What Are You Keeping In the Hen House?

Managing Document Retention

By Stephanie L. Chandler, Jackson Walker L.L.P.[1]

The expansion of the use of technology solutions has proven to be a great opportunity, but also a great challenge to business owners. Our workplaces are now a network that allows users to provide, and to access, information located on different computers throughout the world. Your employees create extensive records of their thought processes and their interactions with others. Employers need to manage this data effectively.

As a result of the Enron document shredding scandal, clients are asking attorneys to reexamine company document retention policies. A document retention policy is a plan that identifies how every document a company produces or receives will be maintained, stored, retrieved and sometimes destroyed.[2] Many companies routinely adopt retention policies for hard copy documents, but few companies consider digital and electronic data in their policies. It is important to have written document retention policies for electronic data to avoid unnecessary risks and expenses, and it is even more important to follow those policies.

A. WHY EVERY BUSINESS NEEDS A WRITTEN DOCUMENT RETENTION POLICY

From a technical perspective, every business should have a document retention policy because 1) saves valuable computer and physical storage space; and 2) reduces the volume of stored documents and data, making it easier to retrieve something when you need it. From a legal perspective, an effective document-retention policy can benefit a business in many ways:

1. Avoiding Spoliation Claims.

An effective document retention policy will provide a defense against unwarranted allegations of spoliation of evidence.[3] Under the rules of discovery in most jurisdictions, data stored on computers is discoverable. For example, Rule 34(a) of the Federal Rules of Civil Procedure clearly authorizes a party to request production of computerized data or electronic data, referred to in the rules as electronically stored information (ESI).[4] A court will likely award sanctions when a party fails to provide electronic data in response to a proper discovery request because the data has been destroyed or impermissibly modified after anticipation of litigation.

a. *Monetary Sanctions*

Courts have consistently imposed monetary sanctions for conduct that constitutes spoliation. Take for example, *In re Prudential Ins. Co. of Am. Sales Practices Litigation*, where the Court imposed a $1 million sanction on Prudential Insurance.[5] Although there was no evidence of willful misconduct, the court was outraged by Prudential's treatment of documents. The Court stated that it had "no record of any written manual that would evidence that Prudential possesses a clear and unequivocal document preservation policy capable of retention by Prudential employees and available for easy reference."[6] Even though there was no willful misconduct, Prudential was severely punished. However, Prudential could have avoid this punishment by having an effective document retention policy.

b. *Court may give jury instructions on spoliation*

Some courts have allowed juries to draw negative inferences regarding the content of destroyed electronic documents. This is referred to as a "spoliation inference." The use of a spoliation inference permits the jury to infer that a party who destroyed potentially relevant evidence did so out of a realization that the evidence was unfavorable. For example, in *Linnen v. A.H. Robins*, the court ordered the Defendant to not destroy any potentially relevant documents while the lawsuit was pending.[7] The Defendant sent emails and voicemails to all of its employees advising them to save all relevant documents.[8] The Defendant, however, failed to stop its back-up tapes from being recycled or taped-

[1] Stephanie Chandler is a partner with the law firm of Jackson Walker L.L.P.. Ms. Chandler's practice consists of representing corporate clients in transactions ranging from corporate formation to public offerings of securities and SEC compliance matters. Her experience includes entity formation, minority and women owned business certification, venture capital transactions, mergers, acquisitions, divestitures, and contract negotiations.

[2] Jason Krause, *Frequent Filers*, ABA J., Aug. 2003.

[3] David F. Bartlett, *Document Retention Policies in the Wake of Enron,* ILL. B.J., June 2002.

[4] Fed. R. Civ. P. 34(a).

[5] 169 F.R.D. 598 (D. N.J. 1997).

[6] *Id.* at 613.

[7] 10 Mass L. Rptr. 189 (Mass. 1999).

[8] Id. at 9.

over.[9] All deleted data was stored on the back-up tapes for a period of three months; therefore, the Defendant destroyed three months of electronic data that could have been compelled during discovery.[10] The Court determined that the appropriate sanction against the Defendant was a spoliation inference.[11] Thus, the jury was instructed that they could infer that the Defendant destroyed the back-up tapes because they realized that the evidence on the tape was unfavorable.

c. *Default or dismissal appropriate in some circumstances.*

Failing to comply with discovery can result in dismissal of a plaintiff's claim or a summary judgment against a defendant. Federal Rule of Civil Procedure 37 allows for dismissal of a plaintiff's claim as a sanction for plaintiff's failure to comply with discovery. Similarly, when a defendant fails to comply with discovery, Rule 37 provides that a default judgment may be awarded.

2. Lowering Litigation Costs

In this day of electronic communication, a high volume of electronic data can be accumulated in a relatively short amount of time. Combing through a huge mass of electronic data for relevant documents can be expensive. Having an effective document retention policy will increase the ease and speed in locating documents and reduce the costs associated with responding to discovery requests.

3. Removing "Smoking Guns"

Even "smoking gun" documents can be legally destroyed pursuant to a uniform and consistent document retention policy.[12] The U.S. Supreme Court stated that "under ordinary circumstances, it is not wrongful for a manager to instruct his employees to comply with a valid document retention policy, even though the policy, in part, is created to keep certain information from others, including the govt."[13]

But when litigation can reasonably be anticipated, attorneys have an obligation to advise clients to take reasonable steps to preserve records subject to discovery.[14] In *Zubulake v. UBS Warburg LLC*, the Defendant's in-house counsel advised them to not destroy or delete any information relevant to the lawsuit.[15] Counsel, however, failed to warn its client to not delete or recycle back-up dates of technological data.[16] The Court ordered the Defendant to bear the substantial cost of restoring the back-up tapes.[17] Counsel could have easily helped the Defendant to avoid this expense and hassle.

B. WHAT SHOULD A DOCUMENT RETENTION POLICY INCLUDE?

Merely having a policy will not solve all the problems discussed above. A bad policy can be worse than no policy at all. The leading case providing guidance on document retention policies is *Lewy v. Remington Arms Co*.[18] In that case the 8th Circuit set forth the following factors for a court to consider in evaluating a retention policy: 1) whether the policy is reasonable considering the facts and circumstances surrounding the relevant documents 2) whether the destroyed documents are relevant to pending or probable lawsuits; and 3) whether the policy was instituted in bad faith.

