TECHNOLOGY-RELATED POLICIES AND PROCEDURES: EMPLOYEE POLICIES, DOCUMENT RETENTION, PRIVACY AND INTELLECTUAL PROPERTY

STEPHANIE L. CHANDLER
Jackson Walker L.L.P.
112 E. Pecan Street, Suite 2400
San Antonio, Texas 78205

State Bar of Texas
IN-HOUSE COUNSEL BOOT CAMP
August 2, 2006
San Antonio

CHAPTER 2

Advanced In House Counsel

Technology-Related Policies and Procedures: Employee Policies, Document Retention, Privacy and Intellectual Property

By: Stephanie L. Chandler[1]
Jackson Walker L.L.P.
112 E. Pecan Street, Suite 2400
San Antonio, Texas 78205

State Bar of Texas
5th Annual Advanced
In-House Counsel Course
August 3-4, 2006
San Antonio, Texas

CHAPTER 2

About the Author

Stephanie L. Chandler. Stephanie L. Chandler is an attorney is the head of the Technology practice group and a member of the Business Transactions section of Jackson Walker L.L.P. Ms. Chandler's practice consists of representing corporate clients in transactions ranging from general corporate representation to public offerings of securities and SEC compliance matters, as well as venture capital transactions and contract negotiations. Her experience also includes advising clients regarding e-commerce, software and other internet and technology usage policies. Ms. Chandler is a member of the State Bar of Texas and the Committee on E-Commerce for the Texas Bar Association Business Law Section. Ms. Chandler is a regular public speaker and the author of multiple articles and publications including "A Practical Guide to Raising Capital," "High-Tech Boxing Match: A Discussion of Copyright Theory Underlying the Heated Battle Between the RIAA and MP3ers," 4 Va. J.L. & Tech. 5 (Spring 1999), "Explosive Growth Forecasted For ASPs: Are You Ready?," "Preparing Your Music Client for Distribution," 22 Hastings Comm/Ent L.J. (1999) and "Internet and Electronic Publishing Issues," ECopyright Law Handbook: Chapter 2 (2002). Ms. Chandler is a repeat selection to the Texas Rising Star list (2005 and 2006), featured in the Texas Monthly magazine, and was one of 5 lawyers in the state featured in the special 2005 Super Lawyers supplement to the magazine . Ms. Chandler received her Juris Doctorate from the University of Virginia School of Law, where she was on the Managing Board for the *Virginia Journal of Law and Technology*, and her B.S.B.A. in finance from University of Nebraska, Highest Distinction.

[1] The author wishes to acknowledge the contributions of the following in preparing this paper: John Koepke, Partner in the Labor and Employment section of Jackson Walker L.L.P. for contributing the form of Computer Software Policy and form of Information Systems Management and Monitoring. Special thanks to Mason Ayer, Ian Barber, Lorilei Cronin, Ashley Franklin and Melissa Gomez for their assistance in preparing this article. Mason Ayer is a Summer Associate Austin office of Jackson Walker L.L.P. Mr. Ayer is currently law student at the University of Virginia, and he received a B.S. in Foreign Service from Georgetown University in 2003. Ian Barber is a Summer Associate in the Austin office of Jackson Walker L.L.P. Mr. Barber is currently a law student at the University of Virginia where he received a B.S. in Commerce in 2002. Lorilei Cronin is a Summer Associate with the Dallas office of Jackson Walker L.L.P.. Ms. Cronin is a law school student at St. Mary's University, and she received a B.A. in Psychology from the University of Texas at Austin in 2000. Ashley Franklin is a summer associate in the Houston office of Jackson Walker. Ms. Franklin attends law school at Baylor University, and she received a B.A. in History from West Texas A&M University. Melissa Gomez is a summer associate in the Houston office. Ms. Gomez is a law student at Texas Southern University, and she received a B.A. in Political Science from St. Mary's University in 2005.

Stephanie Chandler

Attorney
Jackson Walker LLP

Stephanie Chandler is an attorney in the Business Transactions section and the state-wide head of Jackson Walker's Technology section. Ms. Chandler's technology practice consists of representing clients in relation to emerging technology issues, including ventures involved in e-commerce, software development, and biotechnology product commercialization. Additionally, she represents high-technology and traditional clients in the implementation of policies and procedures related to their and their employee's use of the internet and other technological tools and the negotiation of their contracts related to technology acquisition, proprietary rights, employment and independent contractor relationships, clickwrap and shrinkwrap and portal agreements.

COMMUNITY INVOLVEMENT

She is a member of the San Antonio Technology Accelerator Initiative (SATAI) Board of Directors and recently chaired its Entrepreneurial Alliance Committee, developing the curriculum for the SATAI U educational program for entrepreneurs. Ms. Chandler served as Speaker and Content subcommittee chairperson for the North San Antonio Chamber's Technology Summit and on the planning committee for the Trilateral Technology Summit.

Ms. Chandler is also member of the Committee on E-Commerce for the Texas Bar Association Business Law Section and the Venture Capital Subcommittee for the Texas Bar Association.

AWARDS

Ms. Chandler is a repeat selection to the Texas Rising Star list (2005 and 2006), featured in the Texas Monthly magazine, and was one of 5 lawyers in the state featured in the special 2005 Super Lawyers supplement to the magazine. Rising Stars are up and coming attorneys who have either practiced for 10 years or fewer or are under the age of 40. Rising Stars are voted on by Super Lawyers who have seen them in action. Only the attorneys who receive the top 2.5% of the vote are named Rising Stars.

Ms. Chandler was selected by the San Antonio Business Journal as one of "40 Rising Stars Under 40" recognizing her accomplishments in business, community, and career and was recognized by the Scene in SA as one of 13 young professionals under 30 in the San Antonio Community (2004) and by the Scene in SA as a "Rising Star" in the San Antonio Legal Community (2005).

PUBLICATIONS & SPEAKING ENGAGEMENTS

Ms. Chandler is the author of multiple articles and publications including:

- "Is Data and Software Solution Standardization the Wave of the Future?"
- "A Practical Guide to Raising Capital"
- "Top Gotchas - What Missteps Do Early Stage Companies Make?"
- "Federal Trade Commission Serious About Internet Privacy"
- "External Software Infringement Audits: Develop Your Response Plan"
- "Internet and Electronic Publishing Issues," ECopyright Law Handbook: Chapter 2 (2002)
- "High-Tech Boxing Match: A Discussion of Copyright Theory Underlying the Heated Battle Between the RIAA and MP3ers," 4 Va. J.L. & Tech. 5 (Spring 1999)
- "Explosive Growth Forecasted For ASPs: Are You Ready?"
- "Preparing Your Music Client for Distribution," 22 Hastings Comm/Ent L.J. (1999)

Ms. Chandler also is a regular guest lecturer including:

- "Licensing, Partnerships and Alliances" - University of Texas at San Antonio – Biotechnology Course lecture for the Masters of Technology Program
- "Technology and Intellectual Property Law for the General Practitioner" – Bexar County Women's Bar Association
- "Corporate Liability" - Information System Security Association National Symposium

EDUCATION

Ms. Chandler earned her B.S.B.A. degree in Finance, with highest distinction, from the University of Nebraska and her J.D. degree from the University of Virginia where she was Articles Editor for the Virginia Journal of Law and Technology.

TABLE OF CONTENTS

Appendices

NOTE: These sample policies are provided for general educational purposes only and are not intended to be a substitute for professional legal advice. Because the circumstances of each document retention policy are unique and because laws differ from state to state and differ by type of document, you should consult with legal counsel for advice on drafting a policy tailored to the needs of your company.

The expansion of the Internet has proven to be a great opportunity, but also a great challenge to business owners. The Internet is not a place or a destination. Rather, it is a network that allows users to provide, and to access, information located on different computers throughout the world. The Internet consists of a multitude of services, including the World Wide Web, electronic mail, chat,[2] newsgroups,[3] and file transfer protocol sites. In many ways, the Internet is like a very large local area network but without any specific controls over who is connected and what actions will be allowed. All aspects of the Internet are impacted by copyright law.

I. EMPLOYEE INTERNET USAGE AND OTHER EMAIL POLICIES

With the rapid growth of the Internet, employees have begun spending more time on their work computers, using both electronic mail ("e-mail") and accessing web pages on the Internet. It is apparent that e-mail has become one of the primary forms of communication in the workplace, replacing telephone and written communications.[4] In response, most companies have implemented policies regarding employee Internet usage and e-mail,[5] and because of the potential for employees to misuse company computers, the vast majority of employers have found it necessary to monitor employee e-mail and computer usage.[6] As a result, employees are becoming increasingly concerned with protecting their privacy when using work computers.[7] While maintaining privacy is certainly important, courts seem to agree that employers can legally monitor employee e-mail usage and Internet activity.[8] This is especially true when companies have implemented policies regarding employee e-mail and Internet usage,[9] thereby diminishing employee expectations of privacy by providing written notice.[10] Indeed, having evidence of a signed employee consent form limits employer liability from a potential invasion of privacy claim that may be brought by an employee.[11] For example, in *Borninski v. Williamson*,[12] plaintiff sued his former employer for intercepting and invading his e-mail. The defendant employer contended that even if it monitored his communications, plaintiff had consented by signing the company policy consent form.[13] Although plaintiff claimed that he was forced to sign the consent form as a condition for employment and it was therefore invalid, the court rejected this argument and pointed out that "no one forced plaintiff to sign the form and accept employment."[14] The court noted that it is, in fact, a common practice for employers to require employees to consent to the monitoring of their Internet activity in the workplace.[15] Therefore, it seems that employers would be wise to not only have a clear written computer usage policy in place, but should also have all

---

2 An online chat is an electronic means for users to talk to other users through their computers.

3 An online collection of postings related to a particular subject.

4 Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 115 (2005).

5 *See* Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 121-22 (2005) (listing some of the main reasons employers give to justify employee computer usage monitoring. These reasons include: avoiding reduction in employee work productivity, protecting confidential company information, and limiting potential employer liability for "sexual harassment arising from the transmission or display of sexually suggestive or demeaning emails through the company email system").

6 *See* 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute. (reporting that, as of 2005, over 85% of employers were monitoring employee computer usage in some form).

7 *See* Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 121-22 (2005). (explaining that employees feel that by monitoring their e-mail, employers are showing a lack of trust that erodes employee morale).

8 *See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that employee had no reasonable expectation of privacy when he communicated inappropriate comments to his supervisor over the company's e-mail); *see also* Garrity v. John Hancock Mutual Life Ins. Co., 2002 WL 974676 (D. Mass. 2002) (reaffirming that employer's interest in protecting employees from harassment outweighed plaintiff employee's privacy interest in his e-mail communications).

9 *See* Elise Bloom, Madeleine Schach, & Elliot H. Steelman, *Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety*, 29 WM. MITCHELL L. REV. 897, 900 (2003) (noting that "an employer is best protected if it announces its policies regarding employee monitoring and workplace privacy").

10 *See* United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding that an employee did not have a reasonable expectation of privacy in the record of his Internet usage because his employer placed him on notice of the company's clear Internet policy stating that it would "audit, inspect, and/or monitor" employees' Internet activity); *but see* United States v. Slanina, 283 F.3d 670 (5th Circ. 2002) (holding that plaintiff employee did have a reasonable expectation of privacy in files stored on his computer because the defendant employer did not have any policy in place and did not give plaintiff notice that his computer usage would be monitored).

11 *See generally* Borninski v. Williamson, 2005 WL 1206872 (N.D. Tex. 2005).

12 2005 WL 1206872 (N.D. Tex. 2005)

13 *Id.* at *12-13.

14 *Id.* at *13.

15 *Id* at *13.

employees sign forms acknowledging and consenting to employer monitoring of Internet and e-mail usage.

A. PRIVACY OF EMPLOYEE INFORMATION

1. Electronic Mail and Web Usage.

E-mail has become an "essential tool for increasing productivity and efficiency in the work place."[16] One benefit that e-mail has over other forms of communication is that e-mail messages are instantly "logged and recorded for future reference."[17] A disadvantage, however, is that e-mail can easily be used as a tool for bad activities of employees such as discrimination and harassment of fellow employees. This is bad news for employers.

