EMPLOYMENT ISSUES IN THE PAPERLESS WORKPLACE

Prepared for Sterling Seminar Employment Law Update in Massachusetts
Boston, MA; September 6, 2007

Robert R. Berluti, Esq.
Berluti & McLaughlin, LLC
44 School St.
Boston, MA 02108
(617) 557-3030

INDEX

A. LEGAL AND PRACTICAL ISSUES RAISED BY ELECTRONIC PERSONNEL RECORDS STORAGE, ELECTRONIC SIGNATURES, ONLINE PERSONNEL POLICIES, AND PAPERLESS PAYROLL

1. Electronic Personnel Records Maintenance and Retention

In Massachusetts, electronic transactions are governed by the Uniform Electronic Transactions Act. The Act provides, in part, that:

> "If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:
>
> (1) Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and
>
> (2) Remains accessible for later reference."

G.L. c. 110G, § 12(a). The National Electronic Commerce Coordinating Counsel ("NECCC"), an alliance of national state government associations dedicated towards the advancement of electronic government within the states, has recommended the following guidelines for maintaining secure and reliable economic records and systems:[1]

- Identify and assess specific legal, business, and other requirements that apply to e-records;
- Base e-records management measures on the value of the records;
- Focus on the systems and business processes that produce e-records; and
- Training is critical.

[1] These guidelines and the recommendations that follow are quoted directly from the NECCC's Electronic Records Management Guidelines for State Government: Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records, Exposure Draft (Dec. 2001), *available at* http://www.ec3.org/Downloads/2001/Records_Mgmt_ED.pdf, *last accessed* Aug. 10, 2007.

In order to maintain accessible, authentic and complete e-records, NECCC recommends the following:

- Maintain an e-records management policy documenting your organization's policy on information management and storage;
- Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records;
- Adopt and use records retention and disposition schedules in compliance state and local law;
- Adopt and use state preferred technical standards;
- Maintain e-records in encrypted form only as long as security concerns warrant;
- Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period;
- Develop or revise access and personal privacy protection policies to cover e-records;
- Develop methods to provide public access to e-records and to protect personal privacy and confidentiality; and
- Provide access to e-records in the form the user prefers.

To ensure that your e-records are secure, reliable and trustworthy, you should:

- Assign system management roles and responsibilities;
- Develop and maintain problem resolution procedures, including incident reporting and response procedures;
- Test system performance including the reliability of hardware and software;
- Maintain audit trails of system activity by system or application processes and by user activity;

- Provide training and user support adequate to ensure users will implement system procedures;
- Develop a contingency plan that includes data backup, disaster recovery, and emergency operations;
- Establish controls for the accuracy and timeliness of input and output;
- Perform routine backups;
- Maintain physical and environmental security controls;
- Provide for identification and authentication; and
- Maintain external access control mechanisms.

The United States Employee Retirement Income Security Act ("ERISA") also imposes certain record maintenance and retention requirements that can be met through the use of electronic media, if the following conditions are met:

- "The electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity, and reliability of the electronic records;
- The electronic records are maintained in a reasonable order and in a safe and accessible place, so that they may be readily examined (e.g., the system should provide for indexing, preserving, retrieving, and reproducing the electronic records);
- The records are readily convertible into legible paper copy;
- The electronic recordkeeping system is not subject to any agreement or restriction that would limit the ability to comply with any reporting and disclosure requirements of ERISA;
- Adequate records management practices are implemented (e.g., procedures for labeling electronic records, providing a secure storage environment, creating back-ups); and
- The electronic records must exhibit 'a high degree of legibility and readability' when viewed on a computer terminal."

Robert J. Nobile, Guide to Employee Handbooks § 1:43 (West 2007).

The following checklist may be useful in implementing an effective document retention policy:

- Who is the person most knowledgeable about the hardware and software we use, including the versions of software?
- Do we have a document retention policy for when documents such as e-mails may be written over?
- If sued, who do we want to testify about our systems capabilities and limitations?
- If information is copied to our hard drives, CD's, DVDs, Zip drives, etc., is it more accessible than information on back-up tapes that may not be immediately accessible? Similarly, how is this media stored?
- If we receive a letter identifying a dispute or potential disputes that demands the preservation of electronically stored data, how will we handle the letter and our so-called preservation obligations?
- Do we have a records retention policy, computer usage policy, or employee privacy policy?
- Do we communicate and educate our employees about these policies?
- Do we monitor and enforce these policies?