1. Guidelines

It is important to first identify the key people who will be involved in the design and implementation of the document retention program. This allows the different types of documents that the company generates to be identified, as well as what document retention procedures are currently in place. Representatives from human resources, information technology, and administration would normally all be involved in the design and implementation process.

Once the key people are identified, here are some guidelines for what your document retention policy should include:

- Review all applicable law
- Take into account statute of limitations period that may affect documents
- Clearly describe the class of documents to which the policy will apply
- Specify the retention period for each class of documents
- Create procedures detailing how the program will be implemented and enforced
- Identify the staffer responsible for policing and maintaining the program

[9] *Id.*

[10] *Id.*

[11] *Id.* at 11.

[12] David F. Bartlett, *Document-Retention Policies in the Wake of Enron,* ILL. B.J., June 2002.

[13] *Arthur Anderson LLP v. U.S.*, 544 U.S. 696 (2005).

[14] *N.Y. Nat'l Org. for Women v. Cuomo*, 1998 WL 395320 (S.D.N.Y. 1998).

[15] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004).

[16] *Id.* at 424.

[17] *Id.* at 426.

[18] 836 F.2d 1104 (8th Cir. 1988).

- Allow alternatives to, or even suspension of, document-destruction procedures when a duty to preserve arises.[19]

2. Consistency is the Key to Effective Document Retention

The key to an effective document retention policy is consistency. A policy must be uniformly and consistently applied. Companies invite trouble when they selectively enforce document retention polices or only enforce them after learning of a lawsuit.[20] When a document retention policy is not uniformly applied, courts will wonder whether it was created in bad faith.

3. What about Email and Phone Records?

Business now run at the speed of the transmission of bytes. Every day electronic documents are created, transmitted, and modified. There is a common misconception that emails and phone records are different. For example, questions regularly arise as to whether they should be kept for a different amount of time than paper documents. Herein is where the difficulty arises. Electronic data retention should correspond to the general retention schedule for the subject of the document. To effectively manage email, a policy would need to result in electronic documents being cataloged and retained pursuant to the obligations related to the subject matter.

4. Regular Enforcement is Key.

Document retention policies must be regularly enforced even when no litigation or investigation is looming. The policy should call for regular check so ensure that employee practices of destruction and retention consistently conform to the plan. Establish clear accountability for enforcement of the policy. While executive-level employees may be responsible for overall enforcement, staff needs to be educated about the importance of the policy and held accountable. Finally, periodically conduct an internal audit of the policy. It should be reexamined and any necessary adjustments should be made on a regular basis. Without enforcement, the investment made in policy creation will not pay the returns you are desiring.

II. PRIVACY ISSUES WITH CONSUMER DATA

A. PRIVACY POLICIES GENERALLY

The cardinal rule in relation to privacy policies is that a company must do what it says it will do. Only promise employees and customers a level of personal data security that can be delivered and adhere to all promulgated promises.

Under Section 5(a) of the FTC Act, the FTC can initiate enforcement actions against companies for "unfair or deceptive acts or practices." The FTC has used this statutory provision to sue companies that have publicly available privacy policies but do not adhere to those policies. There are two types of suits typically brought under Section 5(a): disregard of privacy policies, and substandard protection of protected data (whether "protected data" is statutorily protected or protected by the terms of the privacy policy).

Any enterprise that has a privacy policy, whether in print or available via link on a home page, should evaluate whether it is actually living up to the promises in that privacy statement. This seems obvious, but the FTC has found many companies in violation for using boilerplate language in privacy policies and not backing that language with action. Since 2001, the FTC has settled or otherwise ended investigations of many large corporations that simply did not live up to the language in their websites' privacy policies, including Tower Records, Guess?,[21] and Microsoft.

Perhaps less obvious is that stating in a privacy policy that one will not share information without authorization creates the duty to protect that information. The result is that an enterprise that shares data it promised to keep confidential is treated the same as an enterprise that has criminals break into its system and steal confidential data, if that system is substandard. Providing inadequate security measures is a violation of the FTC Act if confidentiality is promised in a privacy policy. It's also a violation of the statute and/or common-law doctrine that initially placed the information under privacy protection, if applicable. Recently, Barnes & Noble was forced overhaul the information collection and retention systems on its website and pay a $60,000 fine.[22]

B. PRIVACY MAINTENANCE REQUIREMENTS

Whether sent across the Internet or on trucks loaded with backup tapes, sensitive information about hundreds of millions of people is on the move every day. News headlines abound with stories of breaches. A hacker stole the personal records of at least 1,500 employees and contractors guarding the U.S. nuclear weapons

[19] David F. Bartlett, *Document Retention Policies in the Wake of Enron,* ILL. B.J., June 2002.

[20] David F. Bartlett, *Document Retention Policies in the Wake of Enron,* ILL. B.J., June 2002.

[21] *See* fn. 47.

[22] *See* Press Release, New York Attorney General's Office, Attorney General Reaches Agreement with Barnes and Noble on Privacy and Security Standards (Apr. 29, 2004), *available at* http://www.oag.state.ny.us/press/2004/apr/apr29a_04.html.

stockpile.[23] That news came days after the VA admitted it lost the personal information of 2.2 million active-duty military personnel.[24] Consumers are understandably getting nervous. Twenty percent of 51,000 adults surveyed by the Ponemon Institute in 2004 said they terminated their relationship with a company after finding out their personal information may have been compromised.[25]

While technological advances have made information sharing (and privacy invasion) easier, privacy law policy has remained static. Although not explicitly stated, statutory and case law seem to provide two broad justifications for privacy protection: (i) some data is inherently private and (ii) the widespread availability of some information could create vulnerability. These goals remain the same whether or not an emerging technology is involved. In fact, laws specific to an emerging technology are typically codified variations of common law doctrines. And state common-law tort claims are just as prevalent in technology-related privacy cases as claims based on newer statutes.

