

The Employment Law Seminars

2006-2007

Privacy in the Electronic Workplace

Lynnwood
[Wednesday, February 28, 2007](#)
Embassy Suites Hotel
20610-44th Avenue West
Lynnwood, WA 98036

Tacoma
[Tuesday, March 6, 2007](#)
Sheraton Hotel
1320 Broadway Plaza
Tacoma, WA 98402

Seattle
[Wednesday, March 7, 2007](#)
The Rainier Club
820 Fourth Avenue
Seattle, WA 98101

Bellevue
[Thursday, March 8, 2007](#)
Bellevue Club
11200 SE 6th Street
Bellevue, WA 98004

www.perkinscoie.com

ANCHORAGE BEIJING BELLEVUE BOISE CHICAGO DENVER LOS ANGELES
MENLO PARK OLYMPIA PHOENIX PORTLAND SAN FRANCISCO SHANGHAI SEATTLE WASHINGTON, D.C.

Perkins Coie LLP and Affiliates

Pacific Northwest Labor and Employment Law Departments

Bellevue, Washington

10885 NE 4th Street, Suite 700
Bellevue, WA 98004-5579
Phone: 425.635.1400

Portland, Oregon

1120 N.W. Couch Street, Tenth Floor
Portland, OR 97209-4128
Phone: 503.727.2000

Seattle, Washington

1201 Third Avenue, Suite 4800
Seattle, WA 98101-3099
Phone: 206.359.8000

Copyright © Perkins Coie LLP 2007. All Rights Reserved

Seattle, Washington

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including photocopying, electronic, mechanical, recording or otherwise, without the prior written permission of Perkins Coie LLP.

This briefing handout is not intended to be and should not be used as a substitute for specific legal advice, since legal opinions may be given only in response to inquiries regarding specific factual situations. Subsequent legal developments after the date of specific briefings may affect some of the legal standards and principles discussed. If legal advice is required, the services of counsel should be sought.

Our Presenters

Kevin J. Hamilton focuses his practice on labor and employment counseling and litigation. With over two decades of experience, Kevin has addressed, through counseling, negotiation, or litigation, a broad range of key issues critical to the evolving workplace. He has particular expertise in complex, multiple plaintiff, and class action litigation. Mr. Hamilton chairs the firm's Retail and Consumer Industry practice group, which focuses on the issues across the spectrum confronting the retail and consumer products industry. Prior to joining the firm, he clerked on the United States Court of Appeals for the District of Columbia Circuit and on the Iran-U.S. Claims Tribunal in The Hague, The Netherlands. Kevin is also a frequent *The Seattle Times* book review contributor. He is a graduate of the Georgetown University Law Center and the University of Washington.

Matthew Staples, is an associate in the Seattle office. He works in an array of industries, including telecommunications, retail, gaming, software, finance, media, and advertising. His practice focuses on e-commerce and Internet law, privacy and data security, marketing and advertising, telecommunications regulatory matters, intellectual property licensing, technology transactions and procurement, and business counseling. Matt obtained his law degree from the University of California at Berkeley (Boalt Hall) in 2004.

TABLE OF CONTENTS

- I. INTRODUCTION 1
- II. REGULATING EMPLOYEE USE OF ELECTRONIC COMMUNICATIONS AND RESOURCES 2
 - A. Monitoring Employee E-mail: Current State of the Law 2
 - B. Other Sources of Law Pertinent to Monitoring Electronic Communications and Use of Electronic Resources 3
 - C. Case Law Regarding Employee Privacy in Electronic Communications and Use of Electronic Resources 3
 - D. Monitoring Electronic Communications and Use of Electronic Resources: Emerging Issues 4
 - 1. Use of Employer’s Systems and Resources to Communicate About Union Matters 4
 - 2. Electronic Communications and the Attorney-Client Privilege 5
 - 3. The Next Generation of Electronic Communication: Blogging 5
 - E. A Special Concern: Child Pornography 6
 - F. Best Practices for Controlling Employee Use of Electronic Communications Tools and Other Electronic Resources 7
- III. WORKPLACE INVESTIGATIONS 8
 - A. Workplace Investigations Performed by Third-Party Investigators Must Comply with FCRA 8
 - B. Electronic Surveillance 8
 - 1. Generally 8
 - 2. New Means of Surveillance: Employer Use of Electronic Data Recorders, GPS Tracking Devices, Radio Frequency Identification Tags, and other Location Surveillance Tools 10
 - 3. Case Law 12
 - a. Selected Cases in Which a Reasonable Expectation of Privacy Was Found 12
 - b. Selected Cases in Which No Reasonable Expectation of Privacy Was Found 12
 - 4. Photographs in the Workplace 14
 - 5. Special Concerns 14
 - a. Audio Surveillance 14
 - b. Surveillance and the National Labor Relations Act (NLRA) 14
 - c. Off-Duty Surveillance 15
 - 5. Pretexting 16
 - a. Generally 16
 - b. Telephone Records and Privacy Protection Act of 2006 17

	c.	Other Sources of Liability	17		
	d.	Anti-Pretexting Policies	17		
	7.	What Employers Should Take Away	18		
IV.		PRIVACY AND SECURITY OF EMPLOYEES' PERSONAL INFORMATION	19		
	A.	Medical Records	19		
		1. HIPAA	19		
			a. Covered Entities	20	
			b. Employers as Hybrid Entities	20	
			c. Employers as Health Plan Sponsors	20	
			d. Employers as Employers	21	
				i. HIPAA Applicability in the FMLA and ADA Contexts.....	21
				ii. HIPAA Applicability in Medical Testing Contexts	22
			e. Penalties.....	22	
		2. Americans with Disabilities Act ("ADA")	23		
			a. ADA Restrictions Prior to Offer of Employment.....	23	
			b. ADA Restrictions Applicable to Present Employment	24	
		3. Family and Medical Leave Act ("FMLA").....	24		
		4. Fair and Accurate Transactions Act ("FACTA").....	25		
	B.	Social Security Numbers.....	25		
		1. Generally.....	25		
		2. Reasonable Security Measures Required to Protect SSNs	26		
		3. Secure Disposal of SSNs	27		
	C.	Security Obligations	27		
		1. General Obligation to Secure Personal Information.....	27		
		2. Security Breach Notification: Lost Laptops, Stolen Storage Media, and Hacking Incidents	28		
			a. Overview of Breach Notification Statutes	28	
			b. Security Breach Mitigation and Response	29	
				i. Pre-Breach Planning.....	29
				ii. Initial Breach Response.....	29
				iii. Notify Law Enforcement	30
				iv. Determine Whether, and to Whom, Notice is Required or Desirable.....	30
				v. Pre-Notice Planning / Preparation.....	31

vi.	Notify Credit Reporting Agencies	31
vii.	Notify Employees.....	31
viii.	Other Notices.....	32
ix.	Responding to Employee Concerns.....	32
x.	Potential Remedies.....	32

Privacy in the Electronic Workplace

By **Kevin J. Hamilton**
Matthew Staples¹

I. INTRODUCTION

There has been no more profound change in the American workplace in the last 50 years than the introduction of electronic information processing and storage systems. Enterprise-wide electronic data systems now routinely allow executives and human resource professionals to accomplish in a moment what, a generation ago, would have been an unimaginably difficult task. But, as any student of history will readily acknowledge, there is no more dangerous time than one of momentous change. Novel and transformative technology offers astounding promise but, as the same time, frightening vulnerabilities often not completely understood by those using or managing that very technology.