2. Electronic Signatures

The Electronic Signatures in Global and National Commerce Act ("E-Sign"), Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. § 7001 *et seq*.), was enacted to facilitate the use of electronic records and signatures in interstate and foreign commerce. It defines an electronic signature as an "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 15 U.S.C. § 7006. Although the Act does not explain

what an electronic signature looks like or what technology must be used for its creation, it establishes the following:

1. Electronic signatures and contracts have the same legal validity as written ones;

2. In a case where consumers have a specific legal right to receive information in writing, (e.g., if consumer is guaranteed information regarding mortgage fees), an electronic version of the information can only be provided to them under the following circumstances:

    a. The consumer consents to an electronic version;

    b. Before consenting, consumers are provided with a statement informing them that they have a right to receive the information on paper and may withdraw their consent;

    c. The consumer is provided with a statement detailing the hardware and software requirements for the electronic record;

    d. If the hardware and software requirements are revised, the consumer must be informed of the change and allowed to withdraw consent.

3. If, according to an existing law, a record must be provided by a specified method requiring receipt verification or acknowledgement, electronic records may only be used if the electronic method provides such verification; and

4. ESA permits notarization or other authentication of a document to be satisfied via an electronic signature.

Robert J. Nobile, Guide to Employee Handbooks § 1:45 (West 2007).

E-Sign does not preempt states from adopting their own laws governing electronic records and signatures. The majority of states have adopted the Uniform Electronic Transactions Act ("UETA"), which "was developed by the National Conference of Commissioners on Uniform State Laws to provide a legal framework for the use of electronic signatures and records in government or business transactions." Uniform Electronic Transactions Act, National Conference of State Legislatures, *available at*

http://www.ncsl.org/programs/lis/CIP/ueta.htm, *last accessed* Aug.15, 2007. The UETA "provides a legal framework for electronic transactions [, giving] electronic signatures and records the same validity and enforceability as manual signatures and paper-based transactions." Id. Massachusetts adopted the UETA in 2003.

A state may avoid preemption by E-Sign if its version of the UETA specifically states that its passage is not intended to displace consumer protections provided by federal law. Additionally, E-Sign will not preempt state law if the state's version provides additional consumer protections that E-Sign does not address. Margot Saunders, "Tests for Preemption of State Laws under Electronic Signatures in Global and National Commerce Act," National Consumer Law Center (Apr. 18, 2001), *available at* http://www.consumerlaw.org/issues/e_commerce/mini_memo.shtml, *last accessed* Aug. 10, 2007.

The Uniform Electronic Act as adopted in Massachusetts avoids federal preemption by including the following language: "[t]his chapter applies to a transaction governed by the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. section 7001 *et. seq*., but is not intended to limit, modify or supersede section 101(c) of that Act, 15 U.S.C. section 7001(c)." G. L. c. 110G, § 3 (b)(3).

To facilitate use of electronic signatures, software companies offer a variety of e-signature software products, such as:

a. OnSign—supports e-signatures only for Microsoft Word 97 and 2000. (http://www.onsign.com).

b. E-Signature—a platform-specific solution that supports any Windows, Macintosh and OS/2 application. (http://www.esignature.com).

c. SignOnline—uses the PDF format; available as a PDF Plug-in. (http://www.isignonline.com).

d. iSign—a software development kit; it is limited to those using the Windows platform and Active X controls. (http://www.cic.com).

Robert J. Nobile, Guide to Employee Handbooks § 1:49 (West 2007).

3. Online Personnel Policies

There are no legal impediments to implementing an electronic employee handbook. Employers should, however, follow certain guidelines in utilizing electronic technology to communicate their companies' policies to employees:

- Remember that an electronic handbook needs to enable the employer to effectively communicate with employees (e.g., to introduce employees to company's policies, procedures, programs, and guidelines);

- Make sure that all employees are properly trained on how to use a computer. Lack of training could lead to employee relations problems and, if some protected class members are adversely affected by lack of computer training or access, to charges of unlawful discrimination;

- Keep in mind that the Americans with Disabilities Act (ADA) requires employers to make reasonable accommodations to avoid discrimination against qualified individuals with disabilities. For example, an employee with a physical or mental disability may require accommodations with retrieving the online content of the handbook;

- Consider how field or satellite offices' employees or those who work out of their homes will obtain access to handbook information;

- Remember that in wrongful discharge and other cases, employers have the burden of proving that employees received a copy of the handbook and were on notice that their employment was at will. To avoid liability in this regard, employers should decide whether to require employees to sign an acknowledgement copy of the handbook electronically. Additionally, employees must be informed that they may access the document at any time and that they are responsible for familiarizing themselves with its contents;

- Think about how you will advise employees of policy changes (e.g., e-mail, handout, etc.)

- Implement security measures to ensure that the policy may be modified by authorized personnel only.

Robert J. Nobile, Guide to Employee Handbooks § 1:40 (West 2007).

4. Legal Hurdles of Paperless Payroll

If a company chooses to electronically deposit employees' pay checks directly into their bank accounts, it has to comply with state requirements on providing a pay stub. There are four different approaches that states follow in regards to providing employees with a pay stubs. Note that every state has its own specific requirement of what information a pay stub must contain.

1. States with no requirement: these states do not require employers to provide statements to employees containing their pay information. If an employer chooses to do so, they can do it in electronic format.