The takeaway for businesses today is that there are limits to collecting and sharing private data or data that could lead to vulnerability. Given the unclear application of this rule, and the effort of this section is to detail the types of data that recently enacted privacy statutes have been used to target. The reader should be cautioned that controlling for the specific data types mentioned below is not a safe harbor. But the right starting point for an enterprise-wide evaluation of privacy-related exposure is certainly to look at enforcement's current focus.

1. Inherently Private Information

a. *Medical Records.*

Any business that uses medical records should evaluate whether its current privacy policy affords those records adequate protection. This evaluation is necessary because a number of laws prohibit sharing medical records without authorization. Some laws give privacy protection to specific types of medical records or for medical records used for specific purposes– e.g., the Americans with Disabilities Act, the Family Medical Leave Act, the Fair Credit Reporting Act, and the Occupational Safety and Health Act.[26] Meanwhile, the Health Insurance Portability and Accountability Act ("HIPAA") gives sweeping privacy protection to all individually identifiable health information.

Although HIPAA provides broad protection, it applies to a relatively narrow class of "covered entities," including health plan providers, healthcare clearinghouses, and healthcare providers. Further, HIPAA does not include a private cause of action and caps statutory damages at $25,000 for simple violations and $250,000 for willful violations.

But because other statutory claims and common law tort claims are typically made in conjunction with a HIPAA claim, any statutory cap on damages is a red herring. Recently, Eckerd settled a medical records sharing case with the state of Florida. It had to change its privacy policies and fund a $1 million ethics chair at the Florida A&M School of Pharmacy.[27]

Most physician practices know that they are "Covered Entities" under HIPAA due to their status as medical providers. However, many are not aware that, as an employer, they may be caught in another category of Covered Entity: health plans. In fact, even though the US Department of Health and Human Services was explicit in noting that "employers" are not Covered Entities under HIPAA, many employers (including many healthcare providers) offer fully or partially self-funded health plans to their employees, and those health plans are Covered Entities under HIPAA.

Most HIPAA rules apply equally to all Covered Entities, whether they are providers, plans, or healthcare clearinghouses. Therefore, providers who also offer health plans to their employees will need to ensure that their health plans comply with the Privacy Rule and the Security Rule. One area where HIPAA differentiates Covered Entities relates to the size of the health plan: small health plans (less than $5,000,000 in size) were

[23] *See* Chris Baltimore, Data on US Nuclear Agency Workers Hacked-Lawmaker (June 9, 2006), *available at* http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2006-06-09T232425Z_01_N09199487_RTRIDST_0_CRIME-NUCLEAR-HACKER.XML.

[24] *See* Ann Scott Tyson and Christopher Lee, Data Theft Affected Most in Military National Security Concerns Raised, WASHINGTON POST STAFF WRITERS (June 9, 2006), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/06/AR2006060601332.html.

[25] LOST CUSTOMER INFORMATION: WHAT DOES A DATA BREACH COST COMPANIES? A survey summarizing the actual costs incurred by 14 organizations that lost confidential customer information & had a regulatory requirement to publicly notify affected individuals. (November 2005) *Study available* at www.securitymanagement.com/library/Ponemon_DataStudy0106.pdf.

[26] Heather Rae Watterson, *Genetic Discrimination in the Workplace and the Need for Federal Legislation*, 4 DEPAUL J. HEALTH CARE L. 423, 437 (2001).

[27] *See* Press Release, Florida Attorney General, Eckerd Endows $1 Million Ethics Chair at FAMU, Revises Policies to Help Protect Patient Privacy (July 10, 2002), *available at* http://www.myfloridalegal.com/newsrel.nsf/newsreleases.

granted an extra year to comply with the Privacy Rule (April 2004), as well as an extra year to comply with the Security Rule (April 2006).

If you offer your employees a health plan, that plan must meet the requirements of the Privacy Rule and the Security Rule (and if your plan is a "small" plan, the Security Rule deadline is fast approaching). For most small plans, Security Rule compliance is relatively easy, since the Security Rule is geared toward protecting electronic protected health information; most small plans, especially those that outsource much of their operations to third party administrators, will find that they have very little interaction with electronic PHI. However, small plans are still required to comply.

b. *Electronic Communications*.

Many statutes – e.g., the Electronic Communications Privacy Act, the Cable Communications Policy Act, the Video Privacy Protection Act, the Computer Fraud and Abuse Act, etc. – give privacy protection to information either gained or transferred by some means not possible without emerging technologies. Without digging too deeply into specific statutory causes of action, the theme across these Acts is that an enterprise cannot collect private, individually identifiable information without a privacy policy in place and available; and cannot share private information without authorization.[28]

Although the language here is new (e.g., "video," "computer fraud," etc), the concept is not. These acts serve to update age old torts like surveillance and eavesdropping in private places and public disclosure of private information.[29] It is the norm to see state common law tort claims, like intrusion of seclusion or trespass to personal property, made in conjunction with statutory claims.

The takeaway here is that any company that appears to deal in private, individually identifiable information should take a hard look at its current privacy policies. Information technology has allowed increased access to private information and privacy policies have been slow to keep up. For example, Amazon.com recently settled a class action suit brought for collecting data from its website's users and sharing that data with its affiliates. In that settlement, Amazon.com was forced to change its privacy policy; pay $100,000 to class members; pay $1.9 million to a charitable fund; and pay an additional $1.9 million in plaintiff legal fees and expenses.[30]

2. Information Leading to Vulnerability.

a. *Consumer Financial Data.*

Consumer financial data is probably appropriately considered both inherently private information and a type of information that, if widely available, would encourage fraud against individual consumers. For those reasons, a number of laws regulating collecting and sharing individually identifiable financial information have been created. Any enterprise that buys or sells financial information of any sort should conduct an in-depth evaluation of the laws applicable to the data it uses. For the purpose of this section, however, discussion of applicable statutory law will be limited to the Fair Credit Reporting Act ("FCRA"), and the new requirements to FCRA contained in the more recently enacted Fair Accurate Credit Transactions Act ("FACT Act"), and Gramm-Leach-Bliley Act ("GLBA") .