E-mail is, by now, ubiquitous in the American workplace and, as a result, perhaps the single most fruitful source of evidence in employment-related litigation. Employers rely on first generation “electronic communication policies” at their own risk, as courts have begun to question whether employees have reasonable expectations of privacy even when using e-mail systems belonging to their employers and notwithstanding policies that purport to give employers the right to monitor and record e-mail communications.

The phenomenon of “blogging,” moreover, is so widespread it is not uncommon to find even senior executives blogging on a daily basis. But without careful scrutiny of such “real time” Internet publications, and application of appropriate policies restricting disclosure of confidential information, blogging can result in embarrassing and costly disclosure of closely held information.

Technology, too, holds the promise of revolutionizing workplace investigations. Electronic surveillance allows employers to track the physical movement of employees or company vehicles, to monitor telephone or e-mail traffic, and even to search thousands of hours of surveillance videotape by image with a mouseclick. The very ruthless efficiency of such electronic systems highlights the menace such technology poses to employee privacy or, indeed, to the freedom or autonomy typically thought necessary for effective performance.

And perhaps most frighteningly, electronic data storage systems allow vast amounts of confidential information to be stored and transported on laptops, portable hard drives, flash drives, memory sticks, or DVDs. It is by now disturbingly common to read of yet another lost laptop containing enormous amounts of highly confidential personnel information – date of birth, social security numbers, address and more. A virtual maze of statutes and regulations confront any well meaning employer attempting after-the-fact to respond to the loss of such data collections.

¹ The valuable contributions to this paper by Maralee Downey and Vickie Wallen are gratefully acknowledged.

In this paper, we'll survey the state of the law with respect to privacy and electronic data systems in the workplace with an eye toward practical solutions, issues to consider, and solutions to implement. But in times of rapid change, nothing stands still for long.

II. Regulating Employee Use of Electronic Communications and Resources

For employers, the explosion of electronic information and the efficiency of electronic communication are double-edged swords. On the one hand, advances in technology have eliminated many temporal and geographic barriers, allowing entities of any size to share information and to efficiently conduct business on a national or even global scale. Employers can coordinate with employees, colleagues, and customers anywhere in the world with the click of a mouse. On the other hand, the very efficacy of these technologies leads to novel legal risks. Modern electronic communication (such as e-mail) is more convenient than a phone call and more enduring than a written document. Information that is used to fill a filing cabinet can now be attached to an email message and maintained in physical media the size of a pencil eraser. A failure to properly manage electronic communications and resources can have devastating consequences, exposing the employer to a variety of costly disasters including workplace lawsuits, legal fees, stolen trade secrets, confidentiality breaches, regulator enforcement actions and fines, sexual harassment claims, "hacking" incidents, viruses and other malevolent software, plummeting stock prices, public embarrassment, lost customers, data, and productivity.

E-mail is particularly dangerous. Because of its convenient and casual nature, employees may forget (or be completely unaware in the first place) that email creates a *permanent* record of communications that are discoverable in litigation. A recent survey of U.S. companies conducted by the American Management Association (http://www.amanet.org/press/amanews/2006/blogs_2006.htm) revealed that 24% of organizations surveyed had received subpoenas for employee e-mails, and 15% had been involved in litigation triggered by employee e-mail. While a well-drafted electronic communications policy is vital, mere circulation of the policy is not enough. If an employer truly wants to protect itself against impending e-disasters, it must regularly *train* employees on proper use of electronic communications and resources. Employers must (1) emphasize the permanent nature and legal consequences of e-mails, IMs, and blog postings, (2) tutor employees on what information is appropriate for electronic communication, (3) place appropriate limits and restrictions on the use of laptops and other sources of electronic data; and (4) inform employees that all such communications and use of electronic resources are subject to monitoring and review - without notice - at any time, for any reason.

A. Monitoring Employee E-mail: Current State of the Law

A number of employees have asserted claims against employers for Electronic Communications Privacy Act (ECPA) or Wiretap Act privacy violations stemming from employer monitoring and review of employee e-mail. The Wiretap Act prohibits the interception of electronic communications such as e-mail. 18 U.S.C. §§ 2510 *et seq.* At what point interception occurs, however, can be a topic of some confusion. Courts generally agree that an interception requires the acquisition of the e-mail to be contemporaneous with transmission. When a transmission ends and storage of an e-mail begins has been the subject of a recent decision that suggests a service provider could be liable for interception if it reviews e-mail at the time of receipt in its network, but before delivery to the intended recipient. See U.S. v. Councilman, 418 F.3d 67, 79-80 (1st Cir. 2005). Employers can avoid this uncertainty by obtaining employee consent to such interceptions through the distribution and acknowledgment of a comprehensive electronic communications policy.

Courts have repeatedly dismissed claims that the ECPA applies to businesses. The ECPA only applies to electronic communications services provided “to the public” like a common carrier. 18 U.S.C. § 2701; Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998). Further, the ECPA permits the service provider to access electronic communications such as e-mail for any reason, 18 U.S.C. § 2701(c), but limits disclosure of those communications to certain enumerated exceptions such as consent, legal process, and to protect rights and property.

Thus, the ECPA also employers who provide in-house company computer systems to disclose the contents of employees’ electronic communications “as may be necessarily incident to the rendition of the service *or to the protection of the rights or property of the provider of that service.*” 18 U.S.C. § 2702(b) (emphasis added). In other words, the ECPA will not prevent an employer from monitoring employee e-mail stored on its own system in order to protect the employer’s rights or property. Therefore, the ECPA’s prohibition on intercepting electronic communications is a non-issue in the context of an employer accessing stored employee e-mails on its own private system in accordance with a comprehensive electronic communications policy which has been distributed to and acknowledged by each of its employees.

B. Other Sources of Law Pertinent to Monitoring Electronic Communications and Use of Electronic Resources

There are other sources of employee privacy rights of which employers should be aware in the context of monitoring electronic communications and use of electronic resources. They include:

- **The Fourth Amendment** (for public employers);
- **State Constitutions** (for public employers);
- **State Statutes**; and
- **Common Law Privacy Torts** (namely “intrusion upon seclusion”).

C. Case Law Regarding Employee Privacy in Electronic Communications and Use of Electronic Resources

As a general rule, courts have concluded that a well-drafted electronic communications policy (reserving the right to monitor computer usage on the employer’s system) will defeat an objectively reasonable expectation of privacy. For example:

- A federal district court held that an employee had no reasonable expectation of privacy in e-mails saved on his employer’s network (a network created by the employer, which the employer could access) where the employee was put on notice via “explicit policies” in the employee handbook that office computers were not for personal use and activity would be monitored “as deemed appropriate.” Thygeson v. U.S. Bancorp, (unpublished) 2004 WL 2066746 (D. Or.).
- A California court held that an employee had no reasonable expectation of privacy in the contents of his employer-provided home computer where the employer gave the employee advance notice of its policy that his computer was company property, for company use, and was subject to company monitoring and review “as necessary,” and

the employee signed an acknowledgement of the policy. TBG Insurance Services Corp. v. Superior Court, 96 Cal. App. 4th 443 (2002).

It is critical, however, for employers to understand that sub-par policies or lax enforcement could lead courts to find a reasonable expectation of privacy where they otherwise would not.

The Court of Appeals for the Armed Forces recently concluded that an employee had a reasonable expectation of privacy in e-mails sent from her office computer on her employer's (the government's) server. The court was persuaded by the fact that the employee had a password known only to her and that the employer's log-in banner warned only that the employer could access and monitor the system for "lawful purposes" and ensure authorized use (not to examine the contents of specific e-mails in a manner unrelated to system maintenance). United States v. Long, 64 M.J. 57, 62-65 (CAAF 2006). The court's reasoning in Long follows the Second Circuit's reasoning in Leventhal v. Knapek, holding an employee had a reasonable expectation of privacy in the contents of his office computer where the computer was kept in the employee's private office for his sole use, the employer did not have a general practice of routinely conducting searches of office computers, maintenance of computers was normally announced, and employee had not been placed on notice that he should have no reasonable expectation of privacy. 266 F.3d 64 (2d Cir. 2001).

