Business Guide to Compliance

# Plan Now for Managing Electronic Data & Avoid Tomorrow's Legal Risks

By Cynthia L. Jackson

Baker & McKenzie

# Cynthia L. Jackson

Partner, Baker & McKenzie LLP

Cynthia L. Jackson is a partner in the Palo Alto California office of Baker & McKenzie, the largest law firm in the world with offices in 38 countries. Ms. Jackson is the author of the "Business Guide to Compliance," a booklet designed to educate business leaders on broad compliance issues, government mandates, and e-discovery requirements. She expresses her appreciation to John Raudabaugh, a partner in the Chicago office, for his contributions to portions of the employment monitoring sections, drawn from his amicus curiae brief in *The Guard Publishing Company and Eugene Newspaper Guild,* filed before the NLRB on February 9, 2007.

Ms. Jackson represents companies in litigation and counsels on both domestic and international employment issues including discrimination and harassment claims, personnel policies and implementation, employment and severance agreements, reductions in force, codes of conduct, privacy issues, corporate social responsibility, protection of confidential information and trade secrets, and employment ramifications of mergers and acquisitions.

Ms. Jackson was selected as one of the "Best Lawyers in America" and has been repeatedly designated as a "Northern California Super Lawyer." Ms. Jackson graduated with honors from both Stanford University and the University of Texas School of Law.

Cynthia L. Jackson, Attorney at Law
Baker & McKenzie LLP
660 Hansen Way, Palo Alto, California 94304, USA
Tel +1 650-856-5572  Fax +1 650-856-9299
cynthia.l.jackson@bakernet.com

# Table of Contents

# What's the Fuss About?

Proper archiving, retention, monitoring, filtering, and encryption of electronic data are no longer optional: they are imperative.

In a world where the use of electronic data is rapidly increasing, companies must find ways to manage data now so that they effectively control compliance risks. The proliferation of electronic data is both astonishing and overwhelming. Given the storage power of average computers today, even the most modest mom-and-pop business may have electronic storage capacity equivalent to 2,000 four-drawer file cabinets.[1] The task of managing electronic data is further compounded by the fact that the data is no longer just tangible pieces of paper, but rather are bytes of information that are constantly being edited, changed, and updated from different people and sources. Proper archiving, retention, monitoring, filtering, and encryption of electronic data are no longer optional: they are imperative.

Electronic data systems control and direct machinery, process financial data, manage inventory, place orders, and transmit pictures and documents. They immeasurably increase the speed of verbal and non-verbal communication. Email is the most familiar form of electronic communication, but communication components include online journals ("web logs" or "blogs"), instant messaging (IM) (in which users conduct real-time, online "chats"), conferencing webcams, document and video transfers, and broadband voice services. Such systems, however, also are subject to misuse which may harm a business. Persons may send harassing and intimidating

[1] Jason Krause, *E-Discovery Gets Real,* ABA JOURNAL, February 2007; note George L. Paul & Bruce H. Nearon, *The Discovery Revolution: A Guide to the E-Discovery Amendments to the Federal Rules of Civil Procedure,* ABA SECTION OF SCI & TECH. LAW.

By 2005, 24% of companies had email subpoenaed and 15% had gone to court over lawsuits triggered by just employee email.

messages to employees, managers, and third parties; they may download ("steal") intellectual property from companies or third parties, disparage the company, its products and services, customers, and competitors; or they may covertly transfer stolen data to remote locations or store it in the company-furnished memory. Users can display or distribute materials which courts have deemed harassing and illegal, create and post defamatory material on internet sites and blogs, and plot or even execute crimes, all from the place of business with covert use of the company's equipment.[2]

It is therefore little wonder that 86% of General Counsel in a survey conducted by the Association of Corporate Counsel (ACC) listed their main concern as "keeping track of company activities that may have legal implications".[3] By 2005, 24% of companies had email subpoenaed and 15% had gone to court over lawsuits triggered by just employee email. According to the same survey, 10% of email at work contained sexual, romantic, or pornographic content.[4] Even before the electronic discovery rules of the Federal Rules of Civil Procedure (FRCP) became effective on December 1, 2006, more than one in five companies had electronic communications subpoenaed during the course of litigation or a government investigation in 2004.[5] This figure is more than double the percentage reported in 2001.[6] In fact, U.S. firms spent 1.2 billion dollars in outside electronic discovery services in 2005.[7] That number is estimated at 1.9 billion dollars in 2006.[8] With the passage of the FRCP electronic discovery rules, one could expect such statistics to be eclipsed in short order. Surprisingly, however, in a survey conducted only two months before the FRCP amendments' effective date, only 7% of corporate counsel indicated that their companies were prepared for the amended Rules and 54% were not even aware that the amendments would take effect in December 2006.[9]

U.S. firms spent 1.2 billion dollars in outside electronic discovery services in 2005. That number is estimated at 1.9 billion dollars in 2006.

Companies must also comply with an increasing number of other laws regulating electronic communications, and new legislative proposals abound.[10] Much regulation concerns the protection of sensitive personal information, *e.g.,* Electronic Communications Privacy Act of 1986[11]; Health Insurance Portability and Accountability Act of 1996[12]; Children's Online Privacy Protection Act of 1998[13]; Gramm-Leach-Bliley Act of 1999[14]; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[15]; California Security Breach Notification Act of 2002[16]; California Security of Personal Information Act of 2004[17]; and numerous other domestic and foreign laws and regulations.[18]

[2] *Electronic Workplace: Is Your Company's Work Blogging Down?* FEDERAL EMPLOYMENT LAW INSIDER, September 2006 at 2; Michael R. Phillips, *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks,* Treasury Inspector General for Tax Administration, July 31, 2006.
[3] ACC & SERENGETI, MANAGING OUTSIDE COUNSEL SURVEY REPORT, October 23, 2006.
[4] *2006 Workplace E-mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-mail, IM & Blog Violators,* AMA, July 11, 2006, http://www.amanet.org/press/amanews/2006/blogs_2006.htm.
[5] AMA/ePolicyInstitute Research, *2004 Workplace E-mail and Instant Messaging Survey Summary,* at 1.
[6] *Id.*
[7] Sacha Consulting, Ramon Nunez, Metal INCS, Gregory McCurdy, Microsoft Corp, ABA Digital Evidence Project, The National Law Journal/www. NLJ.com, September 19, 2005.
[8] *Id.*
[9] Lexis Nexis® Applied Discovery® survey completed at the ACC 2006 Annual Meeting in October 2006.
[10] *Data Security: Federal and State Laws,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, February 3, 2006; *Data Security: Federal Legislative Approaches,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, February 9, 2006; *Obscenity and Indecency: Constitutional Principles and Federal Statutes,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, June 25, 2003.
[11] 18 U.S.C. § 101 *et seq.*
[12] 42 U.S.C. § 201 *et seq.*
[13] 15 U.S.C. § 6501 *et seq.*
[14] 15 U.S.C. §§ 6801-6809.
[15] 15 U.S.C. §§ 7701-7713.
[16] Cal. S.B. 1386 (2002) (Cal. Civ. Code §§ 1798.82 and portions of 1798.29).
[17] Cal. Civ. Code § 1798.81.5 (Cal. A.B. 1950 (2004)).
[18] Allan Holmes, *The Global State of Information Security 2006,* CIO MAGAZINE, September 15, 2006.