It is important for employers to be vigilant in their monitoring of employees' use of technology. In fact, in 2000, the court in *Blakey v. Continental Airlines, Inc.,*[18] held that employers can incur legal liability for tolerating a hostile work environment.[19] There, an employee sued her former employer over harassing, retaliatory, and defamatory comments made by co-workers on an online computer bulletin board forum which was used by company employees.[20] The court pointed out that even though the bulletin board was not technically inside the workplace, "it may nonetheless have been so closely related to the workplace environment…that a continuation of harassment on the forum should be regarded as part of the workplace."[21] The court further noted that if the employer knew about the comments, it had a duty to stop the harassment.[22] Consequently, employers are encouraged to monitor employee Internet forums and "e-mail messages regularly for evidence of discriminatory material."[23]

Based on a recent survey by the American Management Association (AMA) and The ePolicy Institute, [24] employers have multiple concerns when they implement policies in relation to workplace computer use:

- 76% monitor workers' Website connections
- 65% of companies use software to block connections to inappropriate Websites[25]
- 36% of employers tracking content, keystrokes and time spent at the keyboard
- 50% store and review employees' computer files
- 55% retaining and reviewing email messages

Employees are also facing repercussions from their use. Based on the same study, 26% of employers have fired workers for misusing the Internet. Another 25% have terminated employees for e-mail misuse.

Most employers have policies in place to assure that employees are notified when they are being watched. Of those organizations that engage in monitoring and surveillance activities, fully 80% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; 82% let employees know the company stores and reviews computer files; 86% alert employees to e-mail monitoring; and 89% notify employees that their Web usage is being tracked.[26]

a. *Federal Law and Computer Privacy*.

The Electronic Communications Privacy Act of 1986[27] (ECPA) is a federal law which prohibits intercepting and accessing stored electronic communications without authorization. Although the ECPA seems to protect an individual's privacy interest in e-mail and computer usage, there are some important exceptions that actually allow employers to monitor employee communications. The first, known as the "service provider" exception, exempts employers from liability when they are monitoring or accessing information stored on their own computer systems.[28] The second exception to the ECPA is commonly referred to as the "business use" exception.[29] Under this exception, employers are allowed to monitor employees' electronic communications on equipment provided by the employer and used during the ordinary course of business.[30] The third exception applies when an employer obtains an

---

16 Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 115 (2005).

17 Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 115 (2005).

18 751 A.2d 538 (N.J. Sup. Ct. 2000).

19 *Id.* at 538.

20 *Id.* at 547.

21 *Id.* at 543.

22 *Id.*

23 National Institute of Business Management, You & The Law: Quick, Easy-to-Use Advice on Employment Law 2 (2002).

24 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute.

25 A 27% increase since the 2001 AMA and ePolicy Institute suvey.

26 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute.

27 18 U.S.C. § 2510 (1994).

28 18 U.S.C. § 2511 (2)(a)(i) (2002).

29 18 U.S.C. § 2510 (5)(a) (2002).

30 *Id.*

employee's consent to access information.[31] The last exemption under the ECPA, which allows employers to access employees' stored e-mails, has been recognized by the Third and Eleventh Circuits. In *Fraser v. Nationwide Mutual Insurance Co.*,[32] the Third Circuit Court of Appeals held that by accessing stored e-mails, the employer had not violated the ECPA because the interception was not contemporaneous with the transmission. The Eleventh Circuit, in *United States v. Steiger*,[33] also held that this was an exception to the application of the ECPA. Therefore, because the ECPA bans an interception only if it occurs at the same time as the transmission, it appears to be permissible for employers to access employees' stored e-mails.[34]

Employers can also review their employee's web activities, especially if they are given notice in advance that this may occur. In *United States v. Simons*,[35] the Fourth Circuit considered the legality of a government employer's search of an employee's office for evidence of child pornography and held that the employee did not have a legitimate expectation of privacy with regard to his employer's record of his Internet usage under the circumstances. Interestingly, in *United States v. Slanina*,[36] the Fifth Circuit Court of Appeals held that employee's expectation of privacy in his government office and files stored on his work computer was reasonable, given absence of any city policy placing him on notice that his computer usage would be monitored and fact that other employees did not have access to his computer. Even so, the court found that the O'Connor exception to the warrant requirement for work-related searches of public employees' space applied to search of computer for child pornography by supervisor who was also law enforcement official and that the search was reasonable.

b. *Texas Law and Computer Privacy*.

When employers monitor or intercept employee e-mails, the most common claim employees file, if not filing under the ECPA, is the common law tort of invasion of privacy.[37] In order to prove a claim for invasion of privacy, an employee must first establish that he or she had a reasonable expectation of privacy.[38] To protect themselves from such claims, employers should decrease employee expectation of privacy in e-mail and Internet communications by providing written notice informing employees that their communications will be monitored. In addition, an employee claiming invasion of privacy must also establish that the invasion was substantial and highly invasive.[39] Although the case law is limited, courts that have addressed the issue of employers monitoring employee e-mail have consistently ruled that there has been no intrusion into the employee's privacy. In *Smith v. Pillsbury Co.*,[40] plaintiff sued his former employer for invasion of privacy after he was terminated based on e-mail messages that his employer had obtained.[41] Rejecting plaintiff's claim for invasion of privacy, the court reasoned that "once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."[42] The court held this even despite the fact that the company had repeatedly assured its employees that all workplace e-mail communications would be kept confidential.[43] The court went on to state that even if the employee's rights were violated, "the company's interests in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[44]

Similarly, in *McLaren v. Microsoft Corporation*,[45] the Dallas Court of Appeals concluded that an employee did not have a reasonable expectation of privacy in e-mail messages that were transmitted over his employer's e-mail system and stored on the employee's office computer.[46] The plaintiff argued that because the e-mails

---

31 18 U.S.C. § 2511 (2)(d) (2002).

32 352 F.3d 107 (3rd Cir. 2003).

33 318 F.3d 1039 (11th Cir. 2003).

34 *Id.*

35 206 F.3d 392 (4th Cir. 2000).

36 283 F.3d 670 (5th Cir. 2002).

37 Specifically, "intrusion upon the plaintiff's seclusion or solitude or into his private affairs". There are two elements to this cause of action: (1) an intentional intrusion, physically or otherwise, upon anyone's solitude, seclusion, or private affairs or concerns, which (2) would be highly offensive to a reasonable person." McLaren v. Microsoft Corp., 1999 WL 339015 (Tex. App. Dallas 1999).

38 RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see e.g.*, Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996); McLaren v. Microsoft Corp., 1999 WL 339015 (Tex. App.-Dallas).

39 RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see e.g.*, Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996); McLaren v. Microsoft Corp., 1999 WL 339015 (Tex. App. Dallas).

40 914 F. Supp. 97 (E.D. Pa. 1996).

41 *Id.* at 101.

42 *Id*.

43 *Id.*

44 *Id*.

45 1999 WL 339015 (Tex. App. Dallas 1999).

46 *Id.* at *4.

were stored under his private password with his employer's consent, he had a legitimate expectation of privacy in that information.[47] In rejecting plaintiff's argument, the court noted that a storage locker and e-mail storage system were not the same,[48] and ultimately decided that the company's "interest in preventing inappropriate and unprofessional comments" over its e-mail system" outweighed the plaintiff's privacy interests.[49]

2. Telephone Usage.

Because courts have granted employers great latitude when it comes to monitoring employee e-mail and computer usage, many employers have assumed that this freedom extends to employee telephone usage as well. Consequently, more and more employers have begun monitoring employee telephone usage,[50] and employers have begun informing employees that such monitoring is taking place.[51] As a result of this monitoring, 6% of employers who were surveyed in 2005 reported that they had terminated employees for misusing office phones.[52]

Employers should be warned, however, that the same flexibility that applies to monitoring computer usage does not actually apply to telephone usage. While email communication over company servers is considered reviewable by employers, courts have held that telephone conversations are highly protected and that using a telephone is a more private form of communication.[53] As it stands now, the law suggests that employees do have some privacy rights, even on a company-owned telephone system.[54] However, employees' privacy rights seem to be limited to personal conversations conducted on an employer's telephone system, not business conversations.[55] Generally, under Texas and federal law, employers can monitor employee telephone usage for business purposes (such as customer service and quality control) and where at least one party to the conversation has consented to the monitoring. Employee consent can often be implied based on company policies.[56]

a. *Federal Law and Telephone Privacy*.

The federal Electronic Communications Privacy Act of 1986 (ECPA) also applies to telephone communications. While the ECPA generally "prevents employers from listening to conversations," there are a few exceptions that allow employers to monitor employee telephone use without violating this law.[57] First, there is a "business use exception" that allows employers to monitor employees' business calls. In *Briggs v. American Air Filter Co., Inc.*,[58] the Fifth Circuit held that employer monitoring of employee's phone call did not violate the

47 *See id.* (arguing that because one court had recognized an employee's reasonable expectation of privacy in his locker for which he provided his own lock, this court should also find he had a reasonable expectation of privacy in his password protected e-mails). K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. Houston 1st Dist. 1984), writ refused n.r.e., 686 S.W.2d 593 (Tex. 1985).

48 *See id.* (pointing out that while a locker is a discrete physical place where items can be kept separate and apart from other employees, e-mails by there nature are initially transmitted over a network where third parties can easily access them).

49 *Id.* at *5.

50 *See* 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute (stating that more than 50% of companies surveyed reported that they monitor employee telephone usage).

51 *See* 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute (reporting that the number of companies that monitor telephone usage has grown in the past few years and that over 70% of employers are notifying employees about the telephone monitoring); *see also* 2 LAURA M. FRANZE, ESQ., TEXAS EMPLOYMENT LAW §28:4 (2005) (suggesting that employers have written policies posted in a visible area such as stickers on all telephones reminding employees that calls may be subject to monitoring). Although the Fifth Circuit has not addressed the issue of regular monitoring of employee telephone usage, the Tenth Circuit, in *James v. Newspaper Agency Corporation*, upheld an employer's right to regularly monitor employee telephone usage when all employees were notified in writing. 591 F.2d 579, 581 (10th Cir. 1979).

52 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY, American Management Association (AMA) and The ePolicy Institute.

53 Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); *see also* Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (holding that once the personal nature of a call was established, any continued monitoring would violate the ECPA).

54 JOHN F. BUCKLEY & RONALD M. GREEN, 2006 STATE BY STATE GUIDE TO HUMAN RESOURCES LAW §8.06 (2006).

55 *Id.; see also* Oyoyo v. Baylor Health Network, Inc., 2000 WL 655427 at *7 (N.D. Tex. May 17, 2000) (holding that employer's monitoring of employee's telephone usage was justifiable, and "because the phone was provided for business purposes, employee did not have a legitimate privacy interest in her use of the office phone").

56 Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

57 JOHN F. BUCKLEY & RONALD M. GREEN, 2006 STATE BY STATE GUIDE TO HUMAN RESOURCES LAW §8.06 (2006).

58 630 F.2d 414 (5th Cir. 1980).

ECPA.[59] Instead of relying on whether or not the employee had an expectation of privacy, the court relied on several factors to reach its decision, including: "a) the telephone call in question was a business telephone call, not a personal one; b) the employer's listening-in was limited in purpose and time; and c) the employer had specific suspicions and listened only long enough to confirm that the employee was discussing business matters."[60] Additionally, employers are allowed to monitor employees' telephone usage if there are legitimate business reasons for doing so.[61] For example, in *Arias v. Mutual Central Alarm Service, Inc.*,[62] the court decided that the employer had two adequate business reasons for recording phone calls: "to monitor the security information that was of a sensitive nature, and to maintain an accurate record of emergency calls."[63] However, courts have held that not all reasons for monitoring telephone calls are necessarily sufficient. In *Deal v. Spears*,[64] the court found that suspecting an employee of theft was not a sufficient reason to listen to employee's telephone conversations and that the employer had violated the ECPA by doing so. The second exception to these statutes is consent.[65] Therefore, it is important and necessary for employers to document employee consent to monitor and also to clearly explain what is and what is not private. Employers can accomplish this by adopting written policies concerning employee electronic communications and ensuring that employees sign acknowledgment and consent forms regarding company telephone policies.

b. *Texas Law and Telephone Privacy*.