Note, however, that in the context of public employers subject to the 4th Amendment, courts have held that even if an employee does have a reasonable expectation of privacy in his or her computer, the employer's warrantless search of that computer will be permissible as long as it was reasonable (considering the purpose, means, and scope) in light of the employer's need to conduct a workplace search related to an investigation of employee misconduct).

On January 30, 2007, a mere four months after Long, the Ninth Circuit (the federal appellate circuit encompassing Washington state) withdrew its previous opinion in United States v. Ziegler, (issued in March 2006, in which it had held that an employee had no reasonable expectation of privacy in his workplace computer where the employer's policy informed employees about routine monitoring and access by the employer and included a prohibition against private use) and issued a superseding opinion *expressly dodging* the issue of employee privacy in workplace computers and deciding the case on other grounds. Ziegler, 2007 WL 222167, *5 fn. 9.

While the full impact of the decisions noted above remains to be seen, one thing is clear: This area of the law is far from settled.

D. Monitoring Electronic Communications and Use of Electronic Resources: Emerging Issues

1. Use of Employer's Systems and Resources to Communicate About Union Matters

Section 7 of the National Labor Relations Act ("NLRA") guarantees employees the right to "self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." Section 8 of the NLRA, prohibits employers from interfering with employees' Section 7 rights.

This leaves several questions unanswered, such as whether Section 7 guarantees employees a right to use their employers' computer systems to communicate about union or other concerted, protected matters; or, for that matter, how one might reconcile an employee's Section 7 rights with an employer's policy prohibiting use of its e-mail system "to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations[.]" The National Labor Relations Board is scheduled to hear oral arguments regarding these issues on March 27, 2007, in the matter of Guard Publishing Company. The Board's decision could have a significant impact on electronic communication policies and practices around the country.

2. Electronic Communications and the Attorney-Client Privilege

The attorney-client privilege protects all communications between attorney and client made in the course of obtaining legal counsel. The privilege is not absolute, however, and may be waived by the client's voluntary disclosure of the communications to a third party. Does an employee waive attorney-client privilege by communicating with his or her attorney over the employer's computer system where the employer has reserved a right to monitor and review communications sent over that system? Unfortunately for employers, the most recent answer is *not necessarily*. In Curto v. Medical World Communications, the court held that, despite the employer's policy *clearly* stating that by using the company system the employee waived any right to privacy in such communications, the employee did not waive the attorney-client privilege as to e-mails sent to and received from her attorney on her company laptop used in her home office. The court noted that before returning the laptop to the employer, the employee deleted all personal files including the communications at issue, thereby taking reasonable measures to prevent disclosure. Further, the court agreed with the trial judge, that *the employer's "lack of enforcement" of its computer policy lulled the employee into a false sense of security – believing the policy would not be enforced – and failed to provide the employee with adequate notice that the employer would in fact monitor computer usage*. This factor weighed against finding a voluntary waiver of the attorney-client privilege. The court also compared the soft language of the policy at issue (warning employees that it "may" monitor computer usage) with the firm language in cases where courts found notice sufficient to vitiate a reasonable expectation of privacy ("shall"). See Curto, 2006 WL 1318387 *4-8 (E.D.N.Y.).

The implications for employers are frightening. Without proper policies and consistent enforcement, an employee could use his or her employer's own system to communicate with his or her attorney regarding advice and strategies for suing the employer.

3. The Next Generation of Electronic Communication: Blogging

Online Web journals or logs, commonly known as "blogs," continue to grow in number and significance. Technorati, a blog search engine, claims to track 68.9 million blogs at present (see <http://technorati.com/about/>). According to Technorati, bloggers post approximately 1.6 million posts per day and an estimated 175,000 new blogs are created on a daily basis.

This vast volume of blogs and posts contains many contributions by employees. This is a source of increasing concern to employers world wide (for an interesting discussion see "When Private Sector Employer Fires Worker for Blogging," New

York Law Journal, Vol. 237 (Feb. 5, 2007)). Employee blogs make companies vulnerable to a variety of problems, including lost productivity, leaked information (trade secrets, proprietary information), and lawsuits (harassment/defamation claims based on employee comments, or retaliation/First Amendment/NLRA claims based on attempted regulation by employer). For example, see "CEO blogs spark rumors by telling way too much," by Eric Engleman.

Blogs, like e-mail, must be addressed as part of a comprehensive electronic communications policy. Employees should be given notice and made to acknowledge the fact that blogging on the employer's system *will* be monitored and therefore the employee has no reasonable expectation of privacy in such communications. Blogging off-duty (i.e. not on the employer's time or system) can expose the employer to many of the same problems outlined above. Generally, in employment-at-will states like Washington, employers have broad discretion to terminate employees for engaging in inappropriate activity, including posting inappropriate information on the Internet. Even in employment-at-will jurisdictions, however, legal restrictions may apply in some circumstances to adverse employment action stemming from the content of employee blogs. Before taking action, employers should consider:

- **The First Amendment** (and equivalent state statutes/consitutional provisions): Public employers cannot abridge an employee's right to freedom of speech or association;
- **Anti-Retaliation Provisions:** Title VII, Whistleblower Statutes, Sarbanes Oxley, NLRA; and
- **Title II of the ECPA:** The Stored Communications Act comes into play when an employer seeks unauthorized access to an employee's independently maintained secured website or blog.

E. A Special Concern: Child Pornography

One type of content that might be found on an employee's email messages, computer, or list of visited Web sites is child pornography. Generally, child pornography includes any image of a child engaging in "sexually explicit conduct," including "lascivious exhibition." (If a company has any question as to whether an image or material is child pornography, it should contact legal counsel.) Although a company has no duty to affirmatively monitor its employees' use of email or other electronic resources for the purpose of discovering child pornography, it may be discovered during the various forms of monitoring discussed above.

If a company discovers child pornography on its systems or resources, it must take great care to handle the matter appropriately. On the one hand, the knowing possession of child pornography violates federal law, and a company might be held in violation of the law for "possessing" the images or material in the context of an improper investigation. At the same time, however, a recent case in New Jersey, Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. 2005), makes clear that companies have a duty to investigate and to take reasonable care to report and/or to take effective action to stop an employee from action to stop an employee from accessing illegal child pornography or taking other actions that pose the threat of harm to others. Basically, then, a company must report child pornography but must be extremely careful in doing so.

Unlike electronic communications providers, and those who provide remote computing services to the public, employers that provide Internet access to their employees are not subject to requirements of mandatory reporting of child pornography to the National Center for Missing and Exploited Children. Because they must still take appropriate action to report the child pornography, however, they must involve legal counsel to ensure they do meet their duty of care but do not inadvertently violate the law by knowing possession, copying, or transmission of illegal content.