Unsolicited emails account for 93% of all inbound emails.

In addition to laws regulating document destruction and retention, companies must increasingly guard against hackers and loss of valuable intellectual property through electronic means.[19] The internet can expose the company's most valuable resources to third parties. In 2004, unsolicited emails accounted for 73% of all inbound emails; this was increased to 93% by 2006.[20] Most are annoyances or merely waste time, but malware or malicious logic, such as viruses, worms, downloaders, trojans, spam, link spam, phishing, and pharming endanger the company's network and the business information and intellectual property it houses.[21] Outside parties can "hack" into the company's trade secrets and confidential information, steal passwords, and redirect users to download sites. Of these attacks, 33% are reportedly generated by internal users.[22]

Forty percent of persons in a recent National Center for Supercomputing Applications (NCSA) survey said they visit social networking sites at work, thereby exposing their employer's network to hackers.[23] (68% of surveyed companies reported they had electronic crime in 2004; of those companies, 43% reported unauthorized access to information, systems or networks and 14% reported a theft of IP).[24] In fact, in recently unsealed court papers, it was disclosed that a senior DuPont scientist had downloaded, over the course of less than five months, 22,000 sensitive documents, and had transferred 180 DuPont documents to a laptop computer and then to his new employer covering DuPont's "major technologies and product lines as well as new and emerging technologies in the research and developmental stage," valued at as much as $400 million.[25]

Legal or "harmless" activities can also inflict high costs, and the temptation to engage in such "harmless" conduct is enormous. In a 2004 survey of 840 U.S. companies, 66% responded that employees spend two hours or less daily on the company's system for personal use, 24% spend two to three hours, and an additional 10% spend more than four hours.[26] The same survey reported that 75% of employees send or receive 10 or fewer personal emails daily.[27] Ninety percent of employees spend up to 90 minutes daily engaged in personal use instant messaging, 19% of them add attachments to text messaging, 16% distribute jokes, gossip, or disparaging remarks, 9% send confidential information, and 6% distribute sexual, romantic, or pornographic text in their messages.[28]

As a result of both mandatory legal requirements and voluntary best practice protection, companies must plan, implement, and train *before* a legal crisis arises. Few companies will have the luxury of first thinking about and starting to address such issues after a lawsuit is filed, the intellectual property is already "out the door," private information released, or a hostile work environment created. It is critical

[19] *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth,* CRS REPORT FOR CONGRESS, April 13, 2005.
[20] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004); W*ireless Privacy and Spam: Issues for Congress,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, December 22, 2004; *'Junk E-mail': An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam"),* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, April 15, 2003; *Cybercrooks Deliver Trouble,* WASHINGTON POST, December 27, 2006, D1.
[21] *Pharming,* WEBSENSE, INC. (2006); *The Economic Impact of Cyber-Attacks*, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, April 1, 2004.
[22] Scott Berinato, *The Global State of Information Security 2005,* PRICE WATERHOUSECOOPERS AND CIO, September 15, 2005
[23] *CA/NCSA Social Networking Study Report,* RUSSELLRESEARCH.COM, at 4, http://staysafeonline.org/features/SocialNetworkingReport.ppt.
[24] *2005 E-Crime Watch Survey—Survey Results,* CSO MAGAZINE, U.S. SECRET SERVICE, CERT COORDINATION CENTER., http://www.csoonline.com/info/ecrimesurvey05.pdf.
[25] David Kauffman, *How Safe Is Your Data?,* HR HERO LINE, March 9, 2007.
[26] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004).
[27] *Id.*
[28] *Id.*

for organizations to plan ahead. First, companies need to plan for communications retention, archiving, and monitoring. Second, they need to create encryption processes and proper access restrictions. Third, they need ongoing training and auditing of their processes and policies.



## Who Cares or Needs to Care?

Management of electronic data affects nearly everyone at a company: the General Counsel's office, Compliance Officers, Internal Auditors, Finance, IT Managers, Human Resource and Benefits Personnel, Intellectual Property and Licensing Personnel, Supply Chain Managers, Export Control, Sales, and Business Personnel.

Companies in federal court litigation or just "threatened" by such litigation must also be poised to leap into action to preserve relevant electronically stored data.

For example, U.S. publicly traded companies have a host of reporting, auditing, and transparency obligations as a result of Sarbanes-Oxley (SOX) and the recordkeeping and accounting obligations under the Foreign Corrupt Practices Act. Companies in federal court litigation or just "threatened" by such litigation must also be poised to leap into action to preserve relevant electronically stored data. Companies in banking and finance or health industries are subject to detailed laws and regulations governing collection, use, access, and dissemination of information. Those companies that operate internationally or export hardware or software products will find themselves obligated to manage their data, including encryption, in complex and sometimes conflicting manners.

But even for those companies that are not publicly traded, faced with actual or threatened litigation, engaged in particularly regulated industries or operating in the international market, the age of electronic data imposes challenges. Studies have indicated that one-third of data thefts are committed

No company is immune. Smaller and mid-cap companies should also think ahead and implement systems now.

by current employees and the overwhelming number of actionable disparagement, discrimination, and harassment allegations arise from *authorized* employee users.[29] No company is immune. Smaller and mid-cap companies should also think ahead and implement systems now to safeguards their intellectual property from "theft," protect their employees from claims of a hostile work environment, or to prepare for document destruction overrides in the event of threatened litigation.