2. "Access" states: these states require employers to "furnish," "give," or "provide" a statement with employee's pay information. The statement, however, does not have to be in writing or on paper. Furnishing an electronic pay stub is enough to comply with the access requirement.

3. States that require access and print capability: in states following this approach, employers are required to provide a written or printed statement of employee's pay information. An employer can comply with the requirement by furnishing an electronic pay stub that employees can print.

4. Consent states (Massachusetts): employees must consent to receive a pay stub electronically. Otherwise, the state requires employers to deliver a pay stub either as a detachable portion of the paycheck or as a separate piece of paper. To get an employee's consent to receive the pay stub electronically, an employer can tie electronic pay stubs to direct deposit. That way, when an employee authorizes direct deposit, an employer can include the employee's consent as part of the legal disclaimer on the direct deposit authorization. As a result, employees who choose to participate in the direct deposit program will receive their pay stubs electronically.

IOMA's Payroll Manager's Report (Oct. 2003), *Electronic Pay Stubs: Another Step Toward a 'Paperless' Payroll*, *available at* http://www.talx.com/news/articles/

ElectronicPaystubs.pdf, *last accessed* Aug. 10, 2007.

B. IDENTITY THEFT PROTECTION

The Identity Theft and Assumption Deterrence Act of 2003 ("ITADA"), codified in 18 U.S.C. § 1028(a), defines identity theft as "fraud related to activity in connection with identification documents, authentication features, and information." ITADA makes possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime.

The Massachusetts version of ITADA, at G.L. c. 266 § 37E, states:

> Whoever, with intent to defraud, obtains personal identifying information about another person without the express authorization of such person, with the intent to pose as such person or who obtains personal identifying information about a person without the express authorization of such person in order to assist another to pose as such person in order to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of the crime of identity fraud.

More than 500 data breaches compromising the personal information of millions of individuals have occurred since 2005. Byron Acohido, *TJX Data Theft Leads to Money-Laundering*, USA Today (Jun. 11, 2007). In January 2007, TJX Companies, Inc., the parent company of TJ Maxx and Marshalls, among others, announced that it had fallen victim to what was later determined to be "the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers." Ross Kerber, *Cost of Data Breach at TJX Soars to $256m*, The Boston Globe (Aug. 15, 2007). On August, 14, 2007, the company announced that the costs from the theft have "ballooned" to $256 million. Id. This case highlights the need for companies to create and implement security policies to protect employee and customer data.

A company can effectively shield itself from the threat of employee or customer identity theft by securing customer data, protecting personal information of employees, and staying informed in the crime's current trends. To this end, companies should follow certain guidelines:[2]

Collecting Personal Information

- Collect and maintain only the information that is reasonable for business purposes;
- Make sure there is a good reason for collecting personal information from employees; and
- Acquire information in a safe manner so that it cannot be easily overheard or obtained by other parties.

Storing Information

- While more companies are acknowledging the benefits of going "paperless" with their record keeping, security measures should be placed around any electronic systems used to store personal data;
- If paper records of personal information are kept, access to such files must be carefully secured;
- Conduct regular background checks on all employees and vendors with access to sensitive information. There are many companies that specialize in employment screening, as well as private investigators and online data brokers. Employers can also conduct background checks themselves by logging on to public records and commercial databases;[3]

[2] The majority of these guidelines are quoted directly from Michael Erickson, *Protecting Employees' Personal Information*, *available at* http://www.aascif.org/public/Second_Quarter_2007/EE_privacy.htm, *last accessed* Aug. 10, 2007.

[3] Background checks are in part regulated by the Fair Credit Reporting Act (FCRA), codified in 15 U.S.C. §1681 *et seq*. FCRA was enacted to protect the privacy of consumer report information and to ensure the accuracy of the information supplied by consumer reporting agencies. A consumer report contains information about an individual's personal and credit characteristics, reputation and lifestyle. To be covered by FCRA, a report must be prepared by a consumer reporting agency – a business that specializes in assembling such reports employers. When conducting a background check, an employer may inquire about the following: credit history, education, criminal records, driving record, past employment, references, professional licenses, workers' compensation, and medical history. Privacy Rights

- Ensure that any vendors who may have access to personal information are in compliance with all laws and regulations that apply to them; and

- Lock laptops when not in use and train employees to follow specialized laptop data protection protocols (45 percent of employee identification theft can be traced to stolen laptops).

Disclosing Information

- Hold employees accountable for not following the company's information management guidelines;

- Guide employees to be especially attentive during high risk situations (such as relocation);

- Encourage employees to be cautious in their dealings with vendors;

- Equip employees with tips to spot possible identity theft;

- Provide employees with resources to help in case of information theft;

- Ensure that sensitive information is shared only on a tight need to know basis.