According to Texas law, intercepting or tape recording conversations is allowed as long as one party consents.[66] Therefore, an employer may tape conversations between the employer and his or her employee without the employee's consent (and vice versa).[67] Non-consensual third party interception, however, is illegal.[68]

3. Electronic Activity Tracking.

As the cost of Assisted Global Positioning or Global Positioning Systems (GPS) technology has dropped significantly over the last decade, employers are increasingly turning to GPS as a means by which to track their mobile workforce. In so doing employers are citing a need to limit employer liability and to increase business efficiency. For instance, a GPS device attached to an employee vehicle provides the employer with the ability to monitor vehicle speed and, thereby, the ability to discipline employees whose reckless driving might lead to employer liability. Likewise, GPS monitoring can provide for greater fleet efficiency by identifying less productive employees, allowing for recovery of stolen vehicles, and eliminating inefficient routes.

Based on a recent survey of employers, employers who use GPS satellite technology are in the minority, with only 5% using GPS to monitor cell phones; 8% using GPS to track company vehicles; and 8% using GSP to monitor employee ID/Smartcards.

As GPS monitoring of the mobile workforce has become more and more common, employees have begun to raise privacy concerns. For instance, employees have expressed concern that innocuous actions such as sitting in traffic will be interpreted by the employer as unproductive behavior that might ultimately result in dismissal. The greatest privacy concern, however, has been the potential use of GPS technology to monitor what employees do away from the office while not on duty. Concerns such as these have lead to employee resistance to the use of GPS monitoring. Such privacy concerns led UPS employees subject to GPS monitoring to negotiate a clause in their collective bargaining agreement that would place limits on the type and amount of information UPS may obtain via GPS monitoring.[69] But as discussed below, current legal

---

[59] *Id.* at 420; *but see* Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (reiterating that employers cannot justify monitoring employees' personal calls under the "business use" exception and that doing so violates the ECPA).

[60] *Id.* at 420.

[61] JOHN F. BUCKLEY & RONALD M. GREEN, 2006 STATE BY STATE GUIDE TO HUMAN RESOURCES LAW §8.06 (2006).

[62] 202 F.3d 553 (2d Cir. 2000).

[63] *Id.*

[64] 980 F.2d 1153 (8th Cir. 1992).

[65] *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (proposing that implied consent may be found if an employee has been warned not to make personal calls from particular business phones).

[66] TEX. CODE CRIM. PROC. ANN. art. 18.20 §1(4) (Vernon 2005), amended by 2005 Tex. Sess. Law Serv. Ch. 390, 889 (S.B. 1461, 1551) (effective September 1, 2005); TEX. PENAL CODE ANN. §16.02 (c)(4)(A) (Vernon 2003); *see also* Hall v. State, 862 S.W.2d 710 (Tex. App.—Beaumont 1993, no writ) (stating that wiretap statute restrictions do not apply when private individual consents to having conversation with defendant taped); Esterline v. State, 707 S.W.2d 171 (Tex. App.—Corpus Christi, 1986, writ ref'd) (holding that article 18.20 was not applicable in tape recording of conversation between defendant and informer where only informer had consented to having conversation taped).

[67] 2 LAURA M. FRANZE, ESQ., TEXAS EMPLOYMENT LAW §28:4 (2005).

[68] TEX. CODE CRIM. PROC. ANN. art. 18.20 (Vernon 2005).

[69] CHRISTOPHER LINDQUIST, SWEATSHOPS WITHOUT WALLS (MAY 15, 2005) CIO MAGAZINE (AVAILABLE AT

protections fail to provide employees much recourse when employers invade their private lives by means of GPS monitoring.

Even in the off-duty or off-site context, the courts tend to recognize a right of the employer to investigate and monitor employee activity when it relates to the business interest of the employer.[70] This is to allow the employer the ability to monitor such things as employee drug use, sexual activities, and other activities deemed repugnant by the employer that occur away from the office. The need to investigate these activities has justified "a variety of [investigative] techniques [including] surveillance, wiretapping, interviews, polygraphs, and medical examinations."[71] The use of GPS monitoring of off-duty conduct is such a recent phenomenon that there has yet to be much scrutiny by the courts. But the judicially permitted use of other investigative techniques indicates that potential plaintiffs would have little success claiming the impermissibly of such GPS monitoring.

On the whole, federal law is simply not broad enough to provide protection for employees who are subject to employer GPS monitoring. The federal Electronic Communications Privacy Act of 1996[72] is frequently cited to limit other forms of surveillance techniques. The Privacy Act imposes consent and authorization requirements for employee monitoring that involves the monitoring of a communication. But by its own words, the Privacy Act does not cover "any communication from a tracking device"[73] and thus offers no protection to employees under GPS surveillance.

Various state laws potentially offer more protection against GPS monitoring of employees. Most of these laws, however, were not enacted for the purpose of guarding against such an activity. Further, GPS monitoring of employees is such a recent issue that there is no case law interpreting the applicability of these statutes. A short summary of the potentially applicable laws are as follows:

a. California: Cal. Penal Code § 637.7 makes it a misdemeanor for any person to use an electronic tracking device to determine the location or movement of a person without the consent of the person who is being tracked.

b. Connecticut: CT ST § 31-48b limits the ability of an employer to use an electronic surveillance device or system for purposes of monitoring the activities of their employees "in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions."

c. Hawaii: HI ST § 803-42(a)(7) makes it a class C felony for any person to install or use a mobile tracking device without first obtaining a warrant or other order authorizing the use of such a device, or obtaining consent from the party who is being tracked.

d. Tennessee: T.C.A. § 39-13-606(a) makes it illegal for any person to install an electronic tracking device in an motor vehicle without the consent of the owners of that vehicle for the purposes of following the occupants of the vehicle.

e. West Virginia: W. Va. Code, § 21-3-20 limits the ability of an employer to use an electronic surveillance device or system for purposes of monitoring the activities of their employees "in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions."

In recent years various state legislatures have undertaken to enact legislation that would provide for greater protection against employee surveillance. For instance, in its 2003-04 session the California Legislature entertained a bill that would have required an employer to give notice of its intent to collect information on employee activities by means of "electronic devices."[74] This bill ultimately ended up being vetoed. Likewise, Michigan and Pennsylvania recently entertained bills that targeted employer monitoring of electronic communications and that required detailed employee notification of such monitoring.[75] Finally, the Massachusetts Legislature recently had before it an act that would have allowed an employer to use electronic surveillance to collect information so long as the information is collected at the employer's premises and is confined to the employee's work. This act would have entirely prevented employers from electronically monitoring their vehicles or mobile workers during

HTTP://WWW.CIO.COM/ARCHIVE/051505/MONITOR_SIDEBAR_ONE.HTML).

[70] 1 William E. Hartsfield, Investigating Employee Conduct § 7:15 (2004).

[71] *Id.* at § 7:15.

[72] 18 U.S.C. §§ 2510-2521, 2701-2712 (2000).

[73] 18 U.S.C. § 2510(12)(c).

[74] S.B. 1841, Reg. Sess. (Cal. 2004).

[75] S.B. 893, 187th Gen. Assem., Reg Sess. (Pa. 2003); S.B. 675, 92d Legis., 1st Reg. Sess. (Mich. 2003). Neither of these proposed bills were ever enacted by their respective legislatures.

business hours,[76] which may explain why it never made it out of committee.

Employers may want to consider implementing GPS tracking policies and procedures if they have numerous offsite employees or employees utilizing company vehicles. If such a policy is implemented, it should be a clearly defined policy on its right to access or monitor certain employee activities included in the employee manual disseminated by the employer. Such policy or guideline also should inform employees as to when they will be monitored, and how the information from such monitoring will be used.

By having such policies in place, the employer can reduce the risk that the employee had any expectation of privacy in using company owned equipment. However, employers must ensure that the use of location tracking devices is consistent with the policy it has established and is solely for legitimate business-related purposes such as monitoring productivity or investigating suspected work-related misconduct. Also, whenever possible, it should limit monitoring or tracking to employees' work time only.

B. SPAM

The key controlling law which advertises need to be aware is he federal "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (the "Act"). The Act is directed toward the dissemination of "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."

Although the Act is commonly referred to as the CAN-SPAM Act, it does not have an anti-marketing, privacy-at-all-costs bias. The Act actually permits the unlimited dissemination of commercial e-mail unless the message headers contain false or misleading information. Commercial messages must contain clear and conspicuous identification as an advertisement or solicitation (unless the recipient has given prior express consent to receive such messages), clear and conspicuous means for the recipient to opt-out (an opportunity to unsubscribe and receive no more messages from the sender), and the sender's valid physical postal address. Also, commercial messages may not be sent to individuals who previously opted-out or to an e-mail address that was automatically or deceptively obtained.

1. Summary of Unlawful Activities

The Act proscribes the following:

(1) Sending commercial or transactional e-mail messages that contain false or materially misleading header information.

(2) Sending commercial e-mail messages that the sender knows have misleading subject headings.

(3) Sending commercial e-mail messages that do not contain a clear return address or other Internet-based mechanism that functions for opt-out use for 30 days after transmittal.

(4) Sending commercial e-mail messages to a recipient more than 10 business days after the recipient submitted a request to unsubscribe.

(5) Transferring the e-mail address of an individual whom the seller knows has requested not to receive commercial e-mail messages.

(6) Sending commercial e-mail messages to addresses that the sender knows were obtained from an automated address generation means or a third party who collected the addresses with misleading automated means, i.e., notification that the address would not be distributed.

(7) Using automated means to register for multiple e-mail accounts or online user accounts for sending prohibited commercial e-mail messages.

(8) Accessing a computer without authorization to knowingly relay or re-transmit prohibited commercial e-mail messages.

(9) Knowingly allowing one's business to be promoted in commercial e-mail messages that contain false or materially misleading header information if an economic benefit is expected to be received from such promotion, and failing to take reasonable steps to prevent or report the transmission of such messages.

(10) Sending commercial e-mail that does not contain clear and conspicuous identification that the message is an advertisement or solicitation (unless the recipient has given prior express consent to receive such messages), clear and conspicuous notice of the opportunity to opt-out of receiving messages from the sender, and a valid physical postal address of the sender.

While it is intended to establish national standards for dissemination of commercial e-mail, the Act generally excludes messages that primarily facilitate or confirm transactions; provide warranty or recall information regarding products used or purchased by the recipient; or provide information regarding a subscription, membership, employment, or other commercial

[76] S.B. 2190. 183d Gen. Court, Reg. Sess. § 2(a) (Mass. 2003).

relationship. The Act also addresses pornography, but only with the requirement that, unless the recipient has given consent, e-mails include a subject line or first page warning if the message contains sexually oriented material.

2. Enforcement

Violations of the Act are considered unfair or deceptive practices. The FTC, and in some cases, States, can seek injunctions and statutory damages up to $2 million per suit, but the cap does not apply to violations involving false or misleading header information. Courts may award attorneys' fees. Courts also may award treble statutory damages for willful violations, automated e-mail address harvesting and multiple account registration, and message relay through computers accessed without authorization.

The Act authorizes other federal agencies such as the Federal Reserve Board, the FDIC, the SEC, and the Department of Agriculture to file civil suits for relevant violations. Internet Service Providers are also permitted to bring civil actions in federal district courts. The Act specifies criminal penalties, including five year jail sentences, for egregious violations. Spammers can also suffer forfeiture of equipment used in illegal acts, and forfeiture of real and personal property traceable to revenue from such acts. To aid enforcement, Congress required the FTC to prepare a plan for awarding up to 20% of the total civil penalty assessed against a violator to the first person to identify that violator.

3. Do-Not-Email List; Wireless Messages

While the issue of a national registry similar to the national Do-Not-Call list proved too controversial for resolution within the Act, the Act requires the FTC to create a plan for a national Do-Not-Email registry and a report on the plan's feasibility. The Act also addresses wireless spamming by requiring the FCC to submit rules for protecting cell phone users from unwanted commercial messages.

4. Preemption; Primary Purpose Regulations

The Act generally preempts State laws, except for the portions that prohibit falsity or deception in commercial e-mail. Because the Act focuses on e-mail messages the primary purpose of which is the commercial advertisement or promotion of commercial products or services, the Act requires the FTC to issue regulations defining criteria for determining the primary purpose of an e-mail message.

5. Practitioner Note

Unlike recent UK and California laws, the Act is not a blanket prohibition of spamming, but it does impose certain requirements on the dissemination of commercial e-mail messages. Neglect of those requirements can subject violators to substantial fines and possible jail sentences.

II. DOCUMENT RETENTION POLICIES

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.[77] Many companies routinely adopt retention policies for hard copy documents, but few companies consider digital and electronic data in their policies. It is important, however, for attorneys to advise their clients to have written document retention policies for electronic data to avoid unnecessary risks and expenses.