Ironically, the same technologies that have created the data proliferation headaches may also present a solution through well designed and maintained electronic data management systems, tailored to meet the legal requirements posed by relevant laws and jurisdictions. Such electronic systems should include software systems with document retention and archiving features, document destruction overrides, encryption access restrictions when required, and monitoring, and web filtering capabilities when permitted. In addition to installing such a system, it is imperative that the proper legal parameters be identified and that personnel be trained in advance of a legal crisis to understand how to properly manage such data on a business as usual basis, so that electronic data can be quickly, properly, and easily captured and addressed when the legal need arises. Selection and implementation of electronic data management systems, creation and enforcement of policies, and ongoing personnel training and auditing to ensure that the system is in fact working *before the legal crisis arises* all require the coordinated and thoughtful collaboration of company personnel whether in the General Counsel, HR office, or elsewhere.

Selection and implementation of electronic data management systems, creation and enforcement of policies, and ongoing personnel training and auditing to ensure that the system is in fact working *before the legal crisis arises* all require the coordinated and thoughtful collaboration of company personnel.

[29] Scott Berinato, *The Global State of Information Security 2005*, PRICE WATERHOUSECOOPERS AND CIO, September 15, 2005.

## Legal Requirements to Maintain Electronic Records

Ignorance of the new amendments to the Federal Rules of Civil Procedure can be costly.

Absent a "litigation situation," there is generally no universal duty to preserve electronically stored data (or other records), although certain types of record preservation such as for tax, employment, and corporate records may be required under various federal or state laws. A "litigation situation" on the other hand will trigger information preservation obligations, requiring a company to override its normal document destruction processes. The new amendments to the FRCP codify the need for a "litigation hold" of documents the company reasonably believes are discoverable in anticipation of litigation. The "litigation hold" can be triggered long before the filing of an actual lawsuit, such as when the company receives any internal complaint to a "managing agent," a preservation letter from a potential party or attorney threatening future litigation, prelitigation correspondence, notice of an investigation by a governmental agency, subpoena or governmental request for information, or filing of an administrative charge. Once there is a "litigation situation," the company has a duty under the amendments to take affirmative steps to suspend immediately all routine document destruction and to preserve all records, including electronic data and possibly metadata therein, that it knows or reasonably should know will be relevant to the action or reasonably calculated to lead to the discovery of admissible evidence.

The company was ordered to pay costs and the plaintiff's attorney's fees where the company failed to suspend its email and data destruction policy and preserve relevant documents from time of the *internal employee complaint* regarding sexually harassing behavior.

Even before the recent amendments to the FRCP, courts have had little patience with companies that failed to preserve data when they knew or should have known of impending legal challenge. In *Broccoli v. Echostar Communications Corp,* 229 F.R.D. 506 (D.C. Md. 2005), the court held that the employer had a duty to preserve electronic documents 11 months before the plaintiff/employee's termination. Such duty arose because the future plaintiff had sent his employer verbal and email complaints alleging sexually harassing behavior. The company was ordered to pay costs and the plaintiff's attorney's fees where the company failed to suspend its email and data destruction policy and preserve relevant documents from time of the *internal employee complaint* regarding sexually harassing behavior.

In a series of cases, *Zubulake v. UBS Warburg LLS,* 220 FRD 212 (S.D. N.Y. 2004), 229 F.R.D. 422 (S.D. N.Y. July 20, 2004 Zubulake II), and 231 FRD 159 (S.D.N.Y. February, 3, 2005 Zubulake III), the court held that the company had a duty to preserve electronic documents four months before the plaintiff had even filed a charge of discrimination (and 10 months before she filed a federal court action) because the company knew or should have known that its document destruction policy would result in relevant document destruction. In *Zubulake,* the court found that the defendant's network back up tapes were a likely source of relevant evidence, but that employees outside the legal department took it upon themselves to delete relevant documents which the defendant later recovered through expensive metadata recovery.

In *Wiginton v. CB Richard Ellis,* 229 F.R.D. 568 (N.D. Ill. 2003), the court held that the company had been put on notice of a "class action" by just a letter from the plaintiff's counsel identifying documents and multiple alleged harassers days after the lawsuit had been filed. Specifically, the court held that the company had a duty to preserve computer hard drives, email accounts, and internet records of anyone who had been accused of sexual harassment or who was involved in the case. In addition, the court permitted the plaintiff to renew a motion for sanctions for failure to retain electronic data relating to plaintiff and ten alleged harassers if relevant missing electronic documents were found on back-up tapes of company. In *Consolidated Aluminum Corp v. Alcoa, Inc.,* 2006 U.S. Dist. LEXIS 66642 at *18 (M.D.La. 2006), the court ordered Alcoa to pay for the re-deposition of all "key-players" and for costs and fees of bringing the motion and investigating discovery shortfalls because Alcoa waited approximately two and a half years after it had sent its own demand letter to Consolidated Aluminum before suspending its own routine document destruction policy. In *Samsung Elecs. Co. v. Rambus, Inc.,* 2006 U.S. Dist. LEXIS 50007 (E.D.Va. 2006), defendant and cross-complainant Rambus had contemplated litigation by identifying its most likely litigation target, its possible legal theories and relevant documents for both preservation and destruction before it had initiated its "shred day." Having concluded that Rambus had improperly

destroyed relevant data, the court indicated that it would impose discovery sanctions. Rambus in turn voluntarily dismissed their cross-complaint before the court imposed sanctions.

The consequences of failing to override information destruction systems and institute a litigation hold immediately are staggering. In *Zubulake,* the Court not only ordered the defendant to pay discovery costs but also even more critically, the court issued an "adverse inference instruction" to the jury. Specifically, the court ruled that the jury could infer that the destroyed documents would have assisted the plaintiffs in their discrimination claim because documents were not retained after the date of the EEOC charge, filed ten months before any lawsuit. The jury in turn slapped the defendant with a $29 million verdict. In *United States v. Philip Morris USA Inc.,* 327 F. Supp. 2d 21 (D.D.C. 2004), the court sanctioned Phillip Morris $2.75 million dollars based upon $250,000 in sanctions multiplied by the eleven managers who failed to comply with the company's record retention policies. In addition, the court precluded all eleven managers who failed to comply with the retention policy from testifying at trial regarding defenses to the claims. In *Krumwiede v. Brighton Associates LLC,* 2006 U.S. Dist. LEXIS 31669 (N.D. Ill. 2006), the court entered default judgment when the plaintiff/cross-defendant failed to put a litigation hold on a laptop and continued to delete, alter, modify, and access files before turning



the laptop over to a forensic examiner because the metadata had been altered through continued use even though it had not been entirely deleted. In *Dempsey v. Pfizer,* 813 S.W. 2d 205 (1991), the Texas court dismissed a $42,000,000 claim as a sanction for document destruction.[30]

In addition to monetary sanctions, courts have also imposed tort liability for spoliation of evidence and criminal sanctions.