FCRA applies to companies that buy or sell "credit data."[31] Credit data is any individually identifiable information intended to be used to determine eligibility for financial products. As is common in privacy law, FCRA requires companies that collect credit data to have a privacy policy in place and available to affected individuals, and further requires authorization before sharing credit data. Moreover, FCRA allows individuals to prevent companies that collect credit data for the primary purpose of selling the data (as opposed to the primary purpose of making financial product decisions) from sharing their non-individually identifiable data.

Private actions are authorized under FCRA, and most FCRA cases involve multiple statutory and common law claims. In a recent settlement in Minnesota, US Bancorp – alleged to be a credit reporting agency and certainly a purchaser of credit data – agreed to pay just over $2 million to charities and $500,000 to the state.[32]

[28] *See, e.g.,* Toyrus.com, Data Aggregator Coremetrics Settle Suit Over Surreptitious Data Gathering, 8 Electronic Commerce & L. Rep., Jan. 8, 2003, No. 3, at 25 (detailing settlement requiring Toys R Us to pay $900,000 in fees, create privacy policy and provide conspicuous link to privacy policy detailing data aggregation, and cease selling personal data without individual authorization); Parker v. Time Warner Entertainment Co., 331 F.3d 13 (2nd Cir. 2003) (overruling lower court's denial of class certification for potential 12 million member class for alleged unauthorized sale of personal information gathered online).

[29] Daniel J. Solove, *A Taxonomy of Privacy*, 154 u. pa. l. rev. 477 491-93, 430 (2006).

[30] *See* Complaint, Supnick v. Amazon.com, Inc., No. COO-0221-P (W.D. Wash. June 20, 2000), available at http://www.alexa.com/settlement/complaint.html.

[31] *See* 15 U.S.C. § 1681 et. seq.

[32] *See* Complaint, Minnesota v. U.S. Bank Nat'l Ass'n ND (D. Minn. 1999) (No. 99-872), *available at* http://www.ag.state.mn.us/consumer/Privacy/Pr/pr_usbank_06091999.html.

Finally, the FACT Act affects virtually all companies in the U.S. Among its provisions, this law mandates that businesses must take reasonable measures to destroy information derived from consumer credit reports before discarding them. Shredding papers and wiping or destroying hard drives and backup media will be standard. From December 2006, merchants accepting credit cards must leave all but the last five digits off printed receipts.[33]

GLBA has broader applicability than FCRA. The FTC has interpreted GLBA[34] to give privacy protection to any individually identifiable information[35] gained by any company that engages in an activity related to finance.[36] The upshot is that if an enterprise uses any individually identifiable data that relates to finance in any way, the company's ability to collect and share that data will be limited.

Although GLBA has broader application than FCRA, it does not provide any private causes of action. Still, it is not uncommon for public GLBA action (e.g., investigation) to lead to class actions seeking relief under FCRA and/or state statutory and common-law.[37]

b. *Social Security Numbers.*

At the state level, a trend exists to provide Social Security numbers with privacy protection. A Social Security number is nothing more than a government-originated identifying number. But, given the way many information systems have been built, access to an individual's Social Security number can often enable a new holder to obtain access to types of data widely considered inherently private (e.g., medical records, financial information, etc) and commit identity fraud.

For that reason, many states have, through both common-law interest-balancing approaches[38] and statutory approaches, [39] given Social Security numbers privacy protection. Texas has adopted the statutory approach, such that any enterprise cannot collect Social Security numbers without adopting a privacy policy and making it available to individuals, and cannot share Social Security numbers without authorization. The applicable law can be found in the Texas Business and Commerce Code § 48.102. To comply, the business should ensure that all reasonable efforts are made to protect and safeguard sensitive personal information it has from unlawful use or disclosure.[40] This should include taking precautions to safeguard sensitive personal information stored electronically or on paper. If sensitive personal information stored electronically is compromised, the business should notify the owner of the information.[41] If records with sensitive personal information will not be retained by the business, the business should destroy the records or make arrangements to destroy the records.[42] Any records destroyed should be destroyed by shredding, erasing, or modifying the sensitive information so it is unreadable or undecipherable by any means.[43]

c. *Children's Personal Data.*

The Children's Online Privacy Protection Act ("COPPA") gives privacy protection to children's (under 13) individually identifiable information on websites or other online services.[44] Any enterprise that (i) maintains a website that targets children, or (ii) has actual knowledge that children visit its website, cannot collect individually identifiable information from any children without prior parental consent. COPPA has a host of other requirements, including privacy policy creation and notification, limits to the total amount of information that can be collected, and deletion of children's information at parents' request. Any enterprise that deals with children in an online environment should evaluate whether its privacy policies are in line with COPPA.

This evaluation is necessary because the past five years have seen a significant amount of COPPA litigation. Until recently, exposure seemed relatively low, as cases typically settled for less than $100,000. But COPPA does authorize civil penalties of up to $11,000 per violation, and a 2004 case marked the largest settlement amount to date, $400,000.[45]

---

[33] Text available at http://www.ftc.gov/os/statutes/031224fcra.pdf.

[34] 15 U.S.C. § 6801, et. seq.

[35] *See* Individual Reference Services Group, Inc. v. Federal Trade Commission, 145 F. Supp. 2d 6 (D.D.C. 2001) (aff'd by Trans Union LLC v. FTC, 295 F.3d 42, 46 (D.C. Cir. 2002)).

[36] 16 C.F.R. § 313.3(k)(2)

[37] *See, e.g.,* In re Trans Union Corp. Privacy Litig., 211 F.R.D. 328 (N.D. Ill. 2002).

[38] *See, e.g.,* City of Kirkland v. Sheehan, No. 01-2-09513-7 SEA (Wash. Super. Ct. 2001), *available at* http://www.politechbot.com/docs/justicefiles.opinion.051001.html

[39] *See, e.g.,* 2005 Texas House Bill No. 1130 (2005) (effective September 1, 2005).

[40] Tex. Bus. & Com. Code § 48.102.

[41] Tex. Bus. & Com. Code § 48.103.

[42] TEX. BUS. & COM. CODE § 48.102(b).