F. Best Practices for Controlling Employee Use of Electronic Communications Tools and Other Electronic Resources

Companies depend increasingly upon electronic communications and resources in the workplace. Advances in technology continually create new avenues of potential employer liability. Given the unsettled state of the law, employers are advised to play it safe:

- **Notice:** Create a comprehensive policy addressing electronic communications and use of electronic resources by employees. The policy should address *all* forms of electronic communication and use of electronic resources (e.g., computers, the company network, wireless telephones, electronic storage and retrieval systems, and other resources). The policy should *expressly disclaim* any reasonable expectation of privacy in employees' use of any of these means of communication and other resources, and state in no uncertain terms that *all* communications on the company system, and all use of company-supplied computing equipment and other electronic resources, *shall* be monitored at any time for any reason.
- **Consent:** Require each employee to read and sign an acknowledgement of the policy. This acknowledgment should specify that the employee has no reasonable expectation of privacy in any communication on the communication system or in any other use of the company's computer systems or other electronic resources.
- **Implementation:** Schedule regular training sessions where company representatives and/or outside consultants explain the company's policies regarding electronic communications tools, computing systems and other electronic resources. The training sessions should provide examples of appropriate and inappropriate communications, along with the consequences of such behavior (i.e., address the issues of discrimination, defamation, harassment, trade secrets, privacy torts, and so forth). Reinforce that all communications on the company system, and all use of company electronic resources will be monitored at any time and that the employee has no reasonable expectation of privacy. Consistently enforce the policy in a non-discriminatory manner (monitor random electronic communications and use of electronic resources, including e-mail/internet usage, from time to time; if you intend to monitor employees' location using GPS (as discussed in Part III below), then do so on a nondiscriminatory basis; periodically scan employees' network drives for content that would be prohibited, and otherwise give employees notice that the employer is serious about the policy).

III. WORKPLACE INVESTIGATIONS

A. Workplace Investigations Performed by Third-Party Investigators Must Comply with FCRA

In order to maintain a productive and secure place of business (and to avoid future litigation stemming from negligent hiring decisions), many employers investigate a prospective employee's background before extending an unconditional offer of employment. Background checks performed by third-party investigators (also known as consumer reporting agencies, or "CRAs"), are subject to the requirements of the Fair Credit Reporting Act ("FCRA"). The FCRA is designed to ensure the accuracy, fairness, and privacy of information stored and disseminated by CRAs. An employer's obligations under the FCRA will depend on whether the information sought is a "consumer report" (a report "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living . . .") or an "investigative consumer report" (a consumer report "obtained through personal interviews"). Employer FCRA obligations are summarized in the "FCRA Compliance Obligations" chart provided at the end of these materials.

Additionally, when it comes time for an employer to dispose of personnel files containing consumer information obtained through the hiring or investigative process, simply throwing them out in the trash or recycling bin will not suffice. The Code of Federal Regulations states requires "[a]ny person who maintains or otherwise possesses consumer information for a business purpose" to "properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information[.]" Employers therefore must implement policies to ensure *proper* destruction of consumer information. Examples from the CFR include:

- Burning, pulverizing, or shredding of papers
- Destruction or erasure of electronic media

"Erasure" of electronic media requires that the information not be capable of being recreated. Several commercially available software programs and other tools can erase electronic media effectively through random overwriting of data, degaussing (altering the magnetic structure of data on physical media), and other methods.

Finally, employers must note that FCRA compliance can be complicated. An interesting collection of FTC staff opinion letters from the years 1997-2001 (the FTC staff no longer issues opinions on this topic) can provide insight into how the FCRA works in specific situations. These opinions are available on the FTC website at <http://www.ftc.gov/os/statutes/fcra/index.htm>.

B. Electronic Surveillance

1. Generally

Employers have several legitimate reasons to use electronic surveillance in, and in connection with, the employment context. To provide a few examples, an employer might use electronic surveillance to:

- Evaluate employee performance and monitor productivity (e.g., time logged on to a computer for office workers, and the driving safety and delivery times of fleet vehicle operators);

- Investigate whether employees are stealing, harassing others or otherwise violating company policies;
- Monitor employee activity outside the workplace to determine whether employees seeking worker's compensation or disability benefits are being honest;
- Determine whether employees are sharing confidential company information; and
- Prepare for or defend against impending litigation.

As lawsuits arising out of employee conduct continue to multiply, employers increasingly rely on electronic surveillance as a cost-effective way to reduce expenses. Surveillance does, however, present significant legal risk. Its misuse could violate a number of authorities including the Fourth Amendment, federal statutes, state constitutions, state statutes, and an employee's common law right to privacy.

Public employees' right to privacy is protected by the Fourth Amendment. To assert such protection, however, an employee must have: (a) a subjective expectation of privacy (they must personally believe their actions are private) and (b) an objective expectation of privacy (an expectation that society is prepared to recognize as reasonable). Generally, if an employee has both a subjective and objective expectation of privacy, a public employer will be required to procure a warrant before engaging in a search (including video or photo surveillance). It is, however, well-established that searches by public employers for non-investigatory, work-related purposes and for investigations of work-related misconduct, are permissible as long as there was a reasonable justification for the search at its inception, and the scope of the search was reasonable in light of that justification. O'Conner v. Ortega, 480 U.S. 709, 725-26 (1987). Therefore, even if the public employee has a reasonable expectation of privacy, the employer's surveillance will be constitutional as long as it was reasonable.

For private employees it is the common law tort of invasion of privacy (specifically intrusion upon seclusion, adopted by Washington courts in Reid v. Pierce County, 136 Wn.2d 195, 204-05 (1998)) that remains the core protection against unreasonable electronic surveillance in the workplace. To establish a cause of action for intrusion upon seclusion, an employee must prove that the employer (1) intentionally intruded into the employee's private affairs (i.e. a place where the employee had a "reasonable expectation of privacy" and (2) that such an intrusion would be highly offensive to a reasonable person. Intent and intrusion are rarely at issue, as the employer virtually always intends to conduct the surveillance which is in fact conducted. The court's analysis in surveillance cases usually turns on whether or not the employee had a reasonable expectation of privacy and, if so, whether the surveillance would be highly offensive to a reasonable person.

For both public and private employees the key inquiry is: Did the employee have a reasonable expectation of privacy?

2. **New Means of Surveillance: Employer Use of Electronic Data Recorders, GPS Tracking Devices, Radio Frequency Identification Tags, and other Location Surveillance Tools**

Emerging technologies provide new means for surveilling employees and deserve special mention here. Several commercially-available products allow employers to perform the following types of activities:

- **Monitor the location of fleet vehicles (e.g., delivery trucks) and other “company cars.”** These monitoring solutions can take place in real time, showing a vehicle’s location on a map, or can be downloaded and viewed at a later time by the employer.
- **Monitor the locations of employer-supplied cell phones and other wireless devices (e.g., Blackberry).** Like vehicle tracking devices, these devices can monitor employees in real time and can provide reporting after the fact. Indeed, *all* mobile devices that can function as cellular telephones (including Blackberries and other devices with voice capability) are now *required* to contain global positioning system (GPS) functionality. The Federal Communications Commission (“FCC”) required all wireless devices to be capable of being located within a few hundred meters by December 31, 2005, so as to allow wireless users to be able to be located in emergency situations (e.g., 911 calls). The cost to wireless carriers to provide this capability has been significant, so they have sought to recoup some of the costs by developing commercial products to take advantage of certain handsets’ location capabilities. Some of these commercial offerings integrate location information derived from cell tower triangulation with data obtained from GPS in order to provide a more accurate, consistent or continuous set of data to the monitor. Location derived from voice service in this manner is “customer proprietary network information” under the Telecommunications Act of 1934 (as amended) and may not be disclosed to third parties without the express prior authorization of the customer. In the employment relationship, however, an employer who purchases wireless service for his employees is the “customer.” The employee using the phone is merely a “user” of the wireless service. The employer may, therefore, obtain data from carriers, including triangulated data derived from voice service, as part of location-based services (although, as we discuss later in these materials, employers should obtain the signed acknowledgment of employees to policies that state that the employer can, and will, monitor location information).
- **Monitor the location of employees with RFID tags. Radio frequency identification (“RFID”), a technology used originally in business to track inventory, supplies and deliveries, can also be used to track employees.** RFID tags are tiny and can be inserted into virtually anything, from ID cards to badges. RFID “readers” may be set up in various locations in the workplace (and elsewhere). These readers detect whether the RFID tag is within range, and the resulting data can be mined and used for various purposes. In fact, in a scenario still more Orwellian, some employers working with highly sensitive information have even required their employees to have RFID chips implanted under their skin. Again, data monitoring with RFID can take place in real time.