In addition to monetary sanctions and adverse inference instructions painfully demonstrated by the cases above, courts have also imposed tort liability for spoliation of evidence and criminal sanctions. Frank Quattrone, a former high tech investment banker at Credit Suisse First Boston was permanently barred from the securities industry and fined $30,000 by the NASD. Previously, he was convicted of obstruction of justice and sentenced to 18 months imprisonment for sending an email to others in his group about "cleaning up their files" during an SEC investigation.

As the cases above demonstrate, the FRCP codify what many federal courts,[31] and some state courts have been ordering for several years. But the amendments to the FRCP also impacts litigants in at least two other fundamental ways: 1) it expressly addresses electronic discovery and mandates parties and their attorneys to investigate, preserve, produce, and respond regarding electronic data, leaving no further lingering question whether electronic data is implicated; and 2) it mandates adverse parties to expressly discuss and cooperate with each other

[30] Nor were these cases, all decided prior to the FRCP amendments, aberrational. In *In Re Quintus Corp. v. Avaya, Inc.* 2006 Bank. LEXIS 2912 (Bank. D. De. 2006), the court entered judgment in the amount of $1.88 million based upon its finding of deliberate and prejudicial destruction of evidence which the defendant was required to keep pursuant to regulations and in anticipation of litigation. In *In 3M Innovation Properties C. v. Tomar Electronics, Inc.,* 2006 U.S. Dist. LEXIS 80571 (D. Minn 2006), the court issued an adverse inference because the defendant did not institute a litigation hold. In *In Re Napster,* 462 F.Supp.2d 1060, 1077-78 (N.D. Cal. 2006), the defendant's failure to timely initiate a litigation hold caused the court to order an adverse inference instruction. In *In Re NTL, Inc. Sec. Litig.* 2007 U.S. Dist LEXIS 9110 (S.D.N.Y. 2007), the court held that the corporation newly formed after bankruptcy did not preserve documents, warranting an adverse inference instruction and monetary sanctions. In December 2006, the National Association of Securities Dealers (NASD) alleged that Morgan Stanley falsely represented that millions of emails were lost in the World Trade Center 9/11 attack. That case is still pending.

[31] In August 2006, a judicial conference of state judges approved "*Guidelines for State Trial Courts Regarding Discovery of*

The FRCP mandates adverse parties to expressly discuss and cooperate with each other about electronic data from the outset and throughout the litigation.

about electronic data from the outset and throughout the litigation. Parties will be required to "meet and confer" generally within the first few months of litigation about the preservation of discoverable information, the form in which electronic information will be produced (*e.g.* PDF, Tagged Image File Format (TIFF), "native" format, paper, etc.), whether a party asserts the data is "inaccessible," and how they anticipate dealing with "unduly costly or burdensome" data retrieval and the handling of inadvertent production of attorney-client, trade secret, or other privileged or protected information that might be buried in produced electronic or paper documents under Rule 16 (b) and 26. Unless a party has implemented and understands its document retention policies and practices before a lawsuit is filed, it could be placed at a distinct disadvantage at the mandatory "meet and confer" conference to those parties who have planned ahead and therefore know what proposals are most beneficial to them.

The amended Rules also expressly address the role of electronic data when parties are required to answer written questions (interrogatories) or physically produce documents. For instance, FRCP 33 (d) allows the answering party to specify that the responsive information is in "business records, including electronically stored information" if (i) the answers can be ascertained from such records, (ii) the burden of ascertaining the information is essentially the same for both parties, and (iii) the records are specified. Amended FRCP 34 now expressly allows for a party to specify the desired

*Electronically-Stored Information."* These guidelines, however have no binding effect unless and until they are adopted by the states. To date, Massachusetts and N. Carolina are considering adoption of the State Guidelines. In contrast, on September 1, 2006, New Jersey adopted state electronic discovery rules modeled after the FRCP. Arizona, Florida, Idaho, Maryland, and New Hampshire are also considering rules similar to the amended FRCP. The fact that similar but different electronic discovery rules are emerging among the states further highlights the need that any electronic data management system be facile enough to address both the widespread rules relating to electronic discovery and the subtle differences.



form of production of electronic information (paper or electronic), although absent agreement or a court order, the amended rules presume that electronically stored data will be produced in the form in which it is "ordinarily maintained" or in a reasonably usable form.

One can anticipate that the form of electronic production will be a hotbed of dispute today and for many years going forward.

One can anticipate that the form of electronic production will be a hotbed of dispute today and for many years going forward. Some have argued that the "manner in which it is ordinarily maintained," will require "native file" production. Others object because "native form" will not allow privileged or protected information to be easily removed or to control number the produced documents. Some courts and parties have taken the position that documents must be produced with all their metadata. *Williams v. Sprint/United Management Company,* 230 FRD 640 (D. Kan. 2005); *D.E. Tech v. Dell Inc.,* 2006 U.S. Dist. LEXIS 87902 (W.D. Va. 2006); *Nova Measuring Instruments v. Nanometrics Inc.* 2006 U.S. Dist. LEXIS 49156 (N.D. Cal. 2006); In *Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation,* 2007 U.S. Dist. LEXIS 2650 (E.D. N.Y. 2007). Increasingly, however, courts and others take the position that the presumption should be against production of metadata. *Kentucky Speedway v. National Association of Stock Car Auto Racing Inc.,* 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 2006); *Wyeth v. Impax Laboratories Inc.,* 2006 U.S. Dist. LEXIS 79761 (D. Del. 2006); *The Ponka Tribe of Indians of Oklahoma v. Continental Carbon Co.,* 2006 U.S. Dist. LEXIS 74225 (W.D. Okla. 2006). In fact, the ABA issued a formal opinion 06-442

in 2006 which puts the burden upon the lawyer sending potential protected metadata to "scrub" the metadata or send a different version of the document without metadata to avoid the likelihood of inadvertent production of privileged or otherwise protected metadata. Florida's and Maryland's State Bars have imposed similar obligations on counsel to "scrub" protected metadata before production. However the courts and the State Bars ultimately sort out the debate of metadata, one thing is clear: Companies and their lawyers must understand how their electronic information is stored and what metadata if any is included, before production, and are well advised to be prepared to address such issues well before the federal court mandatory "meet and confer" conference.