[43] TEX. BUS. & COM. CODE § 48.102(b).

[44] 15 U.S.C.A. §§ 6501 et seq.

[45] Consent Decree and Order for Civil Penalties, Injunctive and Other Relief, United States v. Bonzi Software, Inc., Civ. Action No. CV-04-1048 RJK (Ex), available at http://www.ftc.gov/os/caselist/bonzi/040217decreebonzi.pdf

C. PRIVACY OF CONSUMER INFORMATION: LIABILITY FOR DISCLOSURES OF CONSUMER INFORMATION

The nation's fastest growing crime, identity theft, is combining with greater corporate accumulation of personal data, increasingly vocal consumer anger and new state and federal laws to create significant new legal, financial and reputation risks for many companies. Examples of recent litigation include the following:

• In June 2006, a coalition of veterans groups filed a class action lawsuit demanding the VA name those who are at risk for identity theft as a result of the recent Veterans Administration loss of 26.5 million personal records of veterans. The suit seeks $1,000 in damages for each person, a payout that could reach $26.5 billion. The breach occurred when a VA employee violated agency policy and took a laptop with the records on it home, where it was stolen in a burglary.

• In 2003, Victoria's Secret settled a deceptive advertising suit brought by the New York Attorney General after it was found that personal information of the company's customers was inadvertently made accessible on the company's Web site. This was contrary to the company's Internet privacy policy, which stated that customer information was stored in private files on a secure server.[46]

• Guess? Jeans settled charges brought by the Federal Trade Commission under Section 5(a) of the Federal Trade Commission Act for unfair or deceptive acts. A statement on the company's Web site said that customer data was stored in an unreadable, encrypted format, but a hacker obtained access to approximately 200,000 credit card numbers in a clearly readable format. The FTC asserted that Guess?'s representation about encryption was false and misleading, and that the company had failed to implement reasonable security measures.[47]

In July 2003, California passed the Security Breach Information Act ("CSBIA"),[48] which requires any person or business conducting business in California to disclose security breaches involving unencrypted personal data to any California resident whose information was or is believed to have been acquired by an unauthorized person.[49] CSBIA was the first law in the U.S. expressly creating such liability.

Another California law is also of interest to business owners who collect data regarding their customers. In California, a civil action for invasion of privacy may be brought against any vendor, or employee of a vender who intentionally discloses information, not otherwise public, which that person knows or should reasonably know was obtained from confidential information.[50] The California Constitution leaves room for additional rights, remedies, and claims brought by a complainant and does not limit a claim to invasion of privacy.[51] Any vendor found to be in violation of disclosing confidential information shall be liable for a minimum of $2,500.00 in exemplary damages as well as attorney's fees and other litigation costs reasonably incurred in the suit.[52] California leads the trend in consumer privacy laws.

California's notice statute, the CSBIA, has been a model for the following twenty-one other states which have enacted similar statutes addressing disclosure of customer information in an attempt to help protect consumers. Texas' notification statute was effective September 1, 2005 and models California's statute with the only exception being that Texas does not define "personal information."[53] If you collect data from consumers that reside in other states, you should be sure that you comply with their state-specific requirements.

A consistent element in all of the notice statutes which have been enacted is the requirement to notify consumers when their personal information may have been accessed by an unauthorized person. A business owner's intent when a disclosure of consumer information occurs, is not relevant in establishing liability under the above mentioned notice statutes.[54] Given the scope of potential liability for a business which collects data from consumers in one or more of the states listed above, it is important to actions to work to limit potential liability for unintentional disclosure.

It is best to institute the following best practices:

a. *Limit the data you retain.* Nonessential data can be a liability rather than an asset. For example, a business

[46] See press release available at http://www.oag.state.ny.us /press/2003/oct/oct21b_03.html

[47] See press release available at http://www.ftc.gov/ opa/2003/06/guess.htm.

[48] *See* CAL CIV CODE § 1798.29 (West 2006) (commonly known as California Senate Bill 1386).

[49] *Id.*

[50] *See* CAL. PENAL CODE ch. 1.5 § 11149.4 (West 2006).

[51] *Id.*

[52] *Id.*

[53] *See* TEX. BUS. & COMM. CODE § 48.103 (West 2006).

[54] It should also be noted that, in various states there may be pending legislation regarding the protection of consumer information.

should consider whether they really need customers' Social Security numbers and should you store credit card numbers perpetually. Also, archive data after use rather than storing it in readily accessible customer master files, and discard or archive data for inactive accounts.

b. *Secure personal data.* Store data securely, preferably in encrypted form. Avoid storing personal data on laptops, PDAs and other mobile devices. Limit access to only those who need it. Have a full audit trail of who accesses each record. Restrict large-scale downloads and monitor employees for unusual access volume or timing. Ensure good physical as well as information systems security over personal data.

c. *Train your employees.* You should strongly consider completing background checks on all employees who will have access to personal information. In the event of a security breach by an employee, the fact that you conducted background checks will help demonstrate that you took reasonable precautions to guard against theft. In addition to background checks, employees should be required to sign non-disclosure agreements that prohibit them from misusing confidential data. Develop a written data security policy that clearly explains what data is considered confidential and what steps employees are expected to take to safeguard that data. Regularly train your employees on acceptable security practices and remind them of their legal obligation to protect customer information. Ensure they know that their access to such data is monitored and recorded to help prevent and detect data theft. Remind them that such theft is a crime and communicate your policy (if that is the case) of referring to the authorities all such cases for prosecution.

d. *Train your vendors.* Require vendors who handle, process, or store personal data, to have data security measures at least equal to yours. Require vendors to sign nondisclosure agreements to protect data. Insist on periodic security audits and vulnerability assessments to make sure data is being securely handled.

e. *Test your systems.* Once you've put in place appropriate measures, test them. For example, one company recently retained an outside firm to test their security systems. The outside firm scattered USB in the parking lot. When found by the employees a frightening number picked up the USB and immediately inserted it into their computers – you could say curiosity got the best of the majority of them.[55]

f. *Plan for breaches.* No matter how good your information security system is, there is always the potential for a breach. Have a written response plan in place to deal with data recovery, customer notification, public relations, and legal issues.

