VEDDER PRICE

eDiscovery Update

May 2007

Most Organizations Have Not Taken Appropriate Steps to Manage Risks Posed by E-mails

It is well established that companies must take steps to safeguard potentially relevant evidence when litigation is reasonably foreseeable. As numerous, well-publicized decisions demonstrate, many companies are still struggling with developing policies and procedures to comply with this obligation. Now that the Amendments to the Federal Rules of Civil Procedure pertaining to eDiscovery are in effect, there is no question that electronically stored information such as E-mail is subject to the same preservation and production duties as paper records. Yet most companies have avoided managing E-mail in the same way as other business records.

The Dangers of an Outdated or Ineffective E-mail Retention Program

Companies largely fall into two camps with respect to E-mail retention. Either they have retained all E-mail on backup tapes and diskettes (i.e., the "Save Everything Approach"), or they dispose of all E-mails, regardless of content, after the passage of an arbitrary period (i.e., the "Save Nothing Approach"). Both approaches expose companies to significant risk. Indeed, as demonstrated in recent litigation, opting to retain E-mails and other electronic documents indefinitely is an inadequate policy for several reasons. First, it is costly and takes up massive physical and electronic server space. Second, storing too much information on corporate servers can overburden and destabilize them, with a result of a possible loss of information. Third, reviewing an unnecessarily vast number of eRecords during discovery increases attorney review time and, consequently, litigation costs. Moreover, maintaining E-mail indefinitely greatly increases the chance that a company may be found liable during litigation because it is forced to turn over a "smoking gun" document it was not required to maintain in the first place. Recent tobacco and asbestos litigation provides examples of this last point.

If your company follows the "Save Nothing Approach," it is likely disposing of records it is otherwise obligated to retain. Regardless of which approach your company follows, most companies allow their employees to store E-mail off-line or on local hard drives, meaning that the company is retaining these records anyway, and has lost control over some corporate records. If this is the case, it is likely that your company is not adequately searching all repositories where relevant E-mails are stored when responding to discovery requests. This lack of control

In This Issue

could also result in an atmosphere where your E-mail management program is called into doubt.

As recent news reports involving the Congressional investigation into the Justice Department's dismissal of certain federal prosecutors, the White House was criticized for its failure to properly retain and disclose relevant E-mails. According to press accounts, White House officials stated that political advisers to President Bush may have improperly used their political E-mail accounts to conduct official business, and some communications required to be retained under federal law may have been improperly deleted. Having initiated an inquiry of its own, the Bush administration concluded that its policy governing political E-mail accounts was unclear, that it had not been aggressive enough in monitoring off-line use of E-mail, and that some people who had used the private accounts did not follow the policy.[1] As noted above, most companies have inadequate controls over their employees' E-mail usage, creating myriad risks for those companies.

Your Company Must Retain Record E-mails for the Periods Required under Law

Building a lawfully compliant and legally defensible E-mail management program is the first step in minimizing your company's litigation risk and improving its operational efficiency. There are three primary aspects to building and implementing such a program. First, your company should develop an E-mail management program that requires the retention of electronic records that constitute business records. This should be handled in a consistent, systematic and reliable manner, so they can be promptly retrieved when required for legal, regulatory or operational reasons. Second, your company should dispose of stale electronic records as soon as it is legally permissible to do so. Third, your company must develop a litigation hold program that is tailored to its unique litigation environment and that extends to electronic communications. Fourth, your company must disavow the use of pst. files and desktop E-mail archiving, so as to prevent its employees from having discretionary control over the retention and disposition of the E-mails they generate.

What Steps Can Your Company Take to Avoid the Problems Associated with the "Save Everything" and "Save Nothing" Approaches?

Retain Only Record E-mails

Companies are obligated by law to retain only record E-mails. Record E-mails document a specific business-related activity; demonstrate a specific business transaction; identify individuals who participated in a business activity; support facts of a particular business-related event, activity or transaction; or are needed for other specific legal, accounting, business or compliance reasons. Record E-mails must be maintained in accordance with your company's records retention schedule.

In contrast, companies are not required to retain transitory E-mails, such as routine administrative messages, information-only copies of memoranda or notes, company-wide announcements and updates, or unsolicited vendor bids. Disposing of transitory E-mails after a short period (i.e., 30 or 60 days) will reduce the volume of information your company must manage and thus reduce its storage costs and the amount of time outside counsel must spend reviewing unimportant records and legacy data storage systems.

An Effective Litigation Hold Program Is Necessary

Several recent court decisions[2] demonstrate the severe sanctions companies face for destroying E-mails during litigation and underscore the necessity of extending litigation holds to E-mails.

