inference of bad intent. This assumption is usually incorrect. Although e-mail is fleeting and electronic, it is usually more difficult to destroy than a hard copy document. Even when an e-mail is deleted from a user's inbox or sent folder, it can frequently be found on a backup tape or in the company's e-mail archives. Some industry regulations require members to save all communications for a particular statutory period, such as seven years. E-mail may also be present in the inbox, sent folder, or hard drive of a direct or indirect recipient of the e-mail, or on a PDA, home computer, laptop, or thumb drive. Finally, hard drives may contain deleted e-mails or fragments of deleted e-mails, because deleted data remains on a hard drive until it is over-written. Such material can be recovered by a forensic e-mail program.

The attempt to eliminate a smoking gun e-mail may itself become a smoking gun, suggesting consciousness of guilt. The inability to produce evidence can itself be a source of liability, potentially resulting in charges of obstruction of justice, spoliation of evidence, or an instruction to the jury that the missing evidence, if found, would be unfavorable to the side that failed to produce it. The most significant illustration of this principle in recent history is the Arthur Andersen case. The accounting firm, which handled Enron's accounts, was under investigation for its role in the Enron fraud. Massive destruction of documents relating to Enron began following this e-mail:

To: Michael Odom [partner in Arthur Andersen's Houston office]

Date: October 12, 2001

It might be useful to consider reminding the engagement team of our documentation and retention policy. It will be helpful to make sure that we have complied with the policy. Let me know if you have any questions.

Nancy Temple [In-house counsel for Arthur Andersen][18]

Arthur Andersen was indicted and convicted of obstruction of justice. The verdict was later overturned due to an erroneous jury instruction. By that time, however, Andersen had dissolved.

Ethical Deliberation and Self-Assessment

E-mail makes a compelling centerpiece for a legal case. It is not clear, however, whether e-mail can always bear the evidentiary weight placed on it. As noted above, e-mail is not always clear or precise. It can be ambiguous. It may be a joke. It shares some of the characteristics of conversation. Arguably, individuals should not be held to every statement expressed in an e-mail because some of these may be merely preliminary or exploratory, part of the deliberation process rather than final positions. Ethical deliberation, for individuals and particularly for corporations, necessarily involves sharing and discussing thoughts, opinions and arguments, including, in some cases, arguments that may ultimately be rejected as unethical or illegal. These thoughts may continue to evolve without the new view ever being communicated in an e-mail. Therefore, it is important when using e-mail to prove intent that the e-mail is assessed in light of the sender's overall course of conduct, and in the context of other e-mails relating to the offense as a whole. To treat each e-mail as representative of the sender's intent may prematurely freeze deliberation, chill the deliberative process, and result in inferior decisions.

An important question is whether the use of e-mail has already affected the process of deliberation. Does making a statement in writing and sending it to others commit the sender to the statement – both in the eyes of recipients, and the sender's own eyes – in a way that expressing it orally might not have done? Does weighing in on a decision electronically from one's own office, physically isolated from others, create a distancing effect that insulates the individual from the full meaning of his or her conduct? An electronic dialogue does not provide the immediate and emotional feedback that an in-person meeting provides. Arguably, the feeling of empathy – an important element of ethical deliberation – becomes more difficult when one is alone with one's computer. Finally, deliberation by e-mail may contribute to a fragmented or diminished sense of responsibility, in which no one individual feels responsible or accountable for a course of conduct because it is not solely attributable to any one person -- a tendency that is already a feature of organizational decision-making. These questions merit further study, but anecdotal evidence suggests that individuals are willing to say and do things in cyberspace that they might not say or do in person.

E-mail is such powerful evidence because it is in writing. A person may debate the meaning of a particular e-mail, but one cannot easily disavow statements memorialized in an e-mail. E-mail does not exist in a vacuum. It is created in a larger context that includes the background facts. Its meaning depends on this background and on an e-mail trail that includes prior e-mail received and sent by the same sender/recipient to other key individuals. To understand it, it is necessary to think forensically, that is, to consider how it relates to the context in which it takes place. Only then does it become evidence. Thinking forensically does not come naturally to most people. Indeed, it has been widely noted that people in organizations do not always understand the choices facing them as ethical choices at all. Patricia Werhane has called this failure to understand a failure of the "moral imagination." People with limited moral imagination have difficulty seeing and understanding how their actions relate to an overall course of conduct and how it is connected to the conduct of others. The following e-mail, for example, seems uncontroversial:

To: Marty Bahamonde

Date: August 31, 2005, 12:24

Thanks for the update. Anything specific I need to do or tweak?