Please let Jackson Walker L.L.P. know if we can be of assistance in your efforts to develop a document retention policy by contacting Stephanie Chandler at schandler@jw.com or at (210) 978-7704.

This article is published by the law firm of Jackson Walker L.L.P. as an informational resource. It is not intended nor should it be used as a substitute for legal advice or opinion which can be rendered only when related to specific fact situations.

Please visit us at www.jw.com.

[55] See http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1 (visited June 13, 2006).

APPENDIX I

Document Retention Policy

This Document Retention Policy sets for the policies and procedures of [_____] (the "Company") for the identification, retention, storage, protection and disposal of Company records consistent with legal and business requirements. This Document Retention Policy is intended to ensure that the Company's retention policies adhere to customer, legal and business requirements and are conducted in a cost-efficient manner. Failure to comply with our document and record retention guidelines ("Guidelines") can cause negative consequences, including excess storage costs and inability to locate records that are needed. In addition, adherence to these Guidelines will assist the Company in complying with legal requirements and in responding to subpoenas and document production requests.

The Company reserves the right to amend, alter and terminate its policies at any time and for any reason.

STATEMENT OF POLICY

It is the Company's policy to maintain complete, accurate and high quality records. Records are to be retained for the period of their immediate use, unless longer retention is required for historical reference, contractual, legal or regulatory requirements or for other purposes as set forth herein. Records that are no longer required, or have satisfied their required periods of retention, shall be destroyed in an appropriate manner.

The purposes of this Retention Policy are to:

(a) Reduce the cost of information storage.

(b) Ensure that information that has outlived its usefulness is not retained.

(c) Ensure that information that may be useful for further reference is retained appropriately and stored economically.

The policies described in this policy relate to hard copy and electronic documents (collectively referred to as documents) in connection with information used or produced by Company personnel. This policy describes our policies for maintaining documents through their creation, active use, and destruction. This retention policy is administered by _____.

GUIDING PRINCIPLES

1. This policy establishes important policies that enable us to protect information, retain it as needed, and eliminate or destroy it when it is no longer needed.

2. All hard copy and electronic documents created in the course of the Company's business belong to the Company

3. Every employee is responsible for information and document management.

4. Only final documents will be retained; with the exception of contract-related documents unless otherwise required, drafts and preliminary versions of information will be destroyed currently.

5. Every document has an established retention requirement, based on governmental requirements or business needs.

6. Material not to be retained permanently will be permanently destroyed after the required retention period, subject to the approval of _____.

7. Voice messages must be deleted monthly or sooner.

8. Deletion of information from electronic files will be accomplished in such a way that precludes the possibility of subsequent retrieval by Company personnel or third parties.

9. No documents related to threatened or active litigation, governmental investigation, or audit will be destroyed.

SCOPE

These Guidelines apply to all Company records. A Company record is any documentary material, regardless of physical or electronic form, that is generated or received by the Company in connection with the transaction of its business and retained for any period of time. A record that includes both business and personal information, such as an appointment calendar, is a Company record. Examples of Company records include (i) writing of any kind, including, for example, correspondence, reports, memoranda, notes, drafts, diaries and calendars and (ii) information kept in all media forms including, for example, paper, microfilm, microfiche, tapes, cartridges, diskettes, hard drives and electronic records, such as emails and computer files.

Although the specific documents to be retained will, by necessity, vary on a case-by-case basis, the following examples are intended to provide some guidance. In the ordinary course, the following *should* be retained:

- research memoranda and analysis;
- memoranda, emails, spreadsheets, notes (including documents containing notes), correspondence and other documents memorializing information that is material to the Company's operations, including information obtained from persons outside the Company; and
- documents or other records obtained from outside the Company that are not readily accessible if needed in the future.

By contrast, the following types of materials *do not* need to be retained in the ordinary course:

- memoranda, emails, spreadsheets, notes, voicemails, correspondence and other documents memorializing information (i) that is not material to the Company's operations or (ii) that is subsequently memorialized and retained in a final document;
- material generated outside the Company that can be easily obtained if needed in the future (*e.g.*, research reports, industry newsletters and newspaper articles); and
- non-final drafts of memoranda, emails, spreadsheets, notes, voicemails, correspondence and other documents, unless specific circumstances indicate otherwise.

DOCUMENT RETENTION PRINCIPLES

1.1. Retention periods begin after the file/documents are no longer active (*i.e.*, termination of agreements or employment; expiration of contract, arrangement or document; final benefit payment; and disposal of assets).

1.2. The retention periods established by the Company are set forth below. Retention periods are listed in terms of calendar years plus the current calendar year. The destruction date for records is always December 31 of the last year of retention; *e.g.*, if a record has a retention period of the current year plus three and the record is dated 2005, the destruction date for the record is December 31, _____.

1.3. Upon expiration of the applicable retention period, the record is to be reviewed and destroyed unless extended retention is requested in writing, with satisfactory justification, by the head of the department responsible for the record. The department head shall make such request to our Chief Compliance Officer.

1.4. Whenever contractual retention requirements exceed the retention periods listed in these Guidelines, such records will be retained in accordance with the retention requirements of the contract.

1.5. In the event of a conflict, records retention requirements under national or local law will take precedence over the retention periods listed in these Guidelines.

1.6. Records relevant to a pending or reasonably anticipated legal action or tax audit are to be retained until the final resolution of such legal action or audit in addition to any applicable retention period outlined in the Document Retention Schedule set forth below.

1.7. Draft, working or reference documents typically should be discarded when they are superseded by a final document or are no longer in daily use (*i.e.*, at the close of a transaction). However, drafts and working documents that are exchanged externally in the course of any transaction (*i.e.*, acquisitions and leases) should be retained for as long as the final documents are required to be retained (*i.e.*, permanently for acquisitions).

1.8. Any Company employee who believes the retention period governing any type of records should be changed because of changes in legal, auditing or management requirements, or believes a new item should be added to the Guidelines, should submit a request to modify the Guidelines to our Chief Compliance Officer.