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.[78] 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.[79] 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.[80] Although there was no evidence of willful misconduct, the court was outraged by

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

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

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

[80] 169 F.R.D. 598 (D. N.J. 1997).

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."[81] 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.[82] The Defendant sent emails and voicemails to all of its employees advising them to save all relevant documents.[83] The Defendant, however, failed to stop its back-up tapes from being recycled or taped-over.[84] 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.[85] The Court determined that the appropriate sanction against the Defendant was a spoliation inference.[86] 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.[87] 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."[88]

But when litigation can reasonably be anticipated, attorneys have an obligation to advise clients to take reasonable steps to preserve records subject to discovery.[89] 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.[90] Counsel, however, failed to warn its client to not delete or recycle back-up dates of technological data.[91] The Court ordered the Defendant to bear the substantial cost of restoring the back-up tapes.[92] 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*.[93] 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.

[81] *Id.* at 613.

[82] 10 Mass L. Rptr. 189 (Mass. 1999).

[83] Id. at 9.

[84] *Id.*

[85] *Id.*

[86] *Id.* at 11.

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

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

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

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

[91] *Id.* at 424.

[92] *Id.* at 426.

[93] 836 F.2d 1104 (8th Cir. 1988).

1. Guidelines

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
- Allow alternatives to, or even suspension of, document-destruction procedures when a duty to preserve arises.[94]

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.[95] When a document retention policy is not uniformly applied, courts will wonder whether it was created in bad faith.

3. Recent Development – Government's Eyes are Prying

U.S. Attorney General Alberto Gonzales recently requested that AOL, Microsoft, and Google retain customer records for at least two years—so that law enforcement officials will be able to tap into them if needed.[96] The battle over what to do with all that data has just begun. As governments increase their prying, businesses are struggling to keep records private.

III. PRIVACY ISSUES

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?,[97] 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.[98]

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 recently stole the personal records of at least 1,500 employees and contractors guarding the U.S. nuclear

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

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

[96] Microsoft, AOL, Google Asked by U.S. to Keep Internet Records. BLOOMBERG (June 1, 2006) *available at* http://www.bloomberg.com/apps/news?pid=10000103&sid=af87XTpBzphA.

[97] *See* fn. 123.

[98] *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.

weapons stockpile.[99] That news came days after the VA admitted it lost the personal information of 2.2 million active-duty military personnel.[100] Consumers are understandably getting nervous. Twenty percent of 51,000 adults surveyed by the Ponemon Institute last year said they terminated their relationship with a company after finding out their personal information may have been compromised.[101]

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.[102] 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.[103]

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

[99] *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.

[100] *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.

[101] 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.

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

[103] *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.[104]

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.[105] 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.[106]

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."[107] 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.[108]

---

[104] *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).

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

[106] *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.

[107] *See* 15 U.S.C. § 1681 et. seq.

[108] *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.[109]

GLBA has broader applicability than FCRA. The FTC has interpreted GLBA[110] to give privacy protection to any individually identifiable information[111] gained by any company that engages in an activity related to finance.[112] 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.[113]

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[114] and statutory approaches, [115] 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.[116] 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.[117] 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.[118] Any records destroyed should be destroyed by shredding, erasing, or modifying the sensitive information so it is unreadable or undecipherable by any means.[119]

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.[120] 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.[121]

---

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

[110] 15 U.S.C. § 6801, et. seq.

[111] *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)).

[112] 16 C.F.R. § 313.3(k)(2)

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

[114] *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

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

[116] Tex. Bus. & Com. Code § 48.102.

[117] Tex. Bus. & Com. Code § 48.103.

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

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

[120] 15 U.S.C.A. §§ 6501 et seq.

[121] 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.[122]

• 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.[123]

California and Tennessee have enacted versions of consumer privacy laws which regulate the liability incurred by private entities for intentionally or knowingly disclosing consumer information.

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

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

1. California

In July 2003, California passed the Security Breach Information Act ("CSBIA"),[124] 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. [125] CSBIA was the first law in the U.S. expressly creating such liability.

While the CSBIA only applies to security breaches involving the personal information of California residents, national companies typically do not segregate data regarding California customers from other customer or employee data, therefore, this will affect organization-wide security practices. The law defines "personal information" as an individual's first name or first initial, combined with the last name, plus any one of the following identifiers: (1) Social Security number, (2) driver's license number or California Identification Card number or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the account. Any information lawfully made publicly available does not constitute "personal information" for the purposes of this statute.[126] If both the individual's name or the accompanying identifiers are encrypted, then the data does not constitute "personal information." This carve-out may lead to expanded adoption of encryption for data at rest in a company's systems. The statute does not, however, require strong encryption or address the appropriateness of particular forms of encryption.

California defines "breach of the security of the system" as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.[127] Disclosure may be made through written, electronic, or substitute notice.

If a business fails to promptly provide the required notices to individuals after a security breach, any customer injured by the violation may bring a civil action against the business to recover damages. Therefore, companies subject to CSBI should have security incident response scenarios prepared, because the law reflects the realization that the damages resulting from identity theft may be minimized if individuals have the opportunity to respond quickly.

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

[125] *Id*.

[126] *Id*.

[127] *Id*.

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.[128] 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.[129] 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.[130] California leads the trend in consumer privacy laws.

California's notice statute, the CSBIA, has been a model for the following twenty-one states which have enacted similar statutes addressing disclosure of customer information in an attempt to help protect consumers:

2. Arkansas

Any person or business who acquires, owns, or licenses computerized data that contains personal information of a citizen of Arkansas must notify that citizen of a security breach and of the possibility that their unencrypted personal information has been obtained by an unauthorized person. Such disclosure shall be made in the most expedient time and manner possible; and shall be made via written notice, electronic mail, or substitute notice if applicable.[131] This statute was enacted in 2005, and does not apply to a person or business that is regulated by state or federal law which provides a greater protection to consumer information than provided by this chapter.[132] Arkansas was one of the three states that were the first to adopt notice requirements and an exception in attempt to provide greater protection to consumers.[133]

3. Connecticut

Connecticut's version of the breach of security statute, contains the same provisions and requirements as the California statute mentioned above. Connecticut enacted their Breach of Security statute in 2005.[134]

4. Delaware

When an individual or commercial entity becomes aware of a security breach, a good faith, prompt and reasonable investigations is to be conducted to determine the likelihood that personal information has been or will be misused.[135] The individual or commercial entity is required to give notice as soon as possible to the affected Delaware resident only if the investigation found that there was or is likely to be a misuse of a Delaware resident's information.[136] This statute was enacted in 2005, and does not apply to a person or business that is regulated by state or federal law that provides a greater protection to consumer information than provided by this chapter. Delaware was one of the three states that were the first to adopt notice requirements and an exception in attempt to provide greater protection to consumers.[137]

5. Florida

This statute differs from California in that it only requires notice after a breach has been determined. A "breach of security of the system" occurs when unlawful or unauthorized acquisition of computerized data *materially compromises* the security, confidentiality, or integrity of personal information maintained by the person.[138] This statute was enacted in 2005, and does not apply to a person or business that is regulated by state or federal law that provides a greater protection to consumer information than provided by this chapter. Florida was one of the three states that were the first to adopt notice requirements and an exception in attempt to provide greater protection to consumers.[139]

6. Georgia

This statute contains the same provisions and requirements as the California statute mentioned above with two exceptions, (1) this statute applies to any information broker, and (2) "personal information," "breach of the security of the system," and the manner in which notice is to be given are not defined.[140]

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

[129] *Id.*

[130] *Id.*

[131] *See* ARK. CODE ANN. 4-110 (West 2006).

[132] *See* ARK. CODE ANN. 4-110-106 (West 2006).

[133] *See* Satish M. Kini, & James T. Shreve, *Notice Requirements: Common themes and Differences In The Regualtory and Legislative Responses to Data Security Breaches*, North Carolina Banking Institute (March 2006).

[134] *See* CONN. GEN. STAT. ANN. § 36a-701b (West 2006).

[135] *See* DEL. CODE ANN. tit. 6 § 12B-102 (West 2006).

[136] *Id.*

[137] *See* Satish M. Kini, & James T. Shreve, *Notice Requirements: Common themes and Differences In The Regualtory and Legislative Responses to Data Security Breaches*, North Carolina Banking Institute (March 2006).

[138] *See* FLA. STAT. ANN. § 817.5681 (West 2006).

[139] *See* Satish M. Kini, & James T. Shreve, *Notice Requirements: Common themes and Differences In The Regualtory and Legislative Responses to Data Security Breaches*, North Carolina Banking Institute (March 2006).

[140] *See* GA. CODE ANN. § 10-1-912 (West 2006).

7. Illinois

Illinois requires that any data collector that owns or licenses personal information or maintains computerized data that includes personal information concerning an Illinois resident, notify that resident if there has been a breach of the security system.[141] This statute does not define a "breach of the security system" but does include other provisions similar to California.

8. Indiana

This statute only applies to state agencies that own or license computerized data that includes personal information.[142]

9. Louisiana

Louisiana's notification statute includes, any person who conducts business in the state along with any agency or individual that maintains, owns, or licenses computerized data that includes personal information.[143] Any financial institution that is in compliance and subject to the Federal Interagency Guidance is exempt from this Chapter.[144]

10. Maine

The "Notice of Risk to Personal Data Act," goes beyond California's statute to encompass definitions of a "person", "unauthorized person," "system," "information broker," and is enforced by the Department of Professional and Financial Regulation.[145] This statute has been revised to limit liability to an information broker but instead to a "person" but these revisions will not take effect until January 31, 2007.[146]

11. Minnesota

Minnesota's version of the breach of security statute, contains the same provisions and requirements as the California statute mentioned above with the addition of the exception for financial institutions that are in compliance and subject to the Federal Interagency Guidance.[147]

12. Montana

Similar to Florida, the significant variance in Montana's statute is the definition of a "breach of security of the system" which occurs when unlawful or unauthorized acquisition of computerized data *materially compromises* the security, confidentiality, or integrity of personal information maintained by the person.[148] This statute became effective March 1, 2006 and in all other ways models the California statute.

13. Nevada

As does Illinois, Nevada requires that any data collector that owns or licenses personal information or maintains computerized data that includes personal information concerning an Illinois resident, notify that resident if there has been a breach of the security system.[149] This statute does not define a "breach of the security system" but does include other provisions similar to California.

14. New Jersey

New Jersey's notification statute applies to any business or public entity that compiles or maintains computerized records that include personal information alone or on behalf of another business or public entity.[150] The remainder of the statute includes all other notification requirements set forth in the California statute.

15. North Carolina

Under the "Identity Theft Protection Act," this protection statute requires any business in North Carolina to provide notice to their consumers when a security breach has occurred, regardless of the form (e.g. paper, computerized, or otherwise) their personal information is kept in.[151] Any financial institution that is in compliance and subject to the Federal Interagency Guidance is exempt from this Chapter.[152]

16. North Dakota

North Dakota's notice statute simply states that any person who conducts business in the state or owns computerized data that contains personal information must notify the consumer of a breach in the security system.[153] Any financial institution that is in compliance and subject to the Federal Interagency Guidance is exempt from this Chapter.[154]

17. Ohio

Similar to Main, Ohio's notice statute goes beyond California's statute to encompass definitions of a "person", "unauthorized person," "system," "business entity," and is enforced by the Attorney General.[155] Any

[141] *See* IL COMP. STAT. ANN. 817§ 530/10 (West 2006).

[142] *See* IOWA CODE ANN.§ 4-1-11-5 (West 2006).

[143] *See* LA REV. STAT. ANN. § 51:3074 (West 2006).

[144] *See* LA REV. STAT. ANN. § 51:3076 (West 2006).

[145] *See* ME REV. STAT. ANN. tit.10 § 1349 (West 2006).

[146] *See* ME REV. STAT. ANN. tit.10 § 1350-A (West 2006).

[147] *See* MINN. STAT. ANN. § 325E.61 (West 2006).

[148] *See* MONT. CODE. ANN. § 30-14-1704 (West 2006).

[149] *See* NEV REV. STAT. § 603A.220 (West 2006).

[150] *See* N.J. STAT. ANN. § 56:8-163 (West 2006).

[151] *See* N.C. GEN. STAT. ANN. § 75-65 (West 2006).