Amended Rule 37 also allows for a limited "safe harbor" from discovery sanctions for failure to produce electronically stored data, if such data is lost as a result of routine operation of an electronic information system and the operation is in good faith. As noted above, however, a court is unlikely to find such good faith if a party fails to timely impose a "litigation hold." The retention issues go beyond the mainframe to include back-up tapes, hard drives, laptops, and other electronic depositories. Such matters are not nearly as clear as they might seem at first blush. Does your company use PDA's such as BlackBerry's? Are any emails stored only on them and not the company's servers? Do employees print and retain hard copies of documents even though they are periodically purged electronically, and do you know where these copies are kept? Do any employees access bulletin boards, IM programs, or personal email at work, of which your company's electronic managed system might have retained a copy? Does the company keep track of how often it destroys or overwrites electronic data, and can those systems be halted as to specific types of data based on search terms (such as the potential plaintiff's name, job title, or product purchased)? Does your company have clearly communicated policies regarding which emails are saved in personal folders in company computers, and are those policies routinely followed by employees? Does the company know what metadata is on its computers?

An effective electronic data management system needs to address each of these issues well in advance of litigation to ensure that once the "litigation situation" presents itself, a company can immediately identify and preserve all relevant data in whatever form it takes.

An effective electronic data management system needs to address each of these issues well in advance of litigation to ensure that once the "litigation situation" presents itself, a company can immediately identify and preserve all relevant data in whatever form it takes.[32] The electronic data affected by the litigation hold should include not only documents that were created by the person about whom the potential litigation apparently would focus, but also any documents to or about such person, and in the case of possible disparate treatment discrimination or class action claims, any persons in similar circumstances.

[32] Allen Smith, *Amended Federal Rules Define Duty to Preserve Work E-mails*, HR NEWS, December 1, 2006.

## Hostile Free Work Environment

In the United States,[33] it has become almost a given that proper filters and employee monitoring is a best practice in preventing hostile work environment claims. "The suggestion that filters are needed to avoid liability appears to have become conventional wisdom."[34] "Many of the email harassment cases could have been prevented if filters had been used because the email would not have been sent."[35]

Many of the email harassment cases could have been prevented if filters had been used because the email would not have been sent.

As the statistics suggest and even the most cursory review of hostile work environment cases demonstrate, electronic mail systems have been the source of innumerable discrimination and harassment complaints. *EEOC v. Freddie Mac,* Civ. No. 97-1157-A, at 3-4 (E.D. Va. July 24, 1997) (claim filed and pending for at least three years regarding derogatory electronic messages about "ebonics" circulated in the workplace. The employer had a duty to "take prompt and effective remedial action to eradicate.") *Olivant v. Dept. of Environmental Protection,* 1999 WL 430770 (N.J. Admin. Apr. 12) (distribution of sexist "humor" over electronic mail systems constitutes sexual harassment.); *Trout v. City of Akron* (Complaint No. CV-97-115879 (filed Nov. 17, 1997); Verdict, *id.* (Dec. 15, 1998)); $260,000 judgment against the City based on co-workers viewing pornographic materials on their computers. In contrast, in *Delfino v. Agilent,* 145 Cal. App.4th 790 (6th Dist., 2006), the court found no company liability for an employee's use of the employer's computer system to send

[33] On an international basis, monitoring is subject to varying restrictions and prohibitions. This paper is premised primarily on the U.S. process, although as noted in Section VIII, below, even more sophisticated data management is necessary in order to ensure compliance with multiple non-U.S. jurisdiction's requirements.
[34] Eugene Volokh, Professor of Law UCLA, *Freedom of Speech, Cyberspace: Harassment Law and the Clinton Administration,* 63 LAW & CONTEMP. PROBS. 299 (2000).
[35] Wendy R. Leibowitz, *Avoiding E-mail Horror Stories: Policies and Filters the Best Defense,* N.Y. L.J., December 15, 1998, at 5.

threatening messages over the internet because the company took prompt action when it learned of the misconduct. In addition, federal law regulates child pornography which it treats as "contraband," making it illegal to handle, possess, distribute, etc. such material under 18 USC 2251 et al. Indeed, a company is under a legal obligation to report any such known use of such material to the FBI immediately or it risks its own violation of child pornography laws.

To defend and protect against abuses, increasingly companies in the U.S. are using screening devices or filters. A U.S. employer's failure to monitor electronic communications from and entry into its equipment can result in significant liability. Accordingly, U.S. employers should inform U.S. employees that computers are the employer's property, that they exist for business purposes, that communications are subject to monitoring at any time, and that employees should have no expectation of privacy in the use of a job-related personal computer.[36]

Furthermore, courts are becoming increasingly fond of filtering as the least restrictive means of protecting persons from offensive internet content. For example, on March 22, 2007, a district court in Pennsylvania struck down the Child Online Protection Act[37] as unconstitutional in part because filters were a less restrictive means of preventing children from accessing offensive content on the internet than the ways Congress required in the statute.[38] The court found that filters "generally block about 95% of sexually explicit material."[39] They are also "fully customizable and may be set for different ages and for different categorizes of speech or may be disabled altogether…"[40]

In the face of increased regulation, litigation, and the costs of avoidable error, companies are using workplace policies, in addition to technology, to manage productivity, protect resources, and motivate employee compliance. Reportedly, 80% or more of U.S. companies inform workers that it monitors content, keystrokes and time spent at the keyboard; 76% monitor employees' website activity; 65% block connections to inappropriate websites; 82% make clear that the company stores and reviews computer files; 86% alert employees to email monitoring; and 89% notify employees that their web usage is being tracked.[41] In 2005, reportedly 84% of U.S. companies had established policies governing personal email use, 81% had policies governing Internet use, 42% had in place policies regarding personal instant messaging, 34% addressed the operation of personal websites on company time, 23% had policies regarding personal postings on corporate blogs, and 20% of corporate policies restricted the operation of personal blogs on company time.[42] In the same year, 26% of employers acknowledged firing workers for misusing the internet and 25% terminated employees for email misuse.[43]

In the face of increased regulation, litigation, and the costs of avoidable error, companies are using workplace policies, in addition to technology, to manage productivity, protect resources, and motivate employee compliance.