DOCUMENT SCREENING AND PURGING

2.1. Records are to be screened at least once every year to determine if they are "active records" (*i.e.,* subject to immediate use). The screening process is to be planned and carried out within each department.

2.2. Active records are to be stored in the immediate area of the responsible custodian. Active records determined to be inactive are to be reviewed for possible off-site storage or for destruction pursuant to these Guidelines.

2.3. Factors to be considered in the screening process include:

- frequency of reference;
- nature of reference; and
- volume of files.

2.4. Duplicate and multiple materials are to be eliminated. Whenever possible, the version of the record containing the most conclusive information is the one to be retained. In general, the retained copy of a record should not contain personal notations, other than the author's signature.

2.5. Records which have exceeded their required retention period are to be reviewed and, if no longer required, purged.

2.6. Supervisors are to ensure that the business files of terminating or transferring employees are reviewed concurrent with the employee's departure. Such files are to be reassigned to other employees, stored in accordance with these Guidelines or purged.

2.7. Each department is to identify those records which are essential to the continuity of the company and designate them as "vital records" as soon as practicable after the creation of the records. Examples of "vital records" include those documents and records that:

- are essential to the continuation of operations;
- are essential to the Company's legal and financial status;
- are necessary for fulfillment of obligations to shareholders, employees, customers or outside interests;
- contain trade secrets, secret processes, formulas, or innovations which are not registered elsewhere; and
- denote Company ownership of assets which would otherwise be difficult or impossible to establish.

2.8. Electronic backup files, tapes and other storage devises that are designed to retain records beyond the Document Retention Schedule set forth below, are to be solely for purposes of emergency data recovery in the event of a catastrophic information systems failure.

DIRECT RESPONSIBILITIES

3.1. The Chief Compliance Officer has overall responsibility for developing, implementing and maintaining the Company-wide records management process, in accordance with the requirements set forth in these Guidelines, including:

- updating the Document Retention Schedule set forth below;
- maintaining the index of "vital records" from each department;
- conducting orientation and training for Company personnel involved in the records management process;
- notifying personnel, in the event of a pending or threaten lawsuit or tax audit, to halt destruction of Company records;
- developing and maintaining the necessary records management form(s);
- preparing and maintaining inventories of records stored in the Company Record Center;
- ensuring that only authorized persons with a need-to-know gain access to records stored in the Company's Record Center; and
- ensuring that stored records are retained, protected, retrieved, returned to storage, reviewed and destroyed in accordance with these Guidelines.

3.2. Each department is responsible for assisting in the records management process by:

- supporting preparation and maintenance of local records retention schedules;
- identifying, packaging, documenting and transferring applicable records to the [Record Center];
- retaining only those records for which they have custodial responsibility; and
- reviewing and authorizing purging of records in accordance with the appropriate expiration date.

3.3. All employees are responsible for ensuring that accurate and complete records are identified, retained, stored, protected and purged in accordance with these Guidelines.

DOCUMENT RETENTION SCHEDULE

Default Rule: If a document is not listed in any category below, retain for [6] years.

**All periods listed below, except for the 60 day period, are listed in terms of the current year plus the time period stated. Also, time periods only begin at the termination or expiration of the document/contract as noted above.

[the following are examples only, please confer with counsel as to what may be required or appropriate for your industry/business; additionally, requirements may change and policies should be reviewed and updated periodically]

60 Days

- Computer back-up tapes (or the last date on which the records are in common, day-to-day use in the regular course of business)
- Email messages (This Guideline applies to general email messages only; email messages falling into a category for which a specific Guideline exists are governed by that Guideline.)

1 Year

- Calendars
- Chronological Files
- Correspondence (This Guideline applies to general correspondence only; correspondence falling into a category for which a specific Guideline exists is governed by that Guideline.)
- Diaries
- Employment applications, resumes, reference checks, and testing for non-hires
- Notepads
- Telephone message books

2 Years

- Budgets/forecasts
- Building plans and specifications
- Business plans
- Inventories of real property and equipment
- Maintenance and repair reports on equipment (2 years after final disposition)

3 Years

- Affirmative Action Plans
- EEO-1 Reports
- Family and Medical Leave Act ("FMLA") requests and other records
- I-9 Forms (later of 1 year after termination of employment or 3 years)
- Job postings/advertisements
- Maintenance and repair reports on real property
- Personnel files/employment records (*e.g.*, applications, resumes, reference checks, and testing for hired employees; offer letters; disciplinary actions; salary increases; performance evaluations; polygraph test records; exit interviews, etc.)
- Press releases
- Shareholder correspondence, inquiries, voted proxies
- Speeches
- Unemployment compensation claims
- Wage and hour records (*e.g.*, time records, wage rate tables, work schedules, etc.)

4 Years

- FICA records (*e.g.*, Social Security and Medicare records, etc.)
- Unemployment tax records
- W-4 Forms

5 Years

- Accident reports
- Labor-Management Reporting and Disclosure Act ("LMRA") documents (*e.g.*, LM-10 Report)
- OSHA forms, records (*e.g.*, OSHA Log 200, OSHA Form 101, injury and illness records, OSHA annual summary, etc.)
  - But not hazardous exposure documents – *see* below

6 Years

- Appraisals of real property and equipment
- Benefits documents (*e.g.*, benefit changes correspondence, benefits statements, beneficiary designation forms, government filings such as Form 5500s, health insurance records, plan documents, disability and sick benefits files, employee medical records, etc.)
- Contracts and any documents relating thereto (*e.g.*, consulting or employment agreements, separation agreements, letter amendments, etc.)
- Finance and Accounting documents (*e.g.*, disbursement records, check register, canceled checks and drafts, bank statements, balance sheet analysis and supporting workpapers, accounting policies and procedures, ledgers, annual/quarterly reports, SEC workpapers, petty cash records, etc.)
  - But not invoices and certain SEC filings – *see* below
- Human Resources policies, procedures, handbooks, manuals
- Insurance/risk management documents
- Internal audit reports
- Payroll records

- Purchasing documents
- Tax records (or "so long as the contents [of the records] may become material in the administration of any internal revenue laws")
- 1099 Forms