[152] *Id.*

[153] *See* N.D. ADMIN. CODE § 51-30 (West 2006).

[154] *Id.*

[155] *See* OHIO REV. CODE ANN.§ 1349.19 (West 2006).

financial institution that is in compliance and subject to the Federal Interagency Guidance is exempt from this Chapter.[156]

18. Pennsylvania

This notice statute does not take effect until June 20, 2006. Pennsylvania's notice statute applies to an entity that maintains, stores, or manages computerized data that includes personal information.[157] This state also defines a breach as an unauthorized access which *materially affects* the security of personal data.

19. Rhode Island

Rhode Island's notice statute differs from California's in that it does not define "personal information" or "breach of security," and it provides an exemption to any financial institution that is in compliance and subject to the Federal Interagency Guidance.[158]

20. Tennessee

Tennessee's notice statute defines a breach as an unauthorized acquisition of unencrypted computerized data that *materially compromises* the security, confidentiality or integrity of personal information maintained by the information holder.[159] This statute also uses the term "information holder" which is defined as any person or business that conducts business in the state or agency of Tennessee or any of its political subdivisions that owns or licenses computerized data that includes personal information.

21. Texas

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."[160]

22. Washington

Washington's version of the breach of security statute, contains the same provisions and requirements as the California statute mentioned above. Washington's Breach of Security statute became effective July 24,2005.[161]

23. Practitioner Notes.

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. An business owner's intent when a disclosure of consumer information occurs, is not relevant in establishing liability under the above mentioned notice statutes.[162] 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 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.

[156] *Id.*

[157] *See* 73 PA. STAT. ANN. § 2303 (West 2006).

[158] *See* RI GEN. LAWS. 1956 § 11-49.2-3 (West 2006).

[159] *See* TENN. CODE. ANN. § 47-18-2107 (West 2006).

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

[161] *See* WASH. REV. CODE ANN. § 19.255.010 (West 2006).

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

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.[163]

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.

IV. WEB TRACKING REPORTS AND TRADEMARKS

If your company receives web tracking reports[164], it should consider reviewing those with an eye to what those reports may tell you about your trademarks. For example, if your company is facing a decision concerning where you would like to seek international protection for your mark, you may look at your web tracking report to determine where your website's visitors are from. For example, if a large number of your hits are coming from domains such as .uk or .za, this would indicate that you have a lot of visitors to your site from the United Kingdom and South Africa, respectively. Such an analysis could provide valuable insight concerning countries where trademark protection is merited.

Additionally, it may be helpful to determine if other people on the Internet are capitalizing on your trademark. For example, many of these reports will indicate the prior site visited by visitors to your website. For example, in the case of our law firm's site, if we review the report and see that a large number of visitors to our site are coming from a domain named Jackson Walken.com, with an "en" as opposed to an "er", then we may need to visit this domain to determine if it is someone capitalizing on our firm's trademark. Further, this information could be useful in showing a likelihood of confusion if infringement litigation were to ensue.

Web tracking reports can be obtained from most ISP's. Additionally, some website owners, through third part software or subscription services, obtain even more detailed information about visitors to their websites.

V. COPYRIGHT MISUSE

There is a common misconception that content available on the Internet is fair game for any use by web surfers everywhere. For example, one Internet entrepreneur was in the process of setting up a site. In an effort to add content, he was including links with the logos of relevant local government agencies. He sent an email to the administrator of one agencies' site requesting a logo, and justified his request by noting that he already had taken the logos from two other municipalities' websites.[165] This phenomenon, based in part on the mistaken belief that items posted on the Internet are neither protected nor protectible, abounds.[166]

Copyright covers a variety of original works from literary writings, photographs and other images to computer programs and the creative aspects of databases.[167] Most of the text, images, multimedia works, and software that are transmitted over the Internet are copyrightable works. Copyright law impacts all aspects of the Internet, ranging from software programs, sound recordings and musical performances, literary works, motion pictures and other audiovisual works, and visual arts, in addition to the more general content published on a site.

The copyright owner has the right to reproduce the work,[168] to prepare derivatives of the work,[169] to distribute or disseminate copies,[170] to perform the work publicly, and to display the work.[171] When a work is

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

[164] Web tracking reports are the reports which provide insight into a website's visitors. These reports include information such as the number of visitors to a page, the prior site visited, where people go when they leave the site, which search engine query they used to find the site, and what country the visitor resides in.

[165] Shirley Duglin Kennedy, *Linking Policies for Public Websites: In Our Increasingly Litigious Society, They Are Now Essential*, INFORMATION TODAY (Nov. 2000).

[166] *See* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 50-51 (1994) ("The current copyright statute has proved to be remarkably education-resistant . . . . [O]ur current copyright statute could not be taught in elementary school, because elementary school students couldn't understand it. Indeed, their teachers couldn't understand it.").

[167] For example, in a computer program, copyright covers the program's instructions and its code, but not its functions or use (areas typically protectable through the patent process).

[168] Only the copyright owner can make, or allow others to make, copies of the work.

[169] Derivatives include expansions, abridgements and other modified forms of the work.

[170] This right includes distribution through electronic means.

[171] The display of a work includes the display of the work on a website.

created, a copyright is automatically secured.[172] A copyright can also be registered with the U.S. Copyright Office to expand the rights of the holder. Through registration, the copyright owner is able to enforce its rights against an infringer who copies, sells or distributes the work without authorization. The remedies include an injunction to prevent continued infringement and damages.

Computer technology has revolutionized the creation, reproduction, and dissemination of copyrighted works, and has opened the door to copyright abuse on a scale not previously known.[173] It is now possible for digital copies of intellectual property to be produced without any loss of quality, resulting in the ability to make unlimited, identical, high-quality copies. With the advent of popularly-priced scanners, it has become impossible to keep printed material off the Web, as many providers of copyrighted materials have discovered.[174] Penalties for this kind of violation, even without an economic motive, have recently been increased,[175] but violations are still widespread. It is important for business owners to institute policies to avoid infringement.

A. WEBSITE TEXT IS COPYRIGHTABLE

A standard website would be protected as either a literary work or as an audiovisual work, and, therefore, is copyrightable. Section 102(a)(1) of the Copyright Act provides that "literary works" constitute protectable works of authorship.[176] Literary works include novels, nonfiction prose, poetry, newspaper articles, magazine articles, computer software, software manuals, training manuals, catalogs, brochures, the text in ads, and compilations, such as business directories. The essence of a literary work is that it consists of "verbal or numerical symbols or indicia," not that it is presented in any particular format.[177] A work is protected under copyright the moment it is created and fixed in a tangible form so that it is perceptible either directly or with the aid of a machine or device.[178] For example, once the text is fixed in the website, it is afforded the same protections as any other literary work.[179]

Alternatively, depending on how dynamic the site is, it may be protected as an audiovisual work.[180] An

---

[172] This common law copyright can be designated by noting "Copyright © [year] [name of owner]; however, this notice is not necessary for a copyright to exist.

[173] Websites, on-line services, bulletin boards, and file transfer protocol (or FTP) servers are ideal media for replicating and transmitting copyrighted works in terms of ease of use and wide audience.

[174] For example, Playboy Enterprises has discovered the threat of technology-aided infringement repeatedly. *See e.g.*, Playboy Enterprises, Inc. v. Webbworld, Inc., 968 F. Supp. 1171 (N.D.Tex. 1997); Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996); Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

[175] The No Electronic Theft Act (H.R. 2265) has been signed by President Clinton. The Act amends various sections of Titles 17 and 18 of the U.S. Code 17 U.S.C. §§ 101, 506-07; 18 U.S.C. §§ 2319, 2319A, 2320. The text of the law may be viewed at http://www.thomas.loc.gov/home/c105query.html or ftp://ftp.loc.gov/pub/thomas/c105/h2265.rh.txt . Additionally, the No Electronic Theft Act, Pub. L. 105-147, or the NET Act, provides greater copyright protection by amending the provisions of U.S.C. Titles 17 and 18. The Act also clarifies that reproduction or distribution resulting in infringement may be by electronic means. The NET Act provides for criminal liability for individuals who reproduce or distribute one or more copies of copyrighted works valued at more than $1,000. The Act closes the "LaMacchia Loophole" created by U.S. v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994), where the court found that criminal sanctions did not apply in instances where a defendant did not recognize a commercial advantage or private financial gain. In *LaMacchia*, the defendant encouraged lawful purchasers of computer games to upload the games to a bulletin board service for access by other parties in violation of copyright law. The new language now provides that any person who infringes on a copyright willfully either "for purposes of commercial advantage or private financial gain; or by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies … of 1 or more copyrighted works, which have a total retail value of more than $1,000" shall be punished under 18 U.S.C. 2319.

[176] 17 U.S.C. § 102.

[177] *See* Reiss v. National Quotation Bureau, 276 F. 717 (S.D.N.Y. 1921) (coined code words held protectable) (as cited by Nimmer on Copyright § 2.04).

[178] Questions Frequently Asked In The Copyright Office Public Information Section (visited Feb. 27, 2001) <http://www.loc.gov/copyright/faq.html#q2>.

[179] Even if a site incorporates preexisting material it can still be copyrighted. When preexisting material is incorporated into a new work, the copyright on the new work covers only the original material contributed by the author.

[180] Carolina Saez, *Enforcing Copyrights in the Age of Multimedia*, 21 RUTGERS COMPUTER & TECH. L.J. 351, 355 (1995) (stating that multimedia is an "audiovisual work" but states no case law. While multimedia uses a computer program, the Hypertext Markup Language, it consists of much more. Multimedia is comprised of motion-picture films, slides, photographs, written text, and music. A website is a new form of a literary work, not just the underlying computer program that made the literary work possible); Jenevra Georgini, *Safeguarding Author's Rights in Hypertext*, 60 BROOK.L. REV. 1175, 1179 (1994) (the Copyright Act defines an "audiovisual work" as a" a series of related images which are intrinsically intended to be shown by the use of machines or devices such as projectors, viewers, or electronic equipment, together, with accompany sounds, if any, regardless of the nature of the

audiovisual work, such as a motion picture or a music video clip, is expressed by a sequence of related moving images, with or without sound, regardless of the medium in which the work is embodied. The copyright owner of an audiovisual work has the exclusive right to copy, distribute or display the copyrighted work publicly.[181] The public display of a work is a transmission or other communication of "a performance or display of the work … to the public, by means of any device or process, whether the members of the public [are] capable of receiving the performance or display … in the same place or in separate places and at the same or different times."[182] A site, therefor, is displayed when it is loaded into a browser and the creator has all the same rights as any other copyright holder.

Anyone who violates one of the exclusive rights of a copyright owner is an infringer. A copyright owner can recover actual or, in some cases, statutory damages. In addition, courts have the power to issue injunctions or other orders to prevent or restrain copyright infringement, and can order the impoundment and destruction of infringing copies.

B. WORKS FOR HIRE

The copyright of a work is initially vested in the author.[183] Therefore, the key issue in determining who owns the copyright to a any technology solution that a company develops is to determine who the author is. A person or entity can be an author by actually creating the work, by hiring a party to do the work in a "work for hire" situation, and by being a "joint author." If a work is made for hire, the hiring party is the sole holder of the related copyrights unless there is an agreement to the contrary. According to the Copyright Act, for a work to be a work for hire, it must be "specially ordered or commissioned"[184] and must fall within one of the following statutory categories: (1) contribution to a collective work; (2) a part of a motion picture or other audio visual work; (3) a translation; (4) a supplementary work; (5) a compilation; (6) an instructional text; (7) a test; (8) answer material for a test; or (9) an atlas.[185] In addition, the parties must "expressly agree in a written instrument … that the work shall be considered a work made for hire."[186]

If a website or a piece of software is created by an employee within the scope of his employment it is considered a work for hire.[187] On the other hand, when an independent contractor is hired to create a site, the ownership of the resulting software is clear -- the contractor owns it. Even if the party paying for the development retains the right to exert, or even exerts, control in the creative process, without a written agreement, it is not a work for hire.[188] Generally, to determine whether an outside party is an employee, whose work is automatically a "work for hire," or an independent contractor, whose work is only a "work for hire" if a written agreement so specifies, a court will apply "general common law of agency principles."[189]

material objects, such as films or tapes in which the works are embodied").