[36] *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy,* 2001 DUKE L. & TECH. REV. 0026 (2001).
[37] 47 U.S.C. § 231.
[38] *ACLU v. Gonzales,* No. 98-5591 (E.D. Pa. March 22, 2007).
[39] *Id.*
[40] *Id.*
[41] AMA/ePolicy Institute Research, *2005 Electronic Monitoring & Surveillance Survey,* (2005).
[42] *Id.*
[43] *Id.*

## Protecting Intellectual Property is Fundamental to a Successful Enterprise

Email volume is growing 30% per year and contains as much as 80% of a company's intellectual property.

Email volume is growing 30% per year and contains as much as 80% of a company's intellectual property.[44] The potential for disaster is no longer academic. In *Sonoco Products v. Johnson,* 23 P.3d 1287 (Co. App. 2001), the company was awarded almost $7 million in a trade secret misappropriation action where the former employee and new employer conspired to use electronic and physical proprietary information of Sonoco stolen by an employee.[45]

Courts have not only found the employee who absconded with the electronic data liable, but also have found the new employer liable. In *Shurgard Storage v. Safeguard Self-Storage,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000), the plaintiff stated a claim against a subsequent employer under the Computer Fraud and Abuse Act where a former employee of plaintiff used its computers to email proprietary information of the plaintiff to the defendant company, who then hired the employee. In *Charles Schwab v. Carter,* 2005 U.S. LEXIS 21348, no. 04-C-7071 (N.D. Ill. Sept. 27, 2005), the court found that plaintiff successfully pled a cause of action against a former employee's new employer under the Computer Fraud and Abuse Act under a theory of vicariously liability. While the employee was working for plaintiff Schwab, he emailed proprietary information of Schwab to his subsequent employer, Acorn. Schwab alleged that Acorn urged the employee to

[44] Frank Chambers, *EDD Tips for Email from the Front Line,* LAW TECHNOLOGY TODAY, March 2007.
[45] *See also, Sawyer v. Dept. of Air Force,* MSPB 1986, 31 MSPR 193; *US v. Middleton,* 35 F. Supp. 2d 1189 (N.D. Cal. 1999); *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001); *Pacific Aerospace Electronics Inv. v. Taylor,* 295 F. Supp. 2d 1188 (E.D. Wa. 2003).

access Schwab's computer system beyond his authorization.

In *Lowry's Reports v. Legg Mason,* 271 F. Supp. 2d 737 (D. Md. 2003), an employee circulated and reprinted copyrighted material within the workplace. The court noted that it was irrelevant that the employer did not know about the employee's continuing bad acts (after the employer asked the employee to cease the distribution of the copyrighted material). The jury returned a $20 million verdict.[46]

Each of these cases demonstrate that had the U.S. company/victim monitored outgoing proprietary information and had trapped or filtered unauthorized sending of such information, it could have avoided not only years of litigation but also loss of its proprietary information in the first instance. After all, attempting to put the proprietary "toothpaste back into the tube" is rarely successful, with or without a court victory.

[46] Motion for new trial and judgment as a matter of law were denied at *Lowry's Reports, Inc. v. Legg Mason, Inc.,* 302 F. Supp. 2d 455, 461 (D. Md. 2004).



## Privacy: When TMI (Too Much Information) is a Bad Thing[47]

Unlike countries in the European Union (EU) and in some other regions of the world, the U.S. does not have a comprehensive data privacy scheme. Rather the U.S. tends to address data privacy issues on a sectoral or industry basis with discrete laws pertaining to creation, retention, use, and access of personal privacy data. In contrast to the record retention focus of the FRCP, or monitoring lessons from hostile work environment or Computer Fraud and Abuse Act cases, privacy laws regulate and restrict the data that a company is able to collect, process, transfer, retain, use, or disseminate. As a result, it is important that an effective information management systems not only have the ability to retain and archive data when necessary and to monitor within the U.S. when possible, but also the systems should have the ability to restrict and limit the use of and access to privacy information that is imparted to the company for only limited, expressed purposes.

For instance, Gramm-Leach-Bliley Act regulates financial institutions, including businesses engaged in banking, insuring, stocks and bonds, financial advice, and investing. It provides limited privacy protections against the sale of private financial information, codifies protection against "pre-texting" to obtain personal financial information through false pretenses, and allows consumers the right to opt out from limited "nonpublic personal information"

[47] For further information regarding not just U.S. but also global data privacy, see Baker & McKenzie *Global Privacy Handbook* (International Association of Privacy Professionals) ©2006.

HIPAA addresses the collection, use, and access of health related information for "covered entities" defined as health plans, health care clearing houses, and health care providers who transmit health information.

sharing. It also requires financial institutions to maintain information security programs that meet certain criteria specified by their regulatory authority, such as the Federal Trade Commission's Standards for Safeguarding Customer Information.

The Fair Credit Reporting Act (and many similar state laws) primarily governs the use and disclosure of information in "consumer reports" by "consumer reporting agencies" which is broadly defined. It contains restrictions on the collection, use, and disclosure of medical, financial, and court proceedings as well as special restrictions related to identity theft, consumer reports for employment purposes, and "investigatory consumer reports" with third parties. The Act contains numerous requirements for consumer reporting agencies as well as users of consumer reports to safeguard data integrity and accuracy of the data collected and disseminated, as well as internet access, use, and safe disposal of information derived from consumer reports.

Health Insurance Portability and Accountability Act (HIPAA) addresses the collection, use, and access of health related information for "covered entities" defined as health plans, health care clearing houses, and health care providers who transmit health information. The HIPAA regulations govern among other things the use and disclosure of protected health information maintained in any format. A covered entity must appoint a data officer who is generally responsible for the implementation and enforcement of policies and practices required by



HIPAA and is charged with record retention for six years. Covered entities must also comply with the separate Security Standards for the Protection of Electronic Protected Health Information, 45 CFR 160 and 164. In January of 2007, the U.S. Department of Justice announced the first case it has brought under HIPAA involving the prosecution of medical identity theft including 1,130 electronic records from the Cleveland Clinic. A Clinic employee allegedly used the Clinic's computer system to collect and sell patient records to an organized crime ring which used the patient records to fraudulently bill Medicare $7 million. Various state laws also address and control health care data such as California's Confidentiality of Medical Information Act.[48]

The HIPAA regulations govern among other things the use and disclosure of protected health information maintained in any format.