7 Years

- Invoices (later of 7 years or tax settlement)
- Lease agreements
- Partnership agreements

10 Years

- Tax returns (including schedules, workpapers)
- Tax rulings
- Environmental audits, compliance/clean-up
- Workers compensation claims (after final disposition)

20 Years

- Dividend payment orders by shareholders
- SEC filings: 10K, 10Q, 8-K
- SEC Forms 3, 4 and 5
- Shareholder ledger
- Transfer journals
- Unclaimed dividends

30 Years

- Employee medical records, exposure records under OSHA (30 years after termination of employment)
- Health and safety records relating to exposure to hazardous substances (i.e., toxic chemicals, high levels of noise, airborne contaminants or blood borne pathogens)

Final Disposition

- All information relating to charges, including discrimination, EEOC, state human rights departments, etc.
- Internal complaints
- Litigation documents (e.g., briefs, correspondence, discovery materials, pleadings, notes and research, etc.)
- Personnel records pertaining to a complaint, charge, compliance action, or enforcement action; workers' compensation claims
- Settlement papers and releases (i.e., after all terms are completed and statute of limitations has run)

Permanent

- Articles of Incorporation
- Bylaws
- Capital Stock and Bond records
- Closing documents for acquisitions, dispositions
- Copyright and Trademark registration
- Due diligence for acquisitions
- Final legal judgments
- Heart-Scott-Rodino ("HSR") filings (i.e., filings made in connection with major corporate events)
- IRS determination letters
- Minutes of meetings of Board of Directors and Committees of the Board
- Mortgage and Note agreements
- Patents, Trademarks and other Intellectual Property Documentation
- Purchase of business or entity
- Property deeds
- Proxy statements and related correspondence
- Stock certificates

The ABA has also promulgated a standard abbreviated form of Document Retention Policy which is available at http://www.abanet.org/lpm/lpt/articles/sampledocretentionpolicy.pdf.

Also of interest

Arthur Andersen Document Retention Policy

www.washingtonpost.com/wp-srv/business/daily/transcripts/anderson_policy020100.pdf

Appendix V

Document Retention Policy Regulations

The following is a summary of selected Texas and Federal regulations regarding document retention:

SELECTED TEXAS STATUTORY REQUIREMENTS FOR DOCUMENT RETENTION		
Type of Document	**Statute or Rule**	**Time for Retention**
General records retention statute, applicable if statute requires documents to be retained for unspecified period	Tex. Bus. & Com. Code § 35.48	Three years
Partnership tax records	Tex. Rev. Civ. Stat. Ann. § Art. 6132a-1 §1.07(a)(2) (Tex. Rev. Limited Partnership Act § 1.07(a)(2)	Six most recent tax years
State franchise tax records	Tex. Tax Code § 111.0041(a)	Four years
General period of tax assessment	Tex. Tax Code § 111.201	Four years
Tax statute of limitations	Tex. Tax Code § 111.202	Three years after deficiency or after last recording of lien
Sales tax records or receipts	Tex. Tax Code § 151.025(b) (also Comptrollers Rule 3.286)	Four years from date when records made
Employment records, including names, addresses, SSN, dates of employment wages and full time or part time status	40 TAC 815.106(i) (Texas Workforce Coms'n)	Four years

SELECTED FEDERAL STATUTORY AND REGULATORY DOCUMENT RETENTION PERIODS		
Type of Document	**Statute or Rule**	**Time for Retention**
General retention period, if not stated in other statute or rule	44 U.S.C. §3507(g) (Paperwork Reduction Act of 1980)	Three years
Section 10(a) prospectus for Form S-8, Registration Statement	17 CFR § 230.428(a)(2) (SEC)	Five years after documents used as part of prospectus to offer or sell
Employment records of hiring, promotion, transfer, layoff, termination, rates of pay and selection for training	29 CFR §1602.14 (EEOC)	One year from date of record or personnel action or, if charge of discrimination filed or action brought, until final disposition of charge or action
All recordable occupational injuries and illnesses to be maintained in log and summary form	29 CFR §1904.6 (OSHA)	Five years
Employee exposures, medical records and analyses of such exposure or medical records	29 CFR §1910.1020(d)(i) (OSHA)	30 years unless other OSHA rule specifies different period. For example, records of exposure to bloodborne pathogens must be kept for duration of employment, plus 30 years.
General income tax requirement for books of account and records to establish gross income for tax purposes	26 CFR §1.6001-1(IRS)	"So long as contents may become material in administration of any internal revenue law"
Records of property acquisition if material to income tax determination	26 CFR §1.6001-1 (IRS)	Until taxable disposition made
Records of income, deduction, and credits (including gains and losses)	26 CFR §1.6001-1 (IRS)	At minimum, until statute of limitation for return expires. Generally taxes shall be assessed within three years after filing

SELECTED FEDERAL STATUTORY AND REGULATORY DOCUMENT RETENTION PERIODS		
Type of Document	**Statute or Rule**	**Time for Retention**
		return. Claim for refund or credit must be filed within three years of filing or two years after payment whichever later. Six-year statute of limitations if substantial omission of income; seven years if claim is for credit for bad debts or securities losses. No statute of limitations for fraud or for no return (other exceptions possible).
Employment Tax Records	26 C.F.R. § 31.6001-1(e)(2)	Four years after due date or paid
Payroll records and other employment contracts	29 CFR § 516.5 (Wage & Hour DOL)	Three years
Earnings, wage tables, and other employment payment records	29 CFR § 516.6	Two years
Records of employee benefit plans subject to ERISA	29 U.S.C. § 1027	Six years after filing documents
Records of employment evaluation, seniority, job descriptions, or any other documents which explain the basis for wage payment differential between sexes	29 CFR § 1620.32(c) (Equal Pay Act)	Two years minimum
Employment and payroll records containing name, address, date of birth, pay rate, compensation for a week, and other materials pertinent to enforcement of age discrimination Resumes from other applicants, promotions, test papers and physical exams of other individuals	29 CFR § 1627.3(a) 29 CFR § 1627.3(b)	Three years One year

[The dates set forth above are subject to change.
Please confirm requirements are still current before implementing a policy]