- **Use event data recorders (“EDRs”) to recover data from vehicles.** Pursuant to a directive issued to car manufacturers by the National Transportation Safety Board, nearly all vehicles sold today include EDRs, sometimes called “black boxes.” EDRs are intended to record information during a short time period prior to an accident (or other incident in which air bags are deployed). Generally, the owner of a vehicle is the owner of the data contained in any factory-installed EDR in the vehicle. Most factory-installed EDRs encrypt data that is recorded to an EDR, requiring that it be decrypted with the EDR’s encryption algorithm. Many aftermarket EDRs are available, however, and may be used without encryption (or by an employer who possesses the encryption key). These aftermarket EDRs may hold substantially more data. CarChip, for example, is a commercially available EDR that can record up to 300 hours of driving. The information can then be downloaded to a computer and can produce detailed reports about the vehicle’s operation.
- **Use of advanced photography integration techniques.** Many employers have forgone traditional photo surveillance in favor of more advanced video surveillance. The wonders of modern technology are, however, bringing photo surveillance back with a vengeance. Surveillance companies are combining inexpensive web-connected cameras with state-of-the-art video analysis software to give employers the ability to search hours of surveillance footage and pinpoint every place an individual employee has been in the time it takes to click a mouse. With this technology, web-connected cameras take photos of employees at different locations, on different days, from different angles. Then, facial recognition algorithms build a profile of the employee, enabling an employer to search all of its video surveillance and – within seconds – identify that specific employee’s location at any time from any angle. See Noah Shachtman, “The New Security: Cameras That Never Forget Your Face,” *New York Times* (Jan. 25, 2006), available at: <http://www.nytimes.com/2006/01/25/techspecial2/25video.html?ex=1171774800&en=fcb87edf534c6147&ei=5070>.

Most employers and employees are not aware of the functionality provided by these novel technologies. Befitting their novelty and relatively low profile, the use of these technologies by employers has not been the subject of significant legislation or court cases to date. Those laws that do exist, such as those applicable to RFID, are not generally of concern in the employment context.

Importantly, unlike email and Internet monitoring, the ECPA does not apply to GPS tracking devices, owing to the lack of a “communication” and the statute’s explicit exception of “any communication from a tracking device.” 18 U.S.C. § 2510(12)(c). A “tracking device” is defined in ECPA as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” *Id.*, § 3117(b).

In the absence of applicable laws or regulations governing the use of specific technologies, they may consider rewording analogized to conventional video or photo surveillance. That is, the general privacy torts ought to be the primary source of concern to employers, and the legal standards and advice discussed above apply to the use of these technologies to monitor employees. Appropriate employer policies, coupled with training and consistent enforcement, may be relevant to whether an employee has a reasonable expectation of privacy with respect to location surveillance and monitoring made possible with these technologies.

3. Case Law

Under the legal standards above, video or photo surveillance in and of itself does not violate an employee's reasonable expectation of privacy. Whether or not such surveillance constitutes an unwarranted invasion of privacy is a fact-sensitive analysis to be determined on a case-by-case basis. Unfortunately Washington does not have any case law directly addressing the legality of video, photo or location surveillance in the employment context. However, courts from other jurisdictions have considered electronic surveillance and an employee's right to privacy in a variety of contexts. Pulling from the leading surveillance cases around the country, below is a summary of how courts have weighed in on the issue of electronic surveillance in employment.

a. Selected Cases in Which a Reasonable Expectation of Privacy Was Found

- **Locker Rooms:** Employees had a reasonable expectation of privacy in a locker room (where they regularly showered, changed, and used the toilets), a facility specifically designed to protect their privacy. Thus, secret video surveillance violated the Fourth Amendment. Public employer exception from the warrant requirement did not apply because the employer was seeking evidence of criminal (not work-related) misconduct. Trujillo v. City of Ontario, 428 F.Supp.2d 1094, 1101-09 (C.D. Cal. 2006).
- **Restroom Stalls:** Users of a women's restroom had a reasonable expectation of privacy in bathroom stalls. The employer's continual video surveillance of the women's restroom would constitute an invasion of privacy, "irrespective about rumors of drug use and sales." Johnson v. Allen, 613 S.E.2d 657, 660-61 (Ct. App. Ga. 2005).
- **Nurse's Office:** Video surveillance of a nurse manager's office intruded upon the privacy of employee patients videotaped receiving medical treatment. Acuff v. IBP, Inc., 77 F.Supp.2d 914, 924-35 (C.D. Ill. 1999).
- **Restroom:** Even where the employee gave signed consent to be searched at any time, this consent did not authorize the employer to conduct surveillance from the bathroom ceiling. Speer v. Ohio Dep't of Rehabilitation & Correction, 624 N.E.2d 251, 253 (Ohio Ct. App. 1993).

b. Selected Cases in Which No Reasonable Expectation of Privacy Was Found

- **Shared Office Space:** An employee's reasonable expectation of privacy is not as strong in the workplace as it is at home. Employees do not have a reasonable expectation of privacy in open and undifferentiated work areas. Therefore, it was permissible for the employer to use a hidden camera to videotape employee actions in an open, shared office space. Acosta v. Scott Labor, Inc., 377 F.Supp.2d 647, 650-52 (N.D. Ill. 2005).

- **Public Places:** Employee did not have a reasonable expectation of privacy in public places while on vacation. Thus, it was permissible for an employer to order video surveillance of the employee while he was on vacation as the video captured the employee's activities at or near beach in full view of many strangers. Kowalski v. Scott, 126 Fed. Appx. 558, 559-60 (3d Cir. 2005) (unpublished).
- **Employee's Office:** Noting that the reasonable expectation of privacy is less than it would be in an employee's home, a federal district court held that employees did not have objectively reasonable expectation of privacy in their individual offices, company maintenance shop, lift station, weld shop, or other open work areas. Williams v. City of Tulsa, 393 F.Supp.2d 1124, 1129-31 (N.D. Okla. 2005).
- **Car in Public View:** Employee did not have a reasonable expectation of privacy when entering and leaving his residence, nor while he was in his car parked in public view. Therefore, it was permissible for the employer's investigator to videotape the employee using cocaine in these places (even using high tech, night-vision enabled devices). Salazar v. Golden State Warriors, 2000 WL 246586 (N.D. Cal.).
- **Employee's Office:** As to employees' Fourth Amendment claims, they had no objectively reasonable expectation of privacy in city jail office (even where they believed they could exclude others by shutting the door for privacy) because the office was accessible to a number of other people, including inmates, and was a place where the employer had legitimate security concerns. As to employees' invasion of privacy claims, there is no reasonable expectation of privacy in a non-private office and the alleged invasion was not highly offensive because it did not record audio. The employer's justification for video surveillance outweighed the employees' expectation of privacy. Sacramento County Deputy Sheriffs' Association v. County of Sacramento, 51 Cal. App. 4th 1468, 1476-85, 1487 (1997).
- **Open Work Area:** Employees lacked an objectively reasonable expectation of privacy in disclosed soundless video surveillance of an open and undifferentiated work area. Employees' work station was not provided for their exclusive use, nor did they have private offices or cubicles – just a “vast, undivided space.” Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174, 178-81 (1st Cir. 1997).
- **Area Accessible to Others:** Due to its open, public nature, employee security officers had no reasonable expectation of privacy in the security personnel locker area (locker area was part of a storage room that also held the employer's heating and air-conditioning equipment, and other employees in addition to security personnel had complete access to the locker area). Even if the employees had a reasonable expectation of privacy, the employer's hidden video surveillance of the area was reasonable (the employer was investigating reports of employee misconduct in that area, and the surveillance continued only for the limited time necessary to dismiss or confirm the allegations), and thus

did not violate the Fourth Amendment. Thompson v. Johnson County Community College, 930 F.Supp. 501, 506-08 (D. Kan. 1996).