Michael Brown

The assessment changes upon reading the original message from Bahamonde, to which Federal Emergency Management Chief Brown responded:

To: Michael Brown

Date: August 31, 2005, 12:20

Sir, I know that you know the situation is past critical. Here are some things you might not know.

Hotels are kicking people out, thousands gathering in the streets with no food or water. Hundreds still being rescued from homes.

> The dying patients at the DMAT tent being medivac. Estimates are many will die within hours. Evacuation in process. Plans developing for dome evacuation but hotel situation adding to problem. We are out of food and running out of water at the dome, plans in works to address the critical need.
>
> FEMA staff is OK and holding own. DMAT staff working in deplorable conditions. The sooner we can get the medical patients out, the sooner we can get them out.
>
> Phone connectivity impossible.[19]

Brown sent other flippant e-mails in response to communications about the Katrina disaster as well. Ultimately he was the subject of a Congressional investigation into his leadership.

Thinking forensically is not unlike other thought experiments that encourage people to take an objective view of their own actions, such as "How would you feel if your conduct were published on the front page of *The New York Times*?" or "How would you feel if someone did that to you?" Thinking forensically requires the deliberator to consider their e-mail as one piece of evidence, and to link it with other e-mails, and the underlying conduct.

Once this evidence is laid out and considered, it is easier to take an objective point of view. Thus, thinking forensically helps to develop sensitivity not only to the ethical import of one's e-mail, but of one's conduct as a whole. My purpose here is not to suggest that you should hide things or write dishonest e-mails. Rather, it is to encourage you to be aware of the implications of your e-mail, as well as your actions. It is crucial that we recognize that we may not be the only ones interpreting our e-mail. Given this, as people living in a world where e-mail has become an everyday part of our communications, it is incumbent upon us to understand that e-mail can be very different from other forms of communications, and that we need not only to act legally and professionally when drafting and sending e-mail, but to also heighten our ethical sensibilities because the implications of e-mail may be far more weighty than they might normally appear.

Thank you.

Below are the highlights of Jennifer Moore's question-and-answer session with Bentley students, faculty and guests.

Have you seen any cases where e-mails were planted as evidence, to leave a false trail to knowingly outwit others?

JENNIFER MOORE: I haven't seen that, but what I have seen is a lot of fake posts on blogs. In fact, what I've seen often is fraudsters who do it to trick others. There is an interesting web site called diligizer. It is a group of people who have been defrauded and want to discuss with others to ascertain if the person they're dealing with is on the up and up. A lot of times the fraudsters will go on the site and write complimentary blog entries about themselves. It happens all the time. I would suggest it won't be too long until we see a planted e-mail case.

I get e-mail messages on occasion that say, "You have won a wonderful prize of $3 million." I'm wondering whether we have the facility to track down the e-mail creators so that we can prosecute these people.

JENNIFER MOORE: Well, that's an excellent question. There are a lot of scams that appear on your computer. I use my tools to say, "Kill off that address," and then I send it to Microsoft or whoever, to alert them that these guys are doing this. The problem is, as soon as they're kicked off one e-mail server, they come right back on another. It's a way to get spyware on your computer so they can find out about you.

In fact, there was a case that was really egregious, called Direct Marketing. I was involved in this case because I represented a witness. This is a company, I believe based in Connecticut, that developed a really insidious way of getting software to track you. You might click on a pop-up box that would put a malicious software program on your computer. Then there was another little box saying you could get rid of it. When you clicked the box to get rid of it, you just embedded it further. Ultimately, it slowed down your computer to the point that people believed their computers were broken. It was really pernicious.