Disposing of Information

- Dispose of sensitive information that is no longer needed in a timely manner. To reasonably protect files against unauthorized access to personal information, comply with the Fair and Accurate Credit Transaction Act's (FACTA) Disposal Rule.

FACTA was passed by the United States Congress on December 4, 2003 as an amendment to the Fair Credit Reporting Act. See Pub. L. 108-159, 111 Stat. 1952. By the Act's passage, Congress intended to help consumers fight against identity theft. The FACTA Disposal Rule, effective June 1, 2005, states that any person who maintains or

---

Clearinghouse, *Employment Background Checks: a Guide for Small Business Owners*, *available at* http://www.privacyrights.org/fs/fs16b-smallbus.htm, *last accessed* Aug. 10, 2007.

otherwise possesses consumer information for a business purpose is required to dispose of discarded consumer information, whether in electronic or paper form. 16 C.F.R. 682.2.

The Rule applies to:

- Consumer reporting companies;
- Lenders;
- Insurers;
- Employers;
- Landlords;
- Government agencies;
- Mortgage brokers;
- Car dealers;
- Attorneys;
- Private investigators;
- Debt collectors;
- Individuals who pull consumer reports on prospective home employees (nannies or contractors); and
- Entities that maintain information in consumer reports.

The Disposal Rule establishes "reasonable" disposal practices to prevent unauthorized access to confidential consumer information. The Rule suggests adopting the following practices to dispose of consumer information:

- Burning, pulverizing, or shredding of physical documents
- Erasure or destruction of all electronic media
- Engaging services of a third party involved in the business of information destruction.

Federal Trade Commission News Release, *FACTA Disposal Rule Goes into Effect June 1*, *available at* http://www.ftc.gov/opa/2005/06/disposal.shtm, *last accessed* Aug.14, 2007.

C. CURRENT BEST PRACTICES REGARDING EMPLOYEES' USE OF COMPANY COMPUTERS

1. Electronic Surveillance

Employers monitor employees' e-mail and internet usage mostly to combat legal claims involving theft of trade secrets, discrimination, sexual harassment, defamation, and copyright and trademark infringement. According to recent surveys, at least one third of United States employers monitor their employees' computer use. Companies justify electronic monitoring by having a legitimate interest in (1) ensuring employee productivity; (2) securing networks and data; (3) guarding intellectual property and competitive advantage; (4) protecting investment in equipment and bandwidth; (5) preserving a non-threatening work environment; and (6) avoiding legal liability or incriminating electronic evidence. Mark Rowe, *Ethical Implications of Employee Monitoring* (presentation given at the Boston Bar Association CLE Seminar on High Tech Monitoring and Workplace Privacy on June 27, 2007).

On the federal level, electronic monitoring of employees is regulated by the Electronic Communications Privacy Act ("ECPA"). Title I of ECPA amended the federal Wiretap Act, codified at 18 U.S.C. §§ 2510-2522. The amended Wiretap Act prohibits interception of oral, wire, or electronic communications. Title II, also known as the Stored Communications Act ("SCA"), is codified at 18 U.S.C. §§ 2701-11. The SCA prohibits "unauthorized access" to stored wire or electronic communications. Violations of ECPA carry civil and criminal penalties and are subject to private causes of action. Employers, however, may monitor their own proprietary e-mail systems without violating the Wiretap Act or the SCA under the service provider exceptions which allow interceptions on the

employer's own system **made in the ordinary course of business**. Employers may also avoid violations of the Wiretap Act by requiring employees to give written consent to monitoring or by obtaining implied consent, which is obtained by giving **prior notice** to the employees that their communications will be monitored. Massachusetts Employment Law, Vol. II, Handbook Supplement at Chapter 17, § 17.6.2 (Supp. 2006).

On the state level, electronic monitoring in the workplace is regulated by various state constitutional, common law, and statutory sources. In Massachusetts, electronic monitoring in the workplace is governed by G. L. c. 272, § 99. Similar to federal law, the Massachusetts wiretap statute applies to e-mail interceptions, and contains a service provider exception. It is interpreted in accordance wit the federal Wiretap Act. Id.

Employees who oppose electronic monitoring of their e-mail and internet communications may bring claims for invasion of privacy, wrongful termination, infliction of emotional distress, and violation of state and federal wiretapping laws. Similarly, employees argue that electronic monitoring results in:

- The possibility of creating suspicious and hostile workplace;
- The inherent invasion of privacy;
- Interference with unavoidable personal business, especially with longer working hours; and
- Increased workplace stress and pressure and its negative impact on performance.

Mark Rowe, *Ethical Implications of Employee Monitoring* (presentation given at the BBC CLE Seminar on High Tech Monitoring and Workplace Privacy on June 27, 2007).