[181] 17 U.S.C. § 106. *See also* Effects Assoc., Inc. v. Cohen, 908 F.2d 555, 556 (9th Cir. 1990).

[182] 17 U.S.C. § 101.

[183] 17 U.S.C. § 201(b).

[184] 17 U.S.C. § 101.

[185] Some commentators have suggested that sites could qualify as audiovisual works, collective works or compilations, but this determination is not settled.

[186] David Bender, Computer Law § 4.04[5] (1996) (Mr. Bender states, "the author is aware of no case deciding whether a [computer] program falls under any of these nine classes of works." The second paragraph applies only to nine enumerated categories of works, the most relevant to hypertext software being an audiovisual work. However, due to the uncertain final characterization of a computer program it is perhaps best to have an "assignment clause" in addition to a "work for hire clause," because it has not been fully determined whether a computer program, more specifically hypertext, may be the subject of a work for hire as a specially commissioned work).

[187] *See* Bender, *supra* note 186, at § 4.04[5] (1996).

[188] Community for Creative Non-Violence v. Reid, 490 U.S. 730 (1989).

[189] *Cf. id*. at 731. According to the court, the factors to be considered are as follows:

- The skill required (more likely to be an independent contractor if skill level is high);
- The source of instrumentality and tools (more likely to be an independent contractor if hired party uses his own tools);
- The location of the work (more likely to be an independent contractor if hired party works at a place other than hiring party, especially if it is at the hired party's own facility);
- The duration of the relationship between the parties (more likely to be an independent contractor if the duration is short);
- Whether the hiring party has the right to assign additional projects to the hired party (more likely to be independent-contractor if there is no right to assign additional projects);
- The extent of the hired party's discretion over when and how long to work (more likely to be an independent contractor if the hiring party decides when and how long to work);
- The method of payment (more likely to be an independent contractor if paid in one final lump sum upon completion, more likely to be an employee if paid routinely);
- Whether the work is part of the regular business of the hiring party (more likely to be an independent contractor if the work is not part of the services or products that hiring party sells to others);

Given the highly fact intensive determinations of whether the creator is acting as an employee or as an independent contractor, it is not certain who will own the copyright when the development is outsourced. Based on this uncertainty, when development occurs using outside developers, an initial written agreement should clarify whether the hiring party or the contractor will retain ownership of the resulting software and assigning all related copyrights.[190] The ideal way to accomplish this is to provide that a separate stand-alone copyright assignment will be executed upon completion of the project, and that the developer will assist in executing all of the documents necessary for a federal copyright registration to be filed.[191]

C. DATABASES.

Literary works are defined under the Copyright Act to include all "verbal or numerical symbols or indicia, regardless of the nature of the material objects . . . in which they are embodied."[192] Congress specifically stated that this definition includes "computer databases . . . to the extent that they incorporate authorship in the programmer's expression of original ideas . . ."[193] It is the originality in ideas that is key to protection of data.

Copyright protection for databases does not protect the data itself.[194] Only the arrangement of databases is protectible; the data content within the work is not copyrightable.[195] For example, a court found copyrightable a company's database of information about the value of cars developed by dividing the national market into various regions and then giving independent predicted variables (such as make, model and condition of the vehicle) for each region.[196] The factors used to determine whether a compilation is copyrightable are "selection, coordination and arrangement."[197] Like the defense of fair use, the presence of the required factors is determined on an ad hoc basis. This means that whether any particular CGI bin[198] is original enough (in selection, coordination and arrangement) for copyright protection may not be determinable until the issue is actually litigated in court.[199]

A company needs to institute policies so that its employees respect third party copyrights. Policies should make clear that it is not permissible to download copyrighted information to computers. Policies should also address the proper use of third party data.

VI. CONTRACTING ELECTRONICALLY

A business owner may decide that creating enforceable electronic contracts may be part of its strategy for implementing its privacy, security and intellectual property policies. Indeed, the predominant means for protecting one's rights on the Internet is quickly becoming contract.[200]

Creation of contractual restrictions is relatively simple in the digital environment. Once a party downloads a file, the file itself could begin its installation by posting the associated licensing terms and requiring acceptance of those terms before installation continues. Alternatively, the user could be required to accept the terms before receiving access to files through an on-line

---

- Whether the hiring party is in the business (more likely to be an independent contractor if the hired party sells the particular products or services on a regular basis as part of an ongoing business);
- The provisions of the employee benefits (more likely to be an independent contractor if there are no employee benefits); and
- The tax treatment of the hired party (more likely to be an independent contractor if an IRS 1099 form was used instead of a W-2).

Id. at 752-53. It should be noted that other courts have been more flexible in the work for hire context when applied to ownership of the works. *See, e.g.*, Philadelphia Orchestra Ass'n v. The Walt Disney Co., 821 F. Supp. 341 (E.D. Pa. 1993) (interpreting the 1909 Copyright Act to determine whether a work was made for hire); Aymes v. Bonelli, 980 F.2d 857 (2d Cir. 1992) (court found a software program to be work for hire even though the creator was not an employee in the classic sense, based in large part on the direction and supervision of the hiring party).

190 17 U.S.C. § 204 requires that a transfer of ownership in a contract must be in writing to be valid.

191 Even if the site development agreement provides that the site is a work for hire, the party contracting for the site will not qualify as a work for hire unless it falls under one of the statutory provided categories.

192 17 U.S.C. § 101. *See* Atari Games Corp. v. Oman, 888 F.2d 878, 885 n. 8 (D.C. Cir. 1989); Corsearch, Inc. v. Thomsen & Thomsen, 792 F. Supp. 305, 332 n. 10 (S.D.N.Y. 1992).

193 H.R. Rep. No. 94-1476, 94th Cong., 2 Sess. 54 (1976).

194 Feist Publications, Inc. v. Rural Telephone Service Co., Inc. 499 U.S. 340, 111 S.Ct. 1282, 113 L.Ed.2d 358 (1991).

195 *See, e.g.*, CCC Information Services, Inc. v. MacLean hunter Market Reports, Inc., 44 F.3d 61 (2d Cir. 1994), cert. denied 116 S.Ct. 72 (1995) (stating threshold for originality is low).

196 *Id*. at 67.

197 Feist, *supra* note 194, 499 U.S. at 362-63.

198 Common Gateway Interface, or CGI, is one popular method of allowing database interaction from a Webpage.

199 *See e.g.*, ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (finding CD ROM collection of telephone directory information uncopyrightable).

200 HENRY H PERRIT, JR., LAW AND THE INFORMATION SUPERHIGHWAY: PRIVACY ACCESS, INTELLECTUAL PROPERTY, COMMERCE, LIABILITY 10.22 (1996).

registration process.[201] One method of imposing contractual obligations over the Internet is through clickwrap licensing. Contracts created over the Internet are often referred to as clickwrap, mouse-click, or click-through contracts. Some courts have even gone further by recommending the use of online, clickwrap agreements.[202]

Generally, there are no unique rules for clickwrap contracts. Ordinary contract principles apply.[203] For example, a party's assertion that he failed to read a clickwrap contract is no more fruitful than a party's assertion that he failed to read a paper contract.[204]

A. PRACTIONER NOTE

In preparing a clickwrap contract, certain steps should be taken to increase the likelihood of enforceability. The steps are as follows:

1. Require Affirmative Action.

Most courts enforce electronic contracts provided there is evidence of true mutual assent.[205] Requiring the purchaser to show assent by clicking on a button at the bottom of an electronic contract increases the likelihood of enforceability.[206] There are at least three recommended forms of confirming assent to the clickwrap agreement: (1) require the user to assent by clicking on an "I Accept" button, (2) require the user to type specific words of acceptance, such as "I accept the agreement," and (3) require the user to type a particular code, which is available in the text of the clickwrap agreement. The last alternative forces the individual to more closely review the substantive text of the agreement. To increase enforceability, the registration process should terminate immediately if the user does anything other than signaling assent. For example, if the user clicks the "I Decline" button, the registration process or download should immediately discontinue.

2. Place Acceptance Option at the End of Terms.

The contracting party should be required to scroll through the entire clickwrap agreement before the benefit is provided, such as initial use of the service or download of the software or other digital file. Consequently, the contract must be formed prior to the availability of the item or data sought to be protected. The actual "I Agree" button or prompt for typing assent should be on the final screen of the clickwrap. This will allow for a showing

---

[201] *See e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("A vendor … may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vender proposes to treat as acceptance.")

[202] American Eyewear, Inc. v. Peeper's Sunglasses & Accessories, Inc., 106 F. Supp. 2d 895 (N.D. Tex. May 16, 2000) (suggesting incorporation of a clickwrap agreement into the website purchase order to limit exposure to personal jurisdiction); Stomp v. NeatO, LLC, 61 F. Supp.2d 1074 (C.D. Cal. 1999) (recommending an interactive clickwrap agreement that includes a choice of venue clause which a consumer must agree to before being allowed to purchase any products).

[203] *See* Cadapult Graphic Systems, Inc. v. Tektronix, Inc., 98 F. Supp.2d 5, 60 (D.N.J. 2000) as sited by Barnett v. Network Solutions, No. 11-00-00079 <http://www5.law.com/tx/sub /opinions/fulltext/civil/ s001a/11-00-00079.html> (Tex. App. -- Eastland 2001).

[204] Barnett v. Network Solutions, No. 11-00-00079 <http://www5.law.com/tx/sub/ opinions/fulltext/civil/s001a/11-00-00079.html> (Tex. App. -- Eastland 2001). In enforcing the contract, the court noted that, by the very nature of the electronic format, the party seeking to avoid the contract was required to scroll through the entire contract in order to accept its terms. *Id.*

[205] *See, e.g.*, Compuserve, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q.2d 1020 (N.D. Ca. 1998); Groff v. America Online, Inc., 1998 WL 307001 (R.I. Super. 1998) (all recognizing the validity of electronic contracts). Additionally, most commentators believe that clickwrap agreements are even more enforceable than the standard shrinkwrap agreements used on many software products. License notices on the outside wrappers on software to which users consent when they open the package or use the software, referred to as "shrinkwrap agreements", have been enforced in numerous cases, most notably ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Hill v. Gateway 2000, 105 F.3d 1147 (7th Cir. 1997); Brower v. Gateway 2000, Inc., 246 A.D.2d 246 (N.Y. App. Div. 1998); and M.A. Mortenson Co. v. Timberline Software Corp., 970 P.2d 803 (Wash. Court. App. 1999). The commentators site the disclosure of the license terms prior to distribution and the affirmative indication of user acceptance to terms prior to the use of the service or software distribution as reasons for the increased enforceability, some of the key reasons shrinkwrap agreements were not enforced in earlier court decisions. Note, even shrinkwrap agreements with later assent are more likely to be deemed enforceable if a full refund is available if the license is not acceptable.

[206] Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 U.S. Dist. Lexis 4553 (C.D. Cal. Mar. 27, 2000) (dismissed breach of contract claim where website stated merely that "use" constituted assent to terms, but user was not required to take any affirmative steps, such as clicking an acceptance button, to indicate assent); Groff v. America Online, Inc., No. PC 97-0331, 1998 WL 307001, at *5 (R.I. Super. Ct. May 27, 1998) (clicking "I accept" on website constituted effective electronic signature); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct., App. Div. 1999) (enforcing terms on website that appeared next to boxes marked "I agree" and "I disagree", where use required clicking "I agree", and consumer could obtain the services provided elsewhere); Thomas v. Microsoft Corp., No. 88944, 2000 Lexis 513 (Ill. App. Ct. Dec. 28, 1999) (enforcing contract because the plaintiffs "had meaningful choice in determining with which provider to subscribe and whether to assent to their contractual terms" by clicking the "I agree" button).

that the contracting party has had the opportunity to view all of the agreement's terms before accepting.

3. Require Acceptance During the Installation Process.

Even if a clickwrap agreement is assented to in the download process, the user should be required to repeat the process as part of the installation protocol for the software product or database. This is a relatively easy step to incorporate in the installation process and creates a double assurance of assent.

4. Allow Contracting Party to Exit the Process at Any Time.

The registration process should provide the party with the option to terminate the process at any point before final acceptance of the terms of the agreement. This will reinforce the fact that the parties' assent to the terms of the agreement is voluntary and purposeful.