- **Open Work Area:** An employee who was videotaped picking a lock on a desk did not have a REP in an open office area. Marrs v. Marriott Corp., 830 F. Supp. 274, 283 (D. Md. 1992).

4. Photographs in the Workplace

Photo surveillance, like video surveillance, is a cost effective way for employers to minimize expenses in an effort to maintain a safe and productive business. Courts have sanctioned employers' use of photo surveillance in a variety of contexts, including:

- **Increase Efficiency/Safety:** Photographs of employees, while performing their jobs, taken as part of a workplace production study designed to increase overall efficiency and safety (Thomas v. General Electric Co., 207 F.Supp. 792, 799 (W.D. Ky. 1962));
- **Investigation:** Photographs of specified employees, during normal working hours, taken as part of an investigation of alleged workplace misconduct (DeLury v. Kretchmer, 322 N.Y.S.2d 517, 519 (1971)); and
- **Worker's Compensation Investigation:** Photographs of an employee who brought a worker's compensation claim, where the pictures were taken in unobtrusive manner and involved activities which could have been observed by neighbors or people passing by. The photo surveillance was permissible even where the employer's investigator committed a slight trespass to the employee's property (McLain v. Boise Cascade Corp., 533 P.2d 343, 555-57 (1975)).

5. Special Concerns

a. Audio Surveillance

Critically, the employer-friendly rules discussed above only apply to *sound-free* video and photo surveillance. When an employer adds *audio* surveillance its liability increases significantly. Audio surveillance brings an employer within the reach of both the Electronic Communications Privacy Act and the Washington Privacy Act. Nearly all video surveillance equipment comes with audio capability. To avoid increased liability, employers should ensure (check the equipment personally or contact the company responsible for overseeing surveillance) that this function is disabled before commencing surveillance.

b. Surveillance and the National Labor Relations Act (NLRA)

Employers should be aware that the National Labor Relations Board has held any surveillance of employees' organizing activities, whether open or concealed, to be an unfair labor practice under the NLRA. An employer also violates the Act when it leads employees to believe that it is engaging in surveillance, even if no surveillance is actually taking place. Employers

should be cautious when using electronic surveillance to monitor organized employees. Even though employers are, as a general matter, allowed to use video surveillance in open and undifferentiated work areas, and are allowed to monitor employees' locations during work hours, such surveillance might violate employees' rights under the NLRA. Surveillance during union organizing campaigns, accordingly, should be carefully reviewed with labor counsel.

c. Off-Duty Surveillance

As the above discussion reveals, employers generally enjoy significant latitude to electronically surveil employees and otherwise to monitor and investigate employees' use of electronic communications and resources. Once an employee is "off-duty," however, the employer's ability to monitor the employee, and its ability to discipline or terminate the employee based upon any information gained during such monitoring, is lessened significantly.

First, a distinction must be drawn between the ability to surveil or monitor an employee and the ability to *take action* based upon the information gathered during such monitoring or surveillance. Although the principles discussed above will govern the determination of whether the monitoring itself is an invasion of the employee's privacy (informed by, for example, whether off-duty use of company-supplied equipment and resources is disclosed in an appropriate policy), more traditional labor law will govern whether an employer may actually take action based upon information that is gathered during surveillance or monitoring.

Generally, when information is gathered about an employee's off-duty activities, a private employer can only take disciplinary action based upon that information if it can show that the activities are "reasonably related" to the employer and/or have the potential to adversely affect the employer. This standard can be difficult to meet. See, e.g., Nelson v. Dep't Empl. Sec., 655 P.2d 242, 244 (Wash. 1982) (holding that an employee terminated for off-duty shoplifting was entitled to receive unemployment benefits). Additionally, states have adopted (in various forms and combinations) up to four theories of wrongful discharge that violates public policy, protecting employees who (i) exercise statutory rights, (ii) fulfill public obligations, (iii) report the employer's unlawful conduct to a supervisor or outside authorities; and (iv) refuse to commit unlawful acts. These exceptions are interpreted narrowly.

Public employees enjoy still greater protection against off-duty monitoring. Federal employees, in particular, may not be terminated based upon off-duty activities unless the "efficiency of the service" is impaired by the activities. 5 U.S.C. § 7503(a). State and local employers have been held to a similar standard. Unlike those in the private workforce, public employees may invoke constitutional protections to challenge an employer's off-duty monitoring and any actions taken by the employer based upon the information gathered during such monitoring. Moreover, employees have challenged termination of employment based upon such information on equal protection, due process, and "void for vagueness" grounds. The results have, without clear bases in fact or reasoning, varied significantly.

Several states also have specific statutes that limit the ability of employers to discipline or terminate employees for off-duty activities such as the use of lawful products, “lawful activity off the premises of the employer during nonworking hours,” and participation in “legal recreational activity.” These statutes contain various exceptions, however, and the few that appear on their face to apply broadly tend to afford employers the latitude to discipline employees for conduct that conflicts with the employer’s business interests. For example:

- Colo. Rev. Stat. § 24-34-402.5(1)(a) makes unlawful an employer’s termination of an employee for the employee’s participation “in any lawful activity off the premises of the employer during nonworking hours [that is unrelated] to a bona fide occupational requirement”);
- Conn. Gen. Stat. § 31-51q protects an employee’s off-duty exercise of constitutional rights, provided that the employee’s activities “[do] not substantially or materially interfere with the employee’s bona fide job performance or the working relationship between the employee and the employer”;
- N.Y. Lab. Law §§ 201-d(2)(c), (3)(a) prohibits dismissal for “an individual’s legal recreational activities outside work hours, off of the employer’s premises and without use of the employer’s equipment or other property” unless it “creates a material conflict of interest related to the employer’s trade secrets, proprietary information or other proprietary or business interest”); and
- N.D. Cent. Code § 14-02.4-01 (1997) protects “participation in lawful activity off the employer’s premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer.”

5. Pretexting

a. Generally

“Pretexting,” the use of various social engineering methods in order to obtain personal information under false pretenses (i.e., a “pretext”), is another concern that employers must be aware of in their day-to-day security practices and, in particular, in connection with workplace investigations.

Pretexting has existed for years, but leapt to prominence when the Hewlett Packard Company (“HP”) was sued by the State of California for “unfair competition,” based upon HP’s use of, and authorization of the use of, pretexting to investigate certain of its current and former employees and board members, their families, and some journalists in connection with leaks from its board of directors. HP settled the suit in December 2006, agreeing to pay \$14.5 million to the state and to implement several modifications to its corporate governance and ethics compliance processes.

b. Telephone Records and Privacy Protection Act of 2006

In the wake of the HP scandal, the U.S. Congress passed the Telephone Records and Privacy Protection Act of 2006, which was signed into law by the President on January 12, 2007. The law is codified at 18 U.S.C. § 1039. The law makes it a crime for any person, in interstate or foreign commerce, to knowingly and intentionally obtain, or attempt to obtain, confidential phone record information of a “covered entity” by:

- making false or fraudulent statements or representations to an employee of a covered entity;
- making false or fraudulent statements or representations to a customer of a covered entity;
- providing a document to a covered entity knowing that the document is false or fraudulent; or
- accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates the Computer Fraud and Abuse Act, 18 U.S.C. §1030, without prior authorization from the customer to whom the confidential phone record information relates.