To minimize the risk of legal claims based on electronic monitoring, it is recommended that employers implement a written electronic communications policy that accomplishes the following:

- Identifies limitations on workplace e-mail and internet usage;
- Prohibits use of workplace e-mail and internet for transmission or receipt of discriminatory, harassing, defamatory, pornographic or any other unlawful material, as well as confidential and/or trade secret information ;
- Prohibits the use of company's technology for entering into contracts, searching for alternate employment, or soliciting religious, political or charitable donations and/or participation;
- Notifies employees that any electronic communications in the workplace may be monitored by the employer;
- Warns employees that violation of the policy may result in disciplinary action or termination; and
- Requires employees to sign consent forms agreeing to electronic monitoring of workplace e-mail and Internet usage. Another option is having dialogue boxes that employees must click, agreeing to or referencing the terms of use of the company's computer equipment.

Renee Inomata, *Minimizing Risks of Monitoring E-Use in the Workplace*, Burns & Levinson LLP: Internet and Technology Update (Fall 2001).

Massachusetts Attorney Jonathan D. Canter, who has written articles on the subject of reasonableness of employees' expectations of privacy in the workplace, opines that "workplace privacy is a balancing test balancing the expectation of an employee for privacy to the needs of an employer to run a business." What is "reasonable" is a question for a jury to decide. Meanwhile, employers continue to struggle to strike an appropriate balance between respecting employees' privacy rights and protecting corporate interests.

Most attorneys agree that although employers have plenty of legitimate reasons to retrieve and review electronic employee communications, they should minimize their intrusion into employees' privacy as much as possible. Employers might build in some leeway into their electronic policies so that "employees don't feel they are in violation of company policy any time they send a private e-mail." Tony Wright, *Lawyers Say the Expectation for Workers Should Remain Low*, Massachusetts Lawyers Weekly (Sept. 19, 2005).

Cases of Interest Related to Workplace Electronic Surveillance

- Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12413-RWZ, 2002 WL 974676 (D. Mass. 2002) (employee did not have reasonable expectation of privacy in e-mail on employer's system, despite use of personal passwords and e-mail folders).

- Restuccia v. Burk Tech. Inc., No. 95-2125, 1996 WL 1329386 (Mass. Super. Ct. Aug. 13, 1996) (holding interception of e-mail messages by computer's automatic systems was within employer's "ordinary course of business" and did not violate state wiretap statute).

- United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (holding e-mail in temporary, transient storage during the transmission process can be considered to be in transit for Wiretap Act's purposes

- United States v. Simons, 29 F.Supp.2d 324 (E.D. Va. 1998) (interpreting Section 2511 of Wiretap Act to mean that e-mail message must be in transit to be intercepted).

2. Client confidentiality issues in electronic communications

An attorney's obligations regarding the disclosure of confidential information are governed by Massachusetts Rule of Professional Conduct 1.6 which states that "[a] lawyer shall not reveal confidential information relating to representation of a client unless the client consents after consultation" unless an exception enumerated in Rule 1.6 (b) applies. M. R. P. C. 1.6(a).

The standard for protecting client confidentiality is *reasonableness*. If a disclosure occurs, the Supreme Judicial Court has held that "where it can be shown…that reasonable precautionary steps were taken [to ensure a document's confidentiality], the presumption will be that the disclosure was not voluntary and therefore unlikely that there has been a waiver." In Re Reorganization of Electric Mut. Liab. Ins. Co., Ltd., 425 Mass. 419 (Mass. 1997) ("EMICO").

The following factors are relevant when determining whether the attorney-client privilege has been waived by an inadvertent disclosure of confidential information:

- the reasonableness of the precautions taken to prevent inadvertent disclosure;
- the amount of time it took the producing party to recognize its error;
- The scope of the production;
- The extent of the inadvertent disclosure; and
- The overriding interest of fairness and justice.

Amgen Inc. v. Hoechst Marion Roussel, Inc., 190 F. R. D. 287, 292 (D. Mass. 2000). After an analysis of these contributing factors, and the totality of the circumstances, a court may rule "either that the inadvertent disclosure has effected a waiver of the privilege or that the privilege remains intact." Id.

i. Privilege Issues Relating to E-Mail

E-mail communications are protected by the attorney-client privilege if the following factors are met:

1. an attorney-client relationship exists;
2. the communications were received from the client during the

course of his or her search for legal advice from a lawyer in his or her capacity as an attorney;

3. the communications were made in confidence; and

4. The privilege as to these communications has not been waived.

EMICO, 425 Mass. 419 (Mass. 1997).