Developing an effective litigation hold program is also an invaluable tool to demonstrate a company's good faith and reasonable efforts to comply with its pretrial discovery obligations. Where no such program exists, companies will not be given the benefit of the

doubt when their retention practices are called into question.[3] An effective litigation hold program should include:

- A policy that allows for the immediate suspension of the planned disposition of records that may relate to pending or reasonably foreseeable litigation;
- A standard notice (such as a Notice of Litigation Hold) and an acknowledgement procedure from affected employees;
- A list of company employees who should be notified of the issuance of the litigation hold;
- Specific steps and assignments for preserving backup tapes, archived E-mails;
- A method to monitor compliance with any litigation hold in effect;
- Periodic follow-ups with company employees to reiterate the litigation hold instructions; and
- A procedure for rescinding the litigation hold and resuming the disposition of records in accordance with the Company's records retention schedule.

Benefits of Proactively Managing Retention and Litigation Risks

Developing and implementing an effective and lawfully compliant E-mail management program and litigation hold procedures may allow your company to:

- avoid expending unnecessary legal fees by reducing attorney review time in connection with producing documents in discovery;
- avoid potential civil and criminal sanctions during a governmental or agency investigation by retaining necessary documents;
- comply with legal requirements to retain business records;
- avoid claims for "spoliation" of evidence before and during the litigation;
- improve operational efficiency and reduce costs associated with the unnecessary storage and maintenance of stale records;
- minimize the chance that your company will produce a "smoking gun" E-mail it was not required to keep in the first place;
- keep documents confidential and protect them from exploitation by competitors; and
- comply with newly enacted data privacy laws.

Employers May Be at Risk for Employees' Internet Usage

An employee's Internet usage, whether at home or at work, has the potential to expose the employer to legal claims, including sexual harassment, hostile work environment and defamation. Where the allegedly offensive conduct occurs on a company-provided

computer system, employers may be especially vulnerable to legal claims stemming from the behavior of their employees.

However, a recent California Court of Appeals case indicates that there are limits on an employer's responsibility for its employees' Internet usage, even where such usage occurs on a company-provided Internet platform. In *Delfino v. Agilent Technologies*,[4] plaintiffs sued Agilent Technologies for negligent and intentional infliction of emotion distress stemming from anonymous threats allegedly made to them by an Agilent employee over Agilent's computer systems. The Court of Appeals held that Agilent was immune from suit under the federal Communications Decency Act of 1996 ("CDA"), however, which encourages Internet service providers to engage in self-regulation of any offensive or illegal Internet usage by its users, and thus immunizes Internet service providers from lawsuits arising out of such conduct. According to the Court, by providing Internet access to its employees through its computer systems, Agilent qualified as a "service provider" under the CDA, and thus was immunized from claims arising out of its employees' Internet usage.

Most employers engage in some sort of monitoring of the Internet usage occurring on company-sponsored Internet servers. Despite the holding in *Agilent*, employers should be mindful that they may be at risk for legal claims arising from their employees' use of company-provided Internet usage where an employer is on notice that such conduct is taking place. In order to minimize these risks, employers should adopt a comprehensive Internet usage policy that puts its employees on notice of acceptable and unacceptable standards of conduct with respect to their Internet usage.

Liability for Data Security Breaches Expanding

On January 17, 2007, a computer hacker accessed the computer systems of TJX Companies, Inc., a parent company of T.J. Maxx, Marshall's and other retailers, and stole sensitive and confidential information communicated during customer transactions dating back to 2003. Fraudulent use of this stolen information has thus far been detected in Florida, Georgia, Louisiana, Hong Kong and Sweden. As a result of this incident, numerous class actions have been filed against TJX on behalf of consumers whose information was stolen.

In addition to the harm caused consumers, this security breach has also required banks to cancel hundreds of thousands of credit and debit card transactions. As a result, the incident spawned a class action, filed by AmeriFirst Bank on behalf of other similar banks, that is currently pending against TJX in the U.S. District Court for the District of Massachusetts. AmeriFirst alleges claims for negligence, breach of contract and negligence per se, based on the failure of TJX to adhere to the customer records privacy and data security safeguards mandated by the Gramm-Leach-Bliley Act ("GLBA"). While the GLBA does not provide for a private right of action, AmeriFirst asserted an innovative argument. This theory alleges that the GLBA and the Federal Trade Commission's rules provide for generally accepted standards of conduct, the breach of which constitutes negligence.

If this theory is accepted, it could result in added exposure and liability to financial institutions across the country. Accordingly, all companies possessing confidential consumer data will inevitably need to reevaluate their security systems to ensure that adequate safeguards are imposed to prevent similar incidents from occurring in the future. Companies should use the TJX example as motivation to assess whether they are compliant with the Payment Card Industry Data Security Standard, which requires merchants and Internet service providers to restrict access to

cardholder data,[5] as well as the Fair and Accurate Credit Transaction Act (FACTA) disposal rule, which requires that "any person who maintains or otherwise possesses consumer information for a business purpose" must take "reasonable measures" to prevent unauthorized use of discarded consumer information.[6] The FACTA disposal rule also applies to employee information, such as background checks.