5. Record and Maintain Date and Time of Acceptance.

For evidentiary purposes, the date, time and fact that the user accepted the contract should be recorded electronically and retained by the website owner. While evidence of the installation or download process is certainly persuasive, the evidence of actual assent by a particular party is even more so. The process should require the party to provide identifying information, which should be linked to the assent provided. These items of information should be retained for at least as long as the contract is operative. This evidentiary information can be maintained in a variety of ways, such as a database or file system on a hard drive or LAN.[207] Legal review of all clickwrap agreements and the procedure for recording and maintaining assent evidence is extremely important.[208]

6. Express Intentions.

Within the contract text, e-contracting parties should plainly state that they expect their contract to be enforced. A clear statement of the parties' intent to waive pen and paper requirements can assist in enforceability.[209] After the contract is formed and the materials are made available, the website and software should expressly notify that the use of the site and software are subject to the terms and conditions in the applicable clickwrap agreement.

7. Utilize a Splash Screen and Help Menu.

Every time a user enters the site or software product, an entrance screen (often referred to as a "splash screen") should display the following statement: "Use of this product/site is subject to the terms and conditions found under this [product's help window or site's legal page]," in addition to the typical copyright and trademark notices.

8. Utilize Good Drafting Tenets.

The same principles that govern paper and pen transactions, govern electronic contracting. A clickwrap agreement should be just as carefully drafted as any other contract. To aid in enforceability, the following provisions should be considered:

a. *Governing Law Selection.*

E-contracting parties should formally select controlling law of a state where the courts have developed precedent enforcing e-contracts.

b. *Authority.*

The agreement should include a representation and warranty that the party entering into the agreement is authorized to bind his or her principal or employer and has adequate legal capacity to enter into the agreement.

c. *Rights Clarifications.*

Clickwrap agreements can provide for extension of rights beyond those granted by common law and statutory copyright regimes. For example, the contract can increase restrictions, such as preventing the user from the exercising an exemption that is recognized by the law.[210] Licensing can also solve the problems created by complicated portions of copyright law like the "first sale doctrine."[211]

> **PRACTICE TIP:** If the website owner is not concerned with others copying the content, the

---

[207] A LAN is the common acronym for "Local Arca Network."

[208] *See* Smith v. Weinstein, 578 F. Supp. 1297, 1307 (S.D.N.Y. 1984) (comparing contractual rights with rights acquired under copyright law).

[209] *See, e.g.* Barnett v. Network Solutions, No. 11-00-00079 <http://www5.law.com/tx/sub/opinions/fulltext/civil/s001a/ 11-00-00079.html> (Tex. App. -- Eastland 2001); Hotmail Corp. v. Van Money Pie, Inc., No. C98-20064, 1998 U.S. Dist. Lexis 10729 (N.D. Cal. Apr. 16, 1998).

[210] For example, through a contract, the author of a software program downloaded from the web could contractually prohibit the user from making a backup copy or the author of an article could prohibit the use of quotes from or reviews of the work.

[211] Arguably, the "first sale" defense for an alleged copyright infringement may be precluded unless the initial consumer deletes the original copy immediately upon transfer to a second party. *See* KENT STUCKEY, INTERNET AND ONLINE LAW 6.08[3] (1996). In absence of a license, copyright owners are placed in a predicament that their work may be subsequently transferred to other parties beyond the initial consumer while that initial consumer retains the initial copy. Through a license, an online transmission can be differentiated from traditional distribution. The license can prohibit the initial consumer from retaining their copy of the original work or from sending other additional copies to third parties.

following disclaimer may be used to allow unlimited copying:

> You have a license to copy the content of this site as long as: (i) the copyright notice and any other form of attribution remains attached; (ii) such copying is for personal use only and is not for commercial profit; and (iii) the author is notified of any use which deviates in any way from the license granted herein.

d. *Liability and Warranty Limitations.*

Clickwrap agreements can be used to disclaim warranties implied by operation of common law and statutory enactments. This allows the site owner to accept the amount of risk related to the services being provided and the compensation being paid.

> **PRACTICE TIP:** Examples of provisions which should be considered include the following:
>
> User expressly agrees that use of the site is at user's sole risk. The site is provided on an "as is" and "as available" basis.
>
> Site Owner expressly disclaims all warranties of any kind, whether express or implied, including, but not limited to the implied warranties of title, merchantability (including, but not limited to merchantability of computer programs), and fitness for a particular purpose.
>
> Warranties of noninterference with information, noninfringement, and accuracy of informational content are expressly excluded. Competing claims may exist and Site Owner grants only such rights as it actually possesses. The site is provided with all faults, and the entire risk as to satisfactory quality, performance, accuracy, and reliability of any information obtained through the site is with the user.
>
> Site Owner makes no warranty that the service will meet user's requirements, or that the site will be uninterrupted, timely, secure, or error free; nor does Site Owner make any warranty as to the results that may be obtained from the use of the site or that any defects in the site will be corrected.
>
> User understands and agrees that any data obtained through the use of the site is obtained at user's own discretion and risk and that user will be solely responsible for any damage or loss that results from the use of such data.

9. Provide for Easy Ongoing Access to Contract.

Even after the registration process or download, the website or related product should clearly provide that it is governed by a contract with a link or easy access to the full text of the agreement. The contract should also be easily printed in its entirety.

10. Choose Technology Wisely.

The use of digital signature technology can also increase the likelihood of enforceability. Disputes over enforceability are rarer when the contract is memorialized in a clear writing and digital signature technology contributes to satisfying the enforceability requirements of most legal regimes. Where it can feasibly and cost-effectively be used, digital signature technology is recommended.

11. Consider New Traditional Contracts for Prior Customers.

In the context of shrinkwrap agreements, some courts have held that the electronic contracts do not trump explicit prior agreements where those agreements contain integration and "no-modification-unless-in writing" clauses.[212] If the new electronic contract is with customers where prior contracts exist, a written agreement may be necessary.

B. RECENT LEGISLATION RELATED TO CLICKWRAP LICENSES

The Federal Electronic Signatures in Global and National Commerce Act ("E-Sign"),[213] enacted on June 30, 2000, recognizes that electronic signatures and records are as legally binding as other contracts.[214] E-Sign is in large measure based on the text of the Uniform Electronic Transactions Act ("UETA"), and, therefore, allows states to preempt the federal E-Sign rules in

---

[212] *See* Morgan Laboratories, Inc. v. Micro Data Base Systems, Inc., 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997) (citing Arizona Retail Sys. v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993).

[213] 15 U.S.C. § 7001 *et seq.*

[214] Upon signing the bill into law, President Clinton stated, "Under this landmark legislation . . . on-line contracts will now have the same legal force as equivalent paper contracts." Statement by President William J. Clinton Upon Signing H.R. 2130, 36 Weekly Comp. Pres. Doc. 1560 (June 30, 2000). The Senate Report accompanying the bill also confirms this sentiment by stating, "This legislation also assures that a company will be able to rely on an electronic contract and that another party will not be able to escape their contractual obligations simply because the contract was entered into over the Internet or any other computer network." S. Rep. No.106-131 at 2 (1999), 1999 WL 555831.

certain instances by enacting UETA.[215] According to section 101(a) of E-Sign, a contract or a signature will not be denied legal effect, validity or enforceability solely because of its electronic form. An electronic signature, for the purposes of E-Sign, includes processes attached to or logically associated with a contract which are executed or adopted by a person with the intent to sign the record.[216] Therefore, a clickwrap agreement is enforceable as long as it fits within the E-Sign parameters and the two parties to the "clicking" intended to create the agreement.[217]

The National Conference of Commissioners on Uniform State Laws ("NCCUSL") has approved UETA as a uniform law. The purpose of UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signature. UETA also makes clear the validity of clickwrap agreements in interactions between people relating to business and commercial affairs, as long as attribution standards are met. These include the user providing identifying information which can be linked to the clicking of acceptance.[218]

The NCCUSL has also approved a uniform law entitled "Uniform Computer Information and Transactions Act ("UCITA"). UCITA is a contract law statute that applies to computer information transactions which take place online, including agreements to distribute computer software, computer data and databases, and other online information. UCITA makes clear that clickwrap agreements which allow a user to convey his or her assent through a "click" are legally binding as long as the contracting party has the opportunity to review the terms before assenting.[219]

---

[215] "Once the States enact uniform standards consistent with those of UETA, the standards prescribed in this legislation will cease to govern." S. Report 106-131, at 2 (1999).

[216] E-Sign § 106(5).

[217] Please note, though not directly applicable in this context, E-Sign mandates that in a consumer transaction, the consumer must be provided with a clear and conspicuous statement informing them of their right to:

(i) be provided with a copy of any electronic record used in the current transaction in electronic or

non-electronic form;

(ii) withdraw the consent to have the record provided or made available in electronic form;

(iii) be informed of the procedure to effectuate the withdrawal of consent;

(iv) be informed of the scope of the consent he has given and;

(v) be furnished with a statement of hardware and software needed to access and retain the electronic records.

For ease of use for the customer a site may want to include this type of language, even if the transaction is between two businesses.

[218] UETA § 9, Comment 5 and § 14, Comments 2 and 3 (available at <http://www.law.upenn.edu/bll/ulc/fin/act99 19905/ueta99.htm>).

[219] UCITA, § 112 <http://www.law.upenn.edu/bll ulc/ulc_frame.htm>, Reporters Notes #5.

APPENDIX I

Computer Software

It is the intent of the Company to comply with copyright laws and software licensing agreements when acquiring, installing, and using software on personal computers owned by the Company. Unless the license specifically allows otherwise, a given software package may be used on only on one computer and the Company must have an original software license on file for each computer where a given software package is installed. Although most software titles may actually be shared on multiple computers, if those computers are attached to a network, it is a violation of the copyright to do so unless:

- The package was specifically designed to run on a network, and the Company is not exceeding the number of users as designated by that package and the software license contained in that package; or
- The Company has a site license for that product.

_____ is responsible for maintaining records of software licensing agreements for the Company.

In order to ensure compliance with copyright laws and software licensing agreements, and to help prevent computer viruses from being transmitted through the system, you are not permitted to install or download any software or content, such as music, videos, or non-work related zipped files, onto the Company's computer system without prior written approval from management, and after consulting with _____.

It is illegal to make or distribute copies of copyrighted material without the written authorization of the copyright owner (the only exception being the right of the user to make a backup copy for archival purposes). The copyright law makes no distinction between duplicating software for sale or for free distribution. Unauthorized duplication of software, often referred to as "piracy," is a federal crime. You are not permitted to make, acquire, or use unauthorized copies of computer software.

You may use software only in accordance with the terms and conditions of the license included with the software. If you are unwilling to comply with the terms and conditions contained in the software license agreement, you must not use or install the software and should notify you supervisor of the situation.

Employees should notify their immediate supervisor, the _____ Department or any member of management upon learning of violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

APPENDIX II

Information Systems Management and Monitoring

The Company collects and maintains personal information related to decisions affecting an individual's employment status or for legal or necessary business purposes. Any information considered to be Company property, including information located in or on computers and e-mail/voice mail systems, employee lockers, desks, and Company vehicles will be subject to inspection by the Company.

Electronic and Voice Mail Use and Monitoring

We recognize your need to be able to communicate efficiently with fellow employees. Therefore, we have installed an internal electronic mail (e-mail) system to facilitate the transmittal of business-related information within the Company. All messages sent, received, composed and/or stored on these systems are, accordingly, the property of the Company.

The e-mail system is for business only. The use of the Company's e-mail system for personal communications or for non job-related solicitations, including, but not limited to, religious or political causes, is strictly prohibited. Employees are also prohibited from the display or transmission of sexually-explicit images, messages, ethnic slurs, racial epithets or any thing which could be construed as harassment or disparaging of others. Employees should refrain from forwarding non-business related e-mails to other Company employees.

Messages on the voice-mail and e-mail systems are to be accessed only by the intended recipient and by others at the direct request of the intended recipient. However, the Company reserves the right to access messages on both systems at any time. Any attempt by unauthorized persons to access messages on either system will constitute a serious violation of Company policy.

All voice-mail and e-mail passwords must be made available to the Company at all times. Please notify _____ if you need to change your password(s).

The Company reserves the right to access an employee's voice-mail (outgoing and incoming) and e-mail messages at any time. Therefore, an employee's outgoing voice-mail message must not indicate to the caller that his/her message will be confidential or private. The existence of a password on either system is not intended to indicate that messages will remain private.