While Massachusetts' appellate courts have not yet addressed the issue of privilege with respect to communications made using corporate email accounts and/or company-issued computers, the Superior Court has issued a few decisions on the topic that are informative. In these cases, whether or not an employee's email communication with his attorney was privileged turned on the reasonableness of the employee's belief that he could communicate confidentially with his attorney using his company's computer and/or email system. See, e.g., TransOcean Capital, Inc. v. Fortin, 2006 WL 3246401 at *1 (Mass. Super. 2006); Nat'l Econ. Research Assoc., Inc. v. Evans, 2006 WL 2440008 at *1 (Mass. Super. 2006). To determine if the employee's belief was reasonable, the court relied primarily on the company's computer usage and email policies. In both *Fortin* and *Evans*, the court determined that if a company's policies and procedures manual plainly warns that all communications sent or received through the company's information systems belong to the employer and can be read by the company at any time, and that policy is properly disseminated to company employees, an employee cannot reasonably expect to communicate in confidence with his attorney using his corporate email account and/or computer. See Fortin, 2006 WL 3246401 at *4 (employee had reasonable expectation of privacy in emails he sent to his attorney using a corporate computer because the employer

did not have its own computer usage policy and failed to notify its employees that the third-party policy it relied on applied to them); Evans, 2006 WL 2440008 at * 3 (employee's emails to his attorney using his personal Yahoo e-mail account on a company issued computer were privileged because company's computer usage policy did not warn employee's that the content of emails viewed through an internet email account would be stored and viewed by the company).

Attorney Sharon R. Burger, a partner in the litigation department of Nutter McClennen & Fish, LLP, makes the following recommendations for employers and attorneys in her article *Attorney-Client Privilege Meets E-Mail*, Boston Bar Journal (March/April 2007).

Employers should draft clear computer usage policies stating that: (1) anything created, sent or received on a company computer, including laptops and PDAs, belongs to the company; (2) all internet sites visited are logged and the content of those sites may be viewed by the company; (3) no employee may expect privacy in his computer usage, including emails; and (4) the company may monitor computer usage. Such policies should be in writing, issued to every employee, acknowledged by the employee and enforced uniformly. Burger notes that such a strict policy may not work for all employers and suggests that employers consider the impact such a policy may have on morale and employee efficiency.

Attorneys should, moreover, (1) advise clients to familiarize themselves with their employer's computer usage and e-mail policies; (2) use the client's personal e-mail address for all communications; (3) encourage clients to retrieve attorney e-mails from their own

computer instead of from a personal internet account accessed through an employer's computer or network; and (4) appreciate that some clients may be unable to communicate freely during the workday. Sharon Burger, *Attorney-Client Privilege Meets E-Mail*, Boston Bar Journal (March/April 2007).

ii. Dealing with Metadata

Disclosure of confidential information is often caused by inadvertent disclosure of metadata. Metadata is data that provides information about other data. It is embedded in electronic documents, like those created by Microsoft Word, and contains such information as file names, dates, authors and recipients, as well as print-out dates, changes and modification dates and other information.

The "Track Changes," "Comments," and "Previous Versions" features of Microsoft Word can create confidentiality problems for attorneys because they can capture and store potentially confidential information that is not immediately visible to the user but which can be forwarded to and reviewed by third-parties. The "Track Changes" feature is the "most worrisome" because it "keeps track of [the user's] revisions after the changes have been accepted or rejected. Thus, although the document itself may show a clean, final copy, the unseen metadata within the document could contain every change made to that document since it was created." Philip Lyon, *Confidentiality and Ethics in a Hi-Tech World: Some Nuts-and-Bolts Solutions*, the Practical Lawyer, Volume 53, Number 2, Apr. 2007. Attorneys should, therefore, be careful to review metadata for confidential information before transmitting electronic documents to third-parties.

Attorneys can also delete or "scrub" metadata from a file prior to forwarding the document to a third-party. Microsoft provides a tool for removing metadata from Word, Excel or PowerPoint files on its website. Go to www.microsoft.com/downloads and search for "rhdtool.exe." Metadata can also be removed by saving a document in, or converting a document to, either Rich Text Format (.rtf) or Portable Document Format (.pdf) prior to sending it.

In 2004, the New York State Bar Association became the first state bar to issue an official opinion on the ethical issues surrounding the disclosure of metadata, finding that lawyers have an ethical obligation "to use **reasonable care** when transmitting documents . . . to prevent the disclosure of metadata containing client confidences or secrets." N.Y. State Bar Ass'n Comm. On Prof'l Ethics, Op. No. 782 (Dec. 8, 2004) (emphasis added). This comports with Massachusetts's general approach to inadvertent disclosures set forth in In the Matter of Reorganization of Electric Mutual Liability Insurance Co, Ltd., 425 Mass. 419 (Mass. 1997) and Amgen Inc. v. Hoechst Marion Roussel, Inc., 190 F.R.D. 287, 292 (D. Mass. 2000), described above.

Other References

Carolyn Witherspoon, *Confidentiality and Ethics in a Wired World*, the Practical Litigator, Vol. 18, No. 3 (May 2007).

iii. Preventing Theft of Confidential Client Data from Portable Electronic Devices

Confidential client data is often obtained through the theft of company laptops. According to the Privacy Rights Clearinghouse, a large number of laptop thefts have compromised enormous amounts of confidential personal information since 2005. The best

way to prevent such thefts is to implement a company-wide policy prohibiting the storage of confidential client data on laptops unless absolutely necessary and allowing employees remote access to the company's servers via a secure internet connection. If such information has to be stored on a laptop, make sure that the laptop is stored in a secure location, is password protected and that the data on the laptop is encrypted.