The law also restricts the purchase or receipt of confidential telephone records. Specifically, the law also prohibits a person from “knowingly and intentionally” purchasing or receiving, or attempting to purchase or receive, confidential phone record information of a covered entity without prior authorization from the customer to whom the confidential phone record information relates, or if the person knows or has reason to know that this information was obtained fraudulently. Violation of the law is punishable by fines, a prison term of up to ten years, or both. Additional fines and penalties apply in the event of certain aggravated violations.

c. Other Sources of Liability

Pretexting may implicate several other sources of potential liability, including other federal statutes (e.g., the Computer Fraud and Abuse Act (“CFAA”), Title II of the ECPA (the Stored Communications Act), the federal Wiretap Act, state pretexting and identity theft statutes, and certain tort claims. A detailed examination of their application is beyond the scope of this summary, but the sheer panoply of potential liability should cause employers to take steps to prevent internal and external investigators from using pretexting.

d. Anti-Pretexting Policies

Defensively, companies should consider appropriate administrative safeguards in place to prevent themselves from being “pretexted.” Perhaps still more importantly, companies should also have a policy that prohibits pretexting and other illegal methods in connection with workplace investigations. As for the former, all customer-facing employees should be trained to identify basic social engineering techniques and to appropriately authenticate all persons who seek access to personal information of the

company's customers or employees. The appropriate authentication method depends upon the company's business and the nature of the information being requested. Moreover, employers should make clear that the company does not use illegal pretexting to gather information in its internal or external investigations and prohibits its outside investigators from doing so.

7. What Employers Should Take Away

Electronic surveillance is a cost-effective way for employers to maintain a safe and productive place of business. It can also be a valuable investigative tool to monitor employee performance or prepare for impending litigation. Before taking advantage of the benefits electronic surveillance has to offer, however, employers should be sure to consider the following:

- **Reasonable Expectation of Privacy:** Ask whether the area under surveillance is one where employees have a reasonable expectation of privacy. Some factors to consider are (1) whether the area under surveillance is an open and undifferentiated work area (as opposed to an area given to the employee for his or her exclusive use); (2) whether the surveillance takes place from a lawful vantage point (i.e. a place where others could lawfully stand and observe); and (3) whether the area under surveillance is a public area (an area accessible to multiple employees). Remember that even if the employee has a reasonable expectation of privacy, employers can still avoid liability as long as (1) the surveillance was not highly offensive to a reasonable person (private employers/public employers – invasion of privacy tort) or (2) the surveillance was conducted for non-investigatory, work-related purposes or as part of an investigation of work-related misconduct and it was “reasonable” (public employers – Fourth Amendment).

In making these determinations, a healthy dose of common sense is helpful (no locker rooms, restroom stalls, places where people are nude or partially nude), do not surveil employees while off-duty (unless specifically warranted by the circumstances), and be prepared with a statement of legitimate business reasons for electronic surveillance.

- **Traditional Labor Law Still Applies:** Employers must bear in mind that the question of whether surveillance violates an employee's reasonable expectation of privacy and, if so, is highly offensive to a reasonable person is distinct from the matter of what an employer may do with information obtained by lawful surveillance. Even if the surveillance is appropriate in the circumstances, that does not mean that the employer may act on the information.
- **No Audio:** Employers should ensure that the audio function is disabled on all workplace surveillance equipment. Otherwise, employers open themselves up to liability under both federal (ECPA) and state (Washington Privacy Act) statutes.
- **Clear Policies:** Employers can diminish employees' REP through clear, published policies that notify employees of the location and nature of surveillance. Employers should distribute such policies at the outset of the employment relationship and obtain signed acknowledgement/consent forms from employees. Employees' acknowledgment of and consent to a valid

surveillance system will generally bar a subsequent tort action against the employer.

- **No Pretexting:** Companies must take steps to ensure that they do not engage in unlawful pretexting in internal or external investigations of employees or others. Companies must also adopt appropriate procedures for verifying the identity of persons who request personal information, and train their employees regarding those procedures, in order to decrease the likelihood of pretexting.

IV. Privacy and Security of Employees' Personal Information

Employers collect vast amounts of personal information associated with their employees. The treatment of some of this information (e.g., medical records, information regarding disabilities, and employee benefit plans) is governed by individual statutes. A myriad of privacy rules and regulations surround the use and disclosure of employees' medical information, for instance.

Employers may be less aware, however, of restrictions on the collection, use and disclosure of other types of employee personal information. Although most of the attention in recent years has focused on the protection of consumers' personal information, many of the same laws and standards apply to employee information. For example, a recent swath of state laws has been enacted that imposes requirements upon employers' use, collection and disclosure of employees' Social Security numbers. Employers are, moreover, obligated to use reasonable security measures to control unauthorized access to, and use or disclosure of, all sensitive personal information that may be attributed to individually identifiable employees. Additionally, employers are obligated to notify affected employees in the event of a security breach in which those employees' personal information is, or is likely to have been, obtained by an unauthorized person. These obligations are explained below.

A. Medical Records

Employers have the right to collect and act upon certain types of employee medical information to inform employment decisions. An emerging area of regulation and litigation concerns the employer's handling of confidential employee medical information. Even if the employer is entitled to gather and act upon employee medical information, it may have a duty to preserve the confidentiality of that information, once acquired. This duty may even require that the employer restrict access to such information within the workplace, as well as to prevent disclosure to others outside the workplace.

Generally, information obtained about an applicant/employee's medical condition or history should be maintained separately from other employment-related information. Medical information should be kept in a separate medical file that is accessible only to designated individuals. Medical information stored electronically must be protected similarly (for example, by storing it in a separate database that is accessible only to designated individuals). In each case, information should be accessible only on a need-to-know basis.

1. HIPAA

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") restricts the use or disclosure of protected health information ("PHI") by a covered entity. PHI is generally defined as individually identifiable health information that a covered entity transmits or maintains in any form or medium.

a. Covered Entities

A “covered entity” is a health plan (e.g., an individual or group health plan that provides, or pays the cost of, medical care), health care clearinghouse (e.g., billing service), or health care provider that conducts certain standard transactions electronically (e.g., nurse, doctor, and hospital).

HIPAA imposes a general prohibition upon the use or disclosure of PHI by a covered entity, except: (1) for treatment, payment, or health care operations (in compliance with HIPAA requirements), (2) upon the individual’s agreement in certain limited situations (after an opportunity to agree or object), (3) to the individual, subject to his or her rights under HIPAA, (4) as permitted or required by HIPAA (for government or other purposes), or (5) pursuant to an authorization from the individual. In addition to complying with PHI use and disclosure restrictions, a covered entity must implement applicable HIPAA privacy and security rules. These rules require elaborate policies, procedures, and systems with respect to maintaining and releasing PHI, including electronic PHI.

b. Employers as Hybrid Entities

Most employers will not be deemed a covered entity. To the extent an employer operates a health care clinic for its employees, as a small part of its operations, the employer may be a “hybrid entity” under HIPAA. An employer that is a hybrid entity must ensure that its health care component separately complies with applicable HIPAA privacy and security rules.

c. Employers as Health Plan Sponsors

Even if an employer is not a covered entity, it may be subject to HIPAA privacy rules if its employees use and disclose PHI while administering a self-insured or self-funded group health plan (with 50 or more participants), such as medical, dental, and vision plans or flexible spending accounts. HIPAA will also apply to an employer indirectly if the employer’s fully insured health plan (of any size) discloses PHI to the employer.