Numerous states also have express statutes protecting the confidentiality of social security numbers. For instance, California Civil Code section 1798.85 prohibits, among other things, requiring an individual to transmit his or her social security number over the internet unless the connection is secure or the social security number is encrypted. California Civil Code section 1798.81.5 requires businesses to maintain reasonable security procedures to protect a broad range of personal information, including social security numbers, credit card and bank account numbers, drivers license numbers, and more. New York has a similar law regulating the destruction of documents containing personal information, such as a person's social security number.[49]

Companies need to carefully select electronic data

[48] In a recent survey, 98.5% responded that medical organizations have responsibility for securing patients' medical records but less than 40% felt confident that their healthcare providers in fact secured their medical information. Virtually everyone responding believed medical organizations have a legal responsibility to alert patients if someone had accessed medical records without patient consent yet 7 out of 10 did not believe that healthcare providers were diligent about informing patients of suspected security breaches. www.epictide.com.

[49] NY CLS Gen. Bus. §399-h (2007).

Violations of U.S. and state data privacy laws not only often carry criminal penalties, but also impugn the integrity of a company's business and its brand. Once again, planning ahead to avoid the breach is far preferable than simply attempting to repair the damage thereafter.

management systems to address the quickly expanding regimes of data privacy protections. The doctor and the banker both need encryption features to ensure that confidential information, whether it is diagnostic or financial, are safeguarded from inadvertent disclosure. Firewalls and limited access must be installed to avoid unauthorized or overbroad dissemination. Monitoring ability must exist so that if a security breach is detected, proper notice and remedial measure can be taken immediately. Violations of U.S. and state data privacy laws not only often carry criminal penalties, but also impugn the integrity of a company's business and its brand. Once again, planning ahead to avoid the breach is far preferable than simply attempting to repair the damage thereafter.



## Encryption

Encryption is a vital, yet all too often underused technology. "Data encryption is defined as the process of scrambling transmitted or stored information making it unintelligible until it is unscrambled by the intended recipient."[50] It is virtually essential to protect trade secrets and confidential information that may be sent over the internet.

Without having in place encryption capabilities, a company is leaving its secrets out in the open. "In the security world, 2005 will be remembered as the year in which data leakage became a front-page story, spurred mainly by new U.S. laws mandating public disclosure when customer data is stolen or lost."[51] What's even more frightening is that employees with access to confidential data of their employer either aren't prioritizing data security or are unfamiliar with how to use it. In the seminal article, "Why Johnny Can't Encrypt,"[52] two researchers at Carnegie Mellon University discovered that the average, educated, email proficient user did not know how to use encryption technology. The follow up study, "Why Johnny Still Can't Encrypt"[53] found little improvement. Companies must take proactive steps to acquire user friendly encryption systems that match their security needs, and then train employees on how to use the technology.

Data storage systems storing unencrypted information expose companies to risks of hackers stealing

[50] Fred Moore, *Preparing for Encryption: New Threats, Legal Requirements Boost Need for Encrypted Data*, COMPUTER TECHNOLOGY REVIEW, August-September 2005.
[51] Kevin Murphy, *Email Security Uncovered*, COMPUTER BUSINESS REVIEW ONLINE, November 1, 2005 (quoting Alex Hernandez, director of advanced product development at CipherTrust).
[52] Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, available at http://www.gaudior.net/alma/johnny.pdf.
[53] Steve Sheng et al, *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software*, available at http://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf.

Because hackers know that mid-market companies generally spend less on security and encryption, it is estimated that the over 4,000 mid-market companies may be particularly vulnerable to attack unless they too plan to protect their data.

customer information, potentially leading to bad public relations, loss of customers, and costly litigation. For example, in January 2007 TJX Companies, an umbrella company including T.J. Maxx, Marshalls, Home Goods, Bob's Stores, and other retail chains, announced that their computer systems were hacked from 2005-2006, resulting in the theft of information regarding 45.7 million separate payment cards used from 2002-2004 including individual's names and credit and debit card numbers.[54] Radioshack in March 2007 learned that 20 boxes of discarded records included sales receipts with customer credit card numbers. The Texas Attorney General has initiated an enforcement action. In March 2007, Group Heath Cooperative Healthcare System lost two company laptops containing the names, addresses, social security numbers, and Group health ID numbers of local patients and employees.

Each of these incidents could have been largely averted through encryption. Mid-market companies may be particularly vulnerable to attack. Hackers are no longer going for the notoriety of having spawned a global virus. Instead they are in it for the money. Because hackers know that mid-market companies generally spend less on security and encryption, it is estimated that the over 4,000 mid-market companies may be particularly vulnerable to attack unless they too plan to protect their data.[55]

As noted above, encryption is also an affirmative defense to accidental publication of personal information in at least California's Confidentiality of Social Security Number Act.[56] Additionally, various encryption standards are required to be used by government contractors involving intelligence matters.[57] Moreover, it is just plain smart to encrypt to avoid inadvertent disclosure of proprietary information. IT and legal departments must coordinate the company's need for encryption services and determine whether their current system adequately protects them in case of hacking, theft, or lawsuit.

[54] TJX, Frequently Asked Questions, www.tjx.com/tjx_faq.htm.
[55] Allan Holmes, *Many Mid-Market Enterprises Say They Have Neither the Time, Money nor Resources to Spend on Security. Which May Be Why the Crooks Are Targeting Them and Turning the Mid-Market into a Bad Neighborhood,* CIO, March 1, 2007.

[56] CAL. CIV. CODE §1798.29 (part of bill also known as SB 1386).
[57] National Institute of Standards and Technology (NIST), Data Encryption Standard Fact Sheet, at http://csrc.nist.gov/cryptval/des/des.txt.

## International Issues: When Data Compliance Worlds Collide

For companies that operate internationally, it is essential that they understand both the local data compliance and cross-broader rules that apply to electronic data.

The rules of data collection, processing, retention, use, monitoring, access, and destruction not only differ dramatically in jurisdictions outside the U.S., but also in some instances, are directly contrary to U.S. laws. For companies that operate internationally, it is essential that they understand both the local data compliance and cross-broader rules that apply to electronic data.