Similar security concerns are raised by the use of other portable electronic devices, such as the Blackberry, Treo, and the Q, which are easily lost or stolen. Wireless transmissions from these devices can also be intercepted by third-parties. Once again, prohibiting or limiting the storage or discussion of client information on these devices is the best way to prevent intercepted transmissions and/or theft. If such a policy is impractical, make sure to enable each devices password protection feature.

Wireless transmissions can also be intercepted when employees use laptops or other portable devices to send email and data via public wi-fi hotspots. To ensure that such transmissions are secure, install and utilize an encryption program to encode the messages before they are sent.

References

Philip Lyon, *Confidentiality and Ethics in a Hi-Tech World: Some Nuts-and-Bolts Solutions*, the Practical Lawyer, Vol. 53, No. 2 (Apr. 2007).

Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm, *last accessed* Aug. 15, 2007.

iv. Chief Privacy Officers

As our dependence on electronic data management tools, the internet and wireless technology has grown, so has the need to implement a wide-range of privacy and security

policies to protect confidential information that is stored and transmitted electronically. Many companies have responded to this need by creating a new executive position to oversee the creation and implementation of such policies: a Chief Privacy Officer or CPO. In broad terms, the role of a CPO is to:

- Create and revise policies regarding privacy and confidential information security;
- Familiarize employees with the privacy policies;
- Ensure enforcement of such policies;
- Audit and document compliance with the policies; and
- Respond to new legislative and regulatory directives.

Steven C. Bennet, *Do You Need a Chief Privacy Officer?*, The Practical Lawyer, Vol. 53, No. 1 (Feb. 2007). A CPO must have knowledge of relevant privacy and data security laws, as well as technical knowledge of the software and hardware used by the company. A CPO must also have good management skills, as a key function of the job is to coordinate activities among the various departments involved in privacy and data security matters.

Not every company can employ a full-time CPO. There are, however, several viable alternatives. Companies can:

- Create a privacy committee consisting of representatives from the departments that have particular interest in privacy and data security matters;
- Involve outside consultants that can suggest policies, conduct training and orientation, supervise or conduct periodic audits of a company's practices, and recommend improvements;

- For advice, turn to professional organizations that are dedicated to the study and development of "best practices" with regard to privacy and data security, such as Privacy & American Business and The Better Business Bureau.

Id.

D. PRACTICAL E-DISCOVERY ISSUES FOR EMPLOYERS

Studies have shown that 90 percent of business information is maintained in an electronic form. Failure to maintain all electronic information in a formal organized manner providing for easy preservation and retrieval often results in enormous e-discovery costs. Employers face such costs within two categories: 1) the financial cost of preserving, identifying, and searching the documents, and managing e-discovery; and 2) penalties imposed for failure to preserve e-discovery. *Avoiding Gotcha! Are you ready for the New Rules on Preserving Electronic Information?, available at* http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1069, *last accessed* Aug. 10, 2007.

1. Recent Amendments to Federal Rules of Civil Procedure

The new Federal Rules of Civil Procedure regarding electronic discovery that went into effect December 1, 2006 encourage employers to implement practical electronic information retention policies as well as effective litigation hold procedures, and to conduct employee training to ensure policy compliance. The Federal Rules amendments address six key points by:

- Defining a new form of information covered by discovery called Electronically Stored Information (ESI), which a party must preserve and consider in discovery;

- Requiring parties to discuss electronic discovery issues during the initial case planning conference;
- Providing that ESI will be produced as it is "ordinarily maintained or reasonably usable absent agreement to the contrary;
- Creating a limited exception to discovery, when ESI is "not accessible because of undue burden or cost;"
- Establishing a safe harbor from sanctions where a party fails to preserve ESI as a result of the routine, good-faith operation of its electronic information systems; and
- Adding protection in case of inadvertently disclosed privileged information contained in ESI.

Id. Although these rules apply to federal cases only, they will apply in the states which have adopted federal rules as governing their state's civil procedure. Additionally, the new federal rules will serve as a model for the remaining states in revising their own rules. Id.

As e-discovery issues in employment cases become increasingly prevalent, it is important for employers to review their electronic document retention policies. Individuals and businesses alike must be aware of the court's expectations and their obligations regarding electronically stored data. Businesses should have a "go to" computer expert either employed or regularly consulted so that someone knows what systems exist and how they are configured. This information, moreover, should be reduced to writing. The new rules make the development of a records retention policy imperative. If a dispute arises and information is lost because backed up information is destroyed, dire consequences could

result.[4] Similarly, information that no longer exists because it was written over pursuant to a reasonable, written policy will protect a party from sanctions.