For further information on Vedder Price's Records Management and eDiscovery Solutions Group, please contact Bruce A. Radke at 312/609-7689 or bradke@vedderprice.com, or Timothy J. Carroll at 312/609-7709 or tcarroll@vedderprice.com. The editors express their gratitude to Laurel Dearborn, Amy Halbrook and Jared Jodrey for their assistance in preparing these articles.

[1] Sheryl Gay Stolberg, *Advisers' E-Mail Accounts May Have Mixed Politics and Business, White House Says*, N.Y. TIMES, April 12, 2007, at A17.

[2] *See Tantivy Commc'ns, Inc. v. Lucent Tech. Inc.*, No. Civ. A. 2:04 CV 79, 2005 WL 2860976, at *4 (E.D. Tex. Nov. 1, 2005) (holding that hiding documents, misrepresenting the existence of documents, and allowing the destruction of documents is sanctionable conduct, both as to a company and its counsel); *Chan v. Triple 8 Palace, Inc.*, No. 03 Civ. 6048, 2005 WL 1925579, at *6 (S.D.N.Y. Aug. 11, 2005) (awarding sanctions, including an adverse jury instruction, where a company failed to maintain relevant documents); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432-33 (S.D.N.Y. July 20, 2004) (holding that a party must take affirmative steps to preserve documents at the outset of the litigation or whenever litigation is reasonably anticipated); *Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union*, 212 F.R.D. 178, 222 (S.D.N.Y. Jan. 28, 2003) (awarding sanctions against a company and its counsel for acting willfully and in bad faith in failing to comply with discovery to produce relevant electronic documents); *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 79-80 (S.D.N.Y. Sept. 27, 1991) (awarding monetary sanctions to company failed to make reasonable inquiry as to the disposition of records).

[3] *See*, *e.g.*, *EEOC v. Target Corp.*, 460 F.3d 946, 955 (7th Cir. 2006).

[4] 145 Cal. App. 4th 790, 791 (2006).

[5] SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA STANDARDS § 9.1 (2006), https://pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

[6] 16 C.F.R. § 682.3(a) (West 2006).

Upcoming Seminars and Webinars

May 3, 2007

ESI, Clawbacks, Cost Shifting and Disclosure: Understanding the Impact of Amended FRCP Rule 26

10:00 a.m. Pacific/1:00 p.m. Eastern
(Webcast Length: 1 hour)

Faculty: Timothy J. Carroll and Bruce A. Radke

To find out more and to register please visit www.fiosinc.com

~

May 21-23, 2007

Managing Electronic Records "MER" Conference

Westin Hotel
Chicago, Illinois

To find out more and to register please visit www.merconference.com/register/

Records Management, Electronic Communications and eDiscovery Group

Given today's legal and technological environment, many companies have reassessed their records management programs to ensure that they meet the company's operational needs as well as complying with applicable legal requirements. Companies also are examining whether their: (1) employees routinely follow existing retention schedules, (2) stale records are properly and lawfully disposed of; and (3) records are being prematurely discarded.

Vedder Price's attorneys have developed unparalleled experience and knowledge of the laws applicable to records retention, whether in hard copy or electronic form. Its records management team is comprised of attorneys dedicated to enabling its clients to develop customized, yet comprehensive, solutions to: (a) minimize litigation risks and costs; (b) increase records management efficiency; and (c) achieve compliance with all applicable governmental regulations and statutes as well as industry best practices.

The firm counsels companies with regard to all aspects of their records management and eDiscovery needs, including:

- Developing and implementing clear records retention policies designed to meet today's legal and business challenges;
- Assisting in the design and implementation of electronic communications policies covering e-mail, instant messages, voicemail and any other electronic messages sent to or received by company-owned BlackBerrys®, personal digital assistants and other similar electronic communication devices;
- Auditing existing record management programs, including identifying potential compliance gaps, and providing practical and proven recommendations for enhancing current policies and procedures;
- Designing comprehensive training programs on records management and compliance issues; and
- Conducting pre-litigation assessment of eDiscovery issues and records management, and developing comprehensive strategies for aggressively conducting and responding to eDiscovery.

Vedder Price has been at the leading edge in this rapidly evolving field by taking a proactive approach on records management and eDiscovery issues. Its vast experience includes designing and implementing enterprise-wide records retention and electronic communications policies for a Fortune 20 client, as well as counseling a large mutual fund complex and national health care association on various aspects of their records management programs.

VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

Chicago
222 North LaSalle Street
Chicago, Illinois 60601
312-609-7500
Fax: 312-609-5005

New York
1633 Broadway, 47th Floor
New York, New York 10019
212-407-7700
Fax: 212-407-7799

Washington, D.C.
875 15th Street, N.W., Suite 725
Washington, D.C. 20005
202-312-3320
Fax: 202-312-3322

New Jersey
Five Becker Farm Road
Roseland, New Jersey 07068
973-597-1100
Fax: 973-597-9607

www.vedderprice.com