If you get enough evidence that something is a scam, you can report it to the FBI. If they think it's serious enough, they can track it down. There are people who do nothing but forensic computer work and they can trace these e-mails.

E-mails have a life of their own and are tough to destroy. If a version of an e-mail exists on a server somewhere, is that a factor in proving that e-mail evidence was destroyed on one's desktop computer?

Jennifer Moore: That's usually the way people find out that evidence was destroyed; the same evidence that should have been presented crops up somewhere else. The lawyers say, "This is a smoking gun and you didn't give it to us. We got it from someone else. Why didn't you produce it?" It's usually considered evidence of intent to cover something up. There is a phrase in criminal law called "consciousness of guilt." If you run away or try to cover something up, it just simply shows that you knew you were guilty and it proves intent.

Footnotes

[1] See New York General Obligations Law 5-701.

[2] For more information on this, please see the following articles:

Weiss, Debra Cassens. "Did Lawyer's E-Mail Goof Land $1b Settlement on the *New York Times* Front Page?" *ABA Journal* (Online), February 6, 2008, *http://www.abajournal.com/news/lawyers_e_mail_goof_lands_on_nyts_front_page*.

Weiss, Debra Cassens. "*New York Times* Reporter Says Lawyer's E-Mail Goof Not a Big Blunder." ABA Journal (Online), February 11, 2008, *http://abajournal.com/news/nyt_reporter_says_lawyers_e_mail_goof_not_a_big_blunder/*.

[3] "Oops," The New Yorker, June 30, 2003.

[4] *http://www.snopes.com/embarrass/e-mail/skadden.asp*

[5] Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Vintage Books: New York, 1993), pp. 18-22.

[6] Kim Lane Scheppele, *Legal Secrets: Equality and Efficiency in Common Law*; (University of Chicago Press: Chicago, 1990).

[7] *Ibid.*

[8] The law does not require that the corporation actually receive a benefit, or that the employee act primarily in order to benefit the corporation. Criminal liability for an employee's actions may be imputed to the corporation even if the corporation did not gain from the conduct, and even if the conduct violated company policy. Zero v. United States, 689 F. 2d 238, 242 (1st Cir. 1982) holding that employee must have been "motivated at least in part by an intent to benefit the corporation." United States v. Bainbridge Mgmt., 2002 U.S. Dist. Lexis 16686 at *15 (N.D. III Sept. 5, 2002)

[9] *The Gramm-Leach-Bliley Financial Services Modernization Act*, Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999)

[10] 45 C.F.R. 164.501. See *http://www.hhs.gov/ocr/hipaa/privacy.html*

[11] *Muro v. Target Corp.*, 2007 WL 1630407 (N.D. Ill. Nov. 28, 2006). See also "Legal Alert: Court Holds Forwarding Privileged Legal Advice to Employees Not Directly Concerned with its Subject Matter May Waive Privilege," *www.sutherland.com/news*

[12] "2006 Workplace E-mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators," *http://press.amanet.org/press-releases/28/2006-workplace-e-mail-instant-messaging-blog-survey-bosses-battle-risk-by-firing-e-mail-im-blog-violators*. The survey reports that 28% of responding companies said they had fired employees for misusing e-mail, and 30% had fired employees for misuse of the Internet.

[13] *Ibid.*

[14] According to the AMA, some employers monitor telephone calls and voice mails as well as e-mail and Internet activity. *Ibid.*

[15] *http://www.businessweek.com/technology/content/oct2006/tc20061003_396787.htm?chan=top+news_top+news+index_businessweek+exclusives*

[16] *http://www.usatoday.com/money/2004-03-02-ebbers_x.htm.*

[17] Using Employees' E-mail Against Them, *Forbes*, July 10, 2008; See also "Top Ten Smoking Gun E-mails." *http://www.forbes.com/2008/06/20/employee-internet-security-lead-cx_tw_0620e-mail.html?partner=e-mail*;

[18] *CNNMoney*, January 21, 2002 story entitled "Andersen Exec: Shredding Began After E-mail."

[19] *http://i.a.cnn.net/cnn/2005/images/11/03/brown.e-mails.analysis.pdf*

8M10/08UP.CBE.2418