To ensure compliance with the new rules and to reduce the cost of e-discovery, it is suggested that employers accomplish the following:

- Review and update technology use/electronic communications policies to ensure they are tailored to the company in terms of operations, technology advancement and culture;

- Establish and follow an electronic information retention and destruction policy:

- Establish a formalized litigation hold procedure (e.g., records of team meetings, records of actions by relevant custodians to suspend the destruction of relevant electronic and paper information, written communications to relevant employees to preserve information, records of what evidence has been preserved, and cessation of the litigation hold when litigation no longer is anticipated);

- Include electronic information retention policies in employee manuals and distribute it periodically throughout an organization through email reminders;

- Provide workplace training specifically to address technology/electronic communications and electronic information retention policies; and

- Audit the company's practices routinely to verify that it is complying with information retention policies and litigation hold procedures. An audit of backup tapes can be particularly cost effective.

Avoiding Gotcha! Are you ready for the New Rules on Preserving Electronic Information?, available at http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1069, *last accessed* Aug. 10, 2007.

---

[4] Courts are imposing sanctions upon litigants and their counsel for e-discovery abuses, such as negative jury inferences, attorneys' fee awards and dismissal of claims. Joseph P. Lang and James Baffa, *Electronic Discovery: an Overview and Practical Pointers*, *available at* http://www.batescarey.com/newsandarticles/electronicdiscovery_print.asp, *last accessed* Aug. 10, 2007. See also Tara Daub and Christopher Gegwich, *E-Discovery: the New Federal Rules of Civil Procedure*, *available at* http://www.nixonpeabody.com/publications_detail3.asp? ID=1729, *last accessed* Aug.10, 2007.

Cases of Interest:

- Arthur Andersen LLP v. United States, 544 U.S. 696 (2005) (holding conviction for withholding testimony or destroying records to be used in official proceeding requires proof of consciousness of wrongdoing).

- Galvin v. Gillette Co., Nos. 051453BLS, 051543BLS, 2005 WL 1476895 (Mass. Super. May 19, 2005) (refusing to permit vendor to search all e-mail, servers, archives, discs, back-up tapes all hard drives and other databases to investigate and accomplish retrieval, preservation and copying of certain documents due to magnitude of such undertaking).

2. E-discovery and Web-mail Subpoenas

Noah Shaeffer's recent article, "Web-Mail Subpoenas Complicate E-Discovery" that appeared in the July 9, 2007 issue of Massachusetts Lawyers Weekly, addresses controversial issues arising in connection with electronic discovery. The use of electronic discovery has become increasingly controversial with the growing use of such web-based mail services like Hotmail, Yahoo! Mail, and Google's Gmail for both business and personal purposes. For example, requests in civil lawsuits for electronic discovery of e-mail messages create a dispute over whether the web-based mail services must respond to subpoenas for all e-mails sent and received by a party's personal email accounts. People frequently use the web-mail providers for both business and personal correspondence, yet many attorneys believe that unrelated personal e-mails should not be discoverable.

While certain regulations (e.g., Sarbane-Oxley) require businesses to retain old e-mails on their servers for specified periods of time, it is much more difficult to get messages from a web-based account because for example, web-based service providers do not keep deleted e-mails in the system for very long. Moreover, even if the web-based providers had back up tapes of deleted e-mails, it could be a lengthy and expensive process

to review them. Therefore, web-based services tend to strongly oppose the subpoenas both in the case of active and deleted e-mails.

Nevertheless, certain providers have very strict compliance protocols and adopt a policy of producing the requested e-mails if the user, after being notified of the document request, fails to respond directly to the litigant. Certain issues arise in this respect, such as whether parties really understand the implications of such a notice, which may lead to the emails being produced without the account holder's permission. Furthermore, production of personal e-mails may also violate privacy and attorney-client privilege rights.

Parties do have an option to file a motion to quash under the Electronic Communications Privacy Act ("ECPA"). The Act forbids parties from accessing or distributing e-mail messages without the account holder's permission. A recent California Appeals Court case, *O'Grady v. Superior Court*[5], established that the ECPA applies to discovery in both criminal and civil cases. This may mean that a litigant can not circumvent the subscriber, go to the Internet Service Provider and get e-mails from them without the subscriber's consent.

In light of the controversy surrounding the issue of e-discovery in the web-based provider contexts, parties and their attorneys should proceed with caution treating subpoenas to web-mail providers as any other third-party subpoena. To avoid disclosure of correspondence to unintended recipients, individuals should avoid mixing business and personal e-mail correspondence and create separate e-mail accounts. Additionally, they

[5] 139 Cal. App. 4th 1423 (Cal. Ct. App. 2006).

should familiarize themselves with their web-mail services' policy on handling document subpoenas.

APPENDIX

I. Cases

II. Federal Statutes and Regulations

III. Massachusetts Statutes, Rules & Regulations

IV. Other Materials