In the EU for instance, each country has, pursuant to the EU Data Privacy Directive, implemented laws governing the collection, recording, organization, storage, adaptation, alteration, retrieval, blocking, monitoring, use, disclosure, transmission, transfer, and destruction of "personally identifiable information," and in some cases yet further protections for "sensitive personally identifiable" information. Unlike in the U.S., EU "personally identifiable information" is broadly defined and is generally not limited by industry and sector but instead protects unauthorized processing or transmittal of a person's information such as name, address, compensation, benefits, and financial information as well as more "sensitive" information such as health, racial or ethnic original, political affiliation, trade union membership, or marital status. Such laws extend to not only employees but also consumers. Italy, Austria, and a few other countries take it a step further and extend data privacy protection beyond people to companies.

Not only must companies understand what data they are allowed to collect, process, and transmit internationally, but they must also grapple with at times competing and sometimes conflicting laws.

Because the U.S. is essentially considered an "unsafe" jurisdiction by the EU, such information cannot be lawfully transferred, electronically or otherwise, to the U.S. or other "unsafe jurisdictions" unless certain safeguards are in place such as participation in the U.S.-EU Safe Harbor Agreement, adoption of EU Model Clauses, or implementation of approved Data Privacy policies. Even when such protections are in place to transfer personally identifiable data to the U.S., it may not permit "onward transfers" of such data to unidentified third party processors or to other countries, such as data entry services in India. And the EU countries are not alone: Canada, Argentina, Japan, Australia, and many other countries are also adopting varying degrees of data privacy protections.

Not only must companies understand what data they are allowed to collect, process, and transmit internationally, but they must also grapple with at times competing and sometimes conflicting laws. For instance, SOX requires publicly traded companies to have an anonymous whistleblower hotline in which to report suspected financial and securities violations. The thought behind the SOX anonymous hotline is that it would give employees comfort to know that their identities are unknown and avoid fear of reprisal. In contrast, the EU generally frowns on anonymous hotlines as an infringement of privacy rights and limits anonymous reporting. The conflicting priorities of SOXs transparency versus the EU concern of privacy poses an obvious dilemma for publicly traded multinationals and requires a sophisticated data management system to ensure that, among other things, proper limited retention, access, and retrieval are safeguarded while also meeting the U.S. SOX requirements.[58]

Other U.S. "best practices" simply do not translate internationally. For instance, the French Supreme Court in 2001 held that it was not only a wrongful termination but also unconstitutional and a criminal violation when a French company fired a French employee after it learned from monitoring his company computer that he had sent emails containing confidential information to a potential competitor. The French court held that the employee had a constitutional right of privacy during his working hours and at his workplace even where the employer had forbidden the non-professional use of his company computer. Germany has taken a slightly softer tact, but it too restricts monitoring of employee computers if the employer allows the employee to use the company system for personal use. Several EU jurisdictions require any employee monitoring to be, at a minimum, registered and approved by the local data privacy authority.

It is therefore imperative that when selecting electronic data management system that the company understands local legal requirements where the data is collected, used, or accessed. If, as is the case for multinational companies, data arises in or is transferred to multiple jurisdictions, it is critical that data privacy laws be observed and that proper firewalls and access restrictions be present in any data system to prevent data processing, monitoring, or data transfer without proper, compliant safeguards.

[58] For further discussion of overreaching Codes of Conduct and international overuse of anonymous whistleblowing lines, see *"Overreaching Global Codes of Conduct Can Violate the Law"*, by Cynthia L. Jackson, LA and SF Daily Journal, June 7, 2006.

## Best Practice Tips

1. **Plan ahead.** Don't wait for the lawsuit, hostile work environment complaint, trade secret leak, or confidential information loss to start managing your data.

2. **Know what is legally required.** Understand the legal requirements of your industry and jurisdictions in which your company operates. For instance, what are the data retention obligations for particular information in a country, or a state? What safeguards if any exist for restricting access or retention? Do you know what must be encrypted and what notification obligations exist if there is a breach of security? Are filters prudent in a jurisdiction to avoid hostile work environments or are filters deemed an invasion of privacy?

3. **One size might not fit all.** If you operate on a national or international scale, understand the sometimes conflicting obligations that your electronic data management system will have to address. Consider firewalls, access restrictions, and disabling particular functions in some jurisdictions that do not permit monitoring or filtering, for instance.

4. **Assign responsibility to manage the system.** Appoint personnel responsible for maintaining and managing electronic data. This might be a collection of people from legal and IT, with input from HR or other departments. Get the people involved early who will need to make the system work when legal demands arise.

5. **Locate the various forms and keepers of data.** Remember that data can be stored in a desk,

personal digital assistants (PDAs), home computers, laptops, and elsewhere. Before you can manage data for which the law will hold the company accountable, you must first identify what and where it is to ensure that the system you adopt will in fact capture the relevant data. Know what metadata you have.

6. **Select a flexible electronic data management system.** Select a system that is flexible enough to address your company's particular retention, archiving, monitoring, filtering, and encryption needs in the jurisdictions in which your company operates. Pick a system that is "user friendly" so that employees do not take steps to circumvent it. Choose a system that can adapt as legal requirements evolve. Plan for growth and proliferation of data, including metadata.

7. **Don't be a pack rat.** Just because technology gives you the ability to store massive electronic data doesn't mean you should. Needless storage of data not only complicates data retrieval but also can increase hacking risks. For instance, don't keep sensitive customer financial data unless you need it. If you need it, encrypt it.

8. **Adopt policies.** Adopt clear and simple polices consistent with applicable laws addressing such things as document retention, including "litigation holds" well in advance of litigation. In the U.S., adopt a well publicized email employee electronic monitoring policy. Adopt encryption policies for confidential information to avoid inadvertent disclosures. Where permitted, adopt disciplinary procedures to impress upon your workforce that you mean what you say.

9. **Be prepared.** Don't wait for a "litigation situation" (let alone a lawsuit) to put in place a litigation hold process. Create now the process to override any document destruction processes so that the litigation hold can be triggered quickly when necessary. Do your homework before any "meet and confer" court proceeding to address electronic discovery. The litigant who knows what they have and why they have it will be in a stronger position to negotiate the most favorable electronic discovery plan. Don't wait for a security breach to put processes in place for prompt notice and reporting.

10. **Train and audit and then train and audit some more.** A policy and data management system only work if employees know how to use them. It requires conscientious and consistent implementation and maintenance. Purchasing a data management system is only your first step to compliance. New data, new technology, new laws, new threats, new employees, will all require diligent maintenance and ongoing training and auditing.

WP33-0705

postini