Employees should be aware that even when a message has been erased, on some systems it may still be possible to retrieve it from a backup system. Therefore, employees should not rely on the erasure of messages to assume that a message has remained private.

Violation of this policy may result in disciplinary action up to and including discharge.

For business purposes. Management reserves the right to enter, search, and/or monitor the private Company e-mail system and the files/transmission of any employee without advance notice.

Internet Policy

The following Rules for Use of the Internet (the "Rules) have been adopted to ensure proper use of the Company's Internet resources. It is the responsibility of all employees to adhere to these Rules and to use these resources in a professional, ethical and lawful manner.

Employees are given access to the Internet to assist them in the performance of their jobs. The computer and telecommunications systems belong to the Company and may only be used for authorized business purposes.

The Internet is a worldwide network of computers containing millions of pages of information and many diverse points of view. Because of its global nature, users of the Internet may encounter material that is inappropriate, offensive, and, in

some instances, illegal. The Company cannot control the presence of this information on the Internet. Employees are personally responsible for the material they review on and download from the Internet.

- Accessing the Internet. Employees may only access the Internet through the Company's approved Internet firewall.
- Prohibited Activities. Sending, receiving, displaying, printing, or otherwise disseminating material that is fraudulent, harassing, illegal, sexually oriented and/or explicit, obscene, intimidating, defamatory, or otherwise inconsistent with a professional office workplace is prohibited. Employees encountering such material should report it to the Human Resources Director immediately.
- Prohibited Uses. Employees may not use the Company's Internet resources for personal advertisements, solicitations, promotions, destructive programs (i.e., viruses and/or self-replicating code), political material, or any other unlawful use. Participation and/or postings in discussion groups, chat sessions, bulletin boards, and newsgroups are acceptable for business purposes only.
- Communicating Information. Employees should exercise the same or greater care in drafting e-mail, communicating in business discussion groups, and posting items to bulletin boards and newsgroups as they would for any other written communication. Anything created on the computer or Internet may, and likely will, be reviewed by others. If necessary, employees shall take steps to help protect the security of documents, including the encryption of documents.
- Downloading. Computer programs and software should NEVER be downloaded from the Internet. Employees are warned that the downloading of software can cause network and computer instability, as well as security breaches that could be very damaging to the Company and its clients.
- Virus Detection. All documents downloaded from the Internet or from computers or networks that do not belong to the Company, MUST be scanned for viruses and other destructive programs before being placed onto the Company's computer system.
- Push Technology. Due to the nature of Push Technology (i.e., PointCast, NetCast) and it's effects upon network performance, no form of Push Technology is permitted to be run over the network.
- Live Audio Feeds. Audio feeds such as Real Time Audio degrade network performance and are not permitted.
- Security of E-mail. Messages sent through the Company's Internet mail gateway are not encrypted and are subject to possible interception by parties other than the intended recipient. Therefore, all sensitive communications and documents must be encrypted to ensure privacy and confidentiality. Questions concerning encryption should be directed to _____.
- Export Restrictions. Because of export restrictions, programs or files containing encryption technology are not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from _____.
- Disclaimer of Liability. The Company will not be held responsible for any damages, direct or indirect, arising out of the use of its Internet resources.
- Waiver of Privacy. The Company has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites employees visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by employees, and reviewing e-mail sent and received by employees. Employees waive any right to privacy in anything they create, store, send, or receive on their workplace computer, the Company's network, or Internet resources.
- Compliance with Applicable Laws and Licenses. Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and on-line activity. Employees may not load any unlicensed software into any of the Company's computers or use such unlicensed software in conducting business on behalf of the Company.
- Amendments. These Rules may be amended or revised from time-to-time. Employees may review a copy of the current Internet Usage Policy by contacting _____.
- Enforcement of Policy. The enforcement of this policy is the responsibility of _____ located at _____, telephone number (___) _____.

Appendix III

Policy on Computer Security

Introduction

Continuing availability of information is essential to the operation of _____. Expanded use of computers and telecommunications has resulted in more accurate, reliable, and faster information processing, with information more readily available than ever before. _____ has realized increased productivity, in terms of improved delivery of goods and services and lower operating costs, as a direct result of the growing commitment to use information technology.

Information technology has also brought new concerns, challenges, and responsibilities. Information assets must be protected from natural and human hazards.

Protecting information assets includes:

- Physical protection of information processing facilities and equipment.
- Maintenance of application and data integrity.
- Protection against unauthorized disclosure of information.

Additionally, information entered, processed, stored, generated, or disseminated by automated information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside _____. Specifically, the information must be protected from unauthorized or accidental modification, destruction, or disclosure. Otherwise, we risk compromising the integrity of _____ programs, violating individual rights to privacy, violating copyrights, or facing administrative, civil or criminal penalties.

Security Policy

Policy Purpose

The purpose of the _____ Computer Security Policy is to address security issues related to the safety and integrity of information maintained on _____ computerized information systems. This policy is not intended to address the proprietary interests of intellectual property and/or copyright issues.

Policy Applicability

The Computer Security Policy applies to all _____ employees and others (e.g. vendors, independent contractors, etc.) accessing or attaching to computers operated by _____ .

It is the policy of _____ that:

- Persons using or attaching to _____ computer resources will acknowledge compliance with the Computer Security Policy when userids and passwords are assigned, and in some cases, when an application is accessed.
- Computer resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under state statutes and federal laws, as well as through administrative and/or civil sanctions.
- Computer software is _____ property and shall be protected as such.
- Attempting to circumvent security or administrative access controls for computer resources is a violation of this policy, as is assisting someone else or requesting someone else to circumvent security or administrative

access controls. Persons violating the Computer Security Policy will be subject to appropriate administrative, civil, and/or criminal sanctions.

- Violations of the Computer Security Policy will be reported to _____, whether or not damage, unauthorized review and/or unauthorized use of information contained on the system occurred.
- Willful violations of the Computer Security Policy that may be violations of state and federal laws will be reported to the proper authorities.
- Userids and passwords must control access to all computer resources except for those specific resources identified as having public access. All servers must require passwords of 6 or more characters which include at least one numeric and one alpha character.
- Passwords must be changed periodically by the user. All computer resources will require passwords to be changed at least every 90 days and be unique up to or exceeding eight previous passwords.
- Users are responsible for managing their passwords and for all actions and functions performed by their userids, according to the guidelines specified in ***Appendix B***, Password Management.
- All computer resources must provide a notice before logon stating that the computer system is protected by a computer security system; that unauthorized access is not permitted; and that usage may be monitored. The message text for the notice is contained in ***Appendix A***, Security Access Warning Message.
- Information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions must be protected from loss, contamination, or destruction.
- Confidential information shall be accessible only by personnel who are authorized by the owner on a basis of strict "need to know" in the performance of their duties. Data containing any confidential information shall be readily identifiable and treated as confidential in its entirety.
- An auditable, continuous chain of custody shall record the transfer of confidential information. When confidential information from a department is received by another department in the connection with the transaction of _____ business, the receiving department shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing department.
- When an employee terminates employment, their access to computer resources will be terminated.
- End-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.
- All end-user workstations should have virus protection software installed or other, appropriate security measures.
- All information processing areas used to house computer resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel.
- Individuals who have reason to believe that their personal information or computer intrusion/tampering have occurred with respect to their accounts should contact _____ immediately.
- Guest access to servers is permitted only in the _____ .

How You Can Help

- Understand the importance of information and protect it accordingly.
- Do not leave your terminal unattended while logged on to sensitive information.
- Challenge unescorted visitors.
- Executable code should be scanned for viruses before you execute it, even off of a floppy diskette.
- Report all suspected security incidents to _____.
- Make suggestions for security improvements to the data owner.
- Make security of our information resources a part of your everyday life.

Sanctions for Non-Compliance

Sanctions for non-compliance with the _____ Computer Security Policy will be _____.

Appendix A - Security Access Warning Message

Successful prosecution of unauthorized access to _____ computerized systems requires that users are notified prior to their entry into the systems that the data is owned by _____ and that activities on the system are subject to monitoring. All multi-user computer systems will display the following warning message when a user attempts to access the system and prior to actually logging into a system:

> This system is to be used only by authorized personnel, and all others will be prosecuted. Activities on this system are automatically logged and subject to review. All data on this system is the property of _____ , which reserves the right to intercept, record, read or disclose it at the sole discretion of authorized personnel. Specifically, system administrators may disclose any information on or about this system to law enforcement or other appropriate individuals. Users should not expect privacy from system review for any data, whether business or personal, even if encrypted or password-protected. Use of this system constitutes consent to these terms.
>
> Each system must require an active response from the user to move past this screen at the time of sign-on (i.e. user must press the Enter/Return key to continue).

Appendix B - Password Management

Information stored on _____ computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Effective controls for logical access to computer resources minimizes inadvertent employee error and negligence, and reduces opportunities for computer crime.

Each user of an automated system is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access to automated information.

Password Selection

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password which compromises security and accountability of actions taken by the userids which represents the user's identity.

Today, computer crackers are extremely sophisticated. Instead of typing each password by hand, crackers use personal computers to try to determine passwords. Instead of trying every combination of letters, starting with AAAAAA (or whatever), crackers use hit lists of common passwords such as WIZARD or DEMO. Even a modest home computer with a good password guessing program can try thousands of passwords in less than a day's time. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that anybody might guess to be a password is a bad choice.

What are popular passwords? Your name, your spouse's name, or your parents' names. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad, because there are fewer of them; they are more easily guessed. Especially bad are "magic words" from computer games, such a XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some rules for choosing a good password are:

- Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- Include digits and punctuation characters as well as letters.
- Choose something easily remembered so it doesn't have to be written down.
- Use at least 6 characters. Password security is improved slightly by having long passwords.
- It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.
- Use two short words and combine them with a special character or a number, such as ROBOT4ME or EYE-CON.

Password Handling

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, on a Post-It label attached to your computer terminal, on the pull-out drawer of your desk or any other area accessible to anyone else. If you must write your password down, then keep it in a secure area (e.g. your wallet) that only you have access to and do not indicate the system in which the password is used.

A password you memorize is more secure than the same password written down, simply because there is less opportunity for other people to learn a memorized password. But a password that must be written down in order to be remembered is quite likely a password that is not going to be guessed easily.

Never record a password on-line and never send a password to another person via electronic mail.

Do not share your password, it authenticates your ID and you are responsible for all actions taken with your ID. Likewise, do not use another person's ID and password.

***This information on passwords was adapted from the book Practical UNIX Security by Simson Garfinkel and Gene Spafford.*

Appendix C - Personnel Security and Security Awareness

In any organization, people are the greatest asset in maintaining an effective level of security. At the same time, people represent the greatest threats to information security. No security program can be effective without maintaining employee awareness and motivation.

Employee Requirements

Every employee is responsible for systems security to the degree that the job requires the use of information and associated systems. Fulfillment of security responsibilities is mandatory and violations of security requirements may be cause for disciplinary action, up to and including dismissal, civil penalties, and criminal penalties.

Positions in Sensitive Locations or of Special Trust or Responsibility

Individual positions must be analyzed to determine the potential vulnerabilities associated with work in those positions. _____ has designated specific computer positions as requiring background checks prior to employment, due to the sensitive and/or extensive access personnel in these positions have to our computerized information systems. It may also be appropriate for certain divisions to designate locations as sensitive and to require appropriate procedures and safeguards for all employees whose duties include access to those areas.

Security Awareness and Training

An effective level of awareness and training is essential to a viable information security program. Employees who are not informed of risks or of management's policies and interest in security are not likely to take steps to prevent the occurrence of violations. All new employees at _____ must have computer security awareness training provided by the _____.

_____ shall also provide an ongoing awareness and training program in information security and in the protection of computer resources for all personnel whose duties bring them into contact with critical or sensitive computer resources.

Upon termination of a person who occupies a position of special trust or responsibility, or is working in a sensitive area, management shall immediately revoke all access authorizations to Computer resources.

Appendix IV

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, 2008.

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.

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.)
  - But not Workers Compensation claims – *see* below
- 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

18 Years

- Workers compensation claims (after final disposition)

C. 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

D. 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)

E. 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
- Settlement papers and releases (i.e., after all terms are completed and statute of limitations has run)

F. 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
- 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"

SELECTED FEDERAL STATUTORY AND REGULATORY DOCUMENT RETENTION PERIODS		
Type of Document	**Statute or Rule**	**Time for Retention**
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 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