Specific rules enacted under HIPAA apply to disclosures of PHI from an employee health plan or health insurer. For example, a group health plan may not disclose or permit disclosure of PHI to the employer unless plan documents are specially amended and the employer agrees to comply with HIPAA’s privacy requirements. Specifically, the employer must agree to:

- **Refrain from unauthorized use:** PHI may not be used or disclosed other than as permitted by the plan;
- **Use appropriate safeguards:** Steps must be taken to prevent use or disclosure of the PHI other than as provided for in the plan;
- **Report unauthorized disclosure:** The employer must report to the group health plan any use or disclosure of the PHI that is inconsistent with the plan documents or privacy regulations;

- **Ensure subcontractor compliance:** Any subcontractor or agent to whom the employer provides PHI must agree to the same conditions;
- **Ensure employee accessibility to PHI:** An individual's PHI must be accessible to that individual and the individual must be allowed to amend his/her information;
- **Track authorized disclosures:** The employer must provide an accounting of its disclosures of PHI;
- **Report practices to H.H.S.:** The employer must make its practices available to the Secretary of the Department of Health and Human Services for determining compliance;
- **Appropriately dispose of PHI:** The employer must return or destroy PHI when it is no longer needed;
- **Authorize contract termination:** The employer must authorize the health plan to terminate the contract if the health plan determines that the employer has violated a material term of the contract; and
- **Create firewalls:** PHI must be kept separate from other personnel files and employee records.

See 45 C.F.R. § 164.504(e)(2)(i).

d. Employers as Employers

HIPAA generally does not apply to employers in their basic employment role. Employers as a class are not a "covered entity" under HIPAA and medical information in the possession of an employer acquired by virtue of its role as an employer is not PHI. An employer's use or disclosure of such medical information is thus not governed by HIPAA.

i. HIPAA Applicability in the FMLA and ADA Contexts

HIPAA may, however, be triggered by employers when obtaining medical information for FMLA, ADA or other purposes. To avoid HIPAA privacy and security requirements, employers should obtain medical information directly from the employee rather than from the health plan files or the health care provider. If the employer wants to contact the employee's health care provider for additional information or verification, it must obtain a HIPAA authorization from the employee.

Employee authorization is mandatory if a health care provider is to use or disclose PHI for reasons other than treatment, payment or health plan operations. The employee authorization must:

- **Describe the PHI:** The PHI to be used or disclosed must be specifically described;

- **Identify who will receive PHI:** Any person or class of persons who will use, disclose or receive the PHI must be identified;
- **Describe intended use:** Each purpose of the use or disclosure must be described;
- **Specify when the authorization will end:** A date or event that will end the authorization must be specified;
- **Set forth the right to revoke:** The individual's right to revoke authorization must be outlined in writing and how that is done must be explained;
- **Indicate that PHI may be subject to redisclosure:** The authorization must state that the disclosed PHI may be subject to redisclosure by the person receiving the information and that privacy protections may therefore be lost;
- **Include signature and date:** The individual's (or personal representative's) signature and date must be included;
- **Describe a personal representative's authority to act:** If the signature is a personal representative's, include a description of the representative's authority to act for the individual; and
- **State that treatment or benefits may not be conditioned upon authorization:** The authorization must state that treatment, payment, enrollment or eligibility for benefits may not be conditioned on obtaining the authorization to the extent that privacy rules prohibit the imposition of that condition.

It is a good idea for employers to modify their FMLA certification forms to include the HIPAA authorization to expedite receipt of PHI from health care providers.

ii. **HIPAA Applicability in Medical Testing Contexts**

HIPAA also may apply when an employer seeks to receive PHI from covered health care providers related to the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations. Unless the request falls within one of HIPAA's narrow exceptions, the health care provider must obtain authorization from the individual before disclosing the information to the individual's employer. HIPAA does not, however, preclude an employer from conditioning employment on an individual providing an authorization for the disclosure of such information.

e. **Penalties**

The penalties for violations of HIPAA include a \$100 fine for unintentional violations, fines up to \$250,000 for the most serious violations, and criminal

penalties up to one year in prison. The HIPAA statute does not provide a private right of action for HIPAA violations.²

2. Americans with Disabilities Act (“ADA”)

The ADA establishes restrictions of three types involving employee medical information: (1) restrictions on almost all oral or written pre-employment offer inquiries or medical examinations seeking information about an applicant’s disability or severity of disability; (2) restrictions on disclosure of medical records except to statutorily-identified recipients; and (3) restrictions on oral or written post-employment inquiries or medical evaluations unless either voluntary or if undertaken because “job related and consistent with business necessity.” Additionally, the ADA requires that the medical condition or history of any employee shall be collected or maintained on separate forms and in separate medical files.

a. ADA Restrictions Prior to Offer of Employment

Under the ADA, an employer must keep any medical information on applicants or employees confidential, except for the following limited exceptions:

- Supervisors and managers may be told about necessary restrictions on the work or duties of the employee and about necessary accommodations;
- First aid and safety personnel may be told if the disability might require emergency treatment;
- Government officials investigating compliance with the ADA must be given relevant information upon request;
- Employers may be given information to state workers’ compensation offices, state second injury funds or workers’ compensation insurance carriers in accordance with state workers’ compensation laws; and
- Employers may use the information for insurance purposes.

Employers may also provide medical information to decision-makers involved in the hiring process so they can make appropriate employment decisions consistent with the ADA. Such information should only be supplied on a need-to-know basis. Employers may also use the information to determine reasonable accommodation. Even if the applicant voluntarily discloses medical information, the employer must keep such information confidential and may not disclose the condition or the applicant’s need for accommodation.

² Washington’s Uniform Health Care Information Act, Ch. 70.02 RCW, establishes a standard of care for maintenance and disclosure of medical records. The statute also creates civil remedies for the relief of persons damaged by the unauthorized disclosure of medical information, including award of attorneys’ fees to the prevailing party.

While it is not clear on the face of the ADA, the medical confidentiality requirements appear to extend to the employer's duty to all applicants and employees, *regardless of whether they are disabled* within the meaning of the ADA.

b. ADA Restrictions Applicable to Present Employment

Stricter limits on undertaking a medical examination or making inquiries regarding disabilities exist after the employment relationship has commenced. Specifically, an employer cannot require a medical examination or make inquiries of an incumbent employee regarding the existence of a disability, or the severity of a disability, unless the examination or inquiry is shown to be job-related and consistent with business necessity. See 42 U.S.C. § 12112(d)(4)(A); 29 C.F.R. § 1630.14(c). The inquiries or medical examinations must address actual problems with the employee's job performance or legitimate concerns about whether the individual poses a direct threat in the position.

The ADA does not preclude an employer from subjecting an employee to a drug test. Tests for the illegal use of drugs are not considered medical examinations for purposes of the ADA. If the results reveal information about an individual's medical condition beyond whether the individual is currently engaging in the illegal use of drugs, however, this additional information is to be treated as a confidential medical record. 29 C.F.R. § 1630.16(c).

Employers may also offer voluntary medical examinations, such as blood pressure screening clinics, but they must maintain the confidentiality of records generated during such examination. Moreover, when planning for emergencies, employers may ask employees whether they will require assistance in the event of an evacuation because of a disability or medical condition.

3. Family and Medical Leave Act ("FMLA")

Under the Family and Medical Leave Act of 1993 (FMLA), an employer may require that the need for leave for a serious health condition of the employee or the employee's immediate family member be supported by a certification issued by a health care provider. Similarly, an employer may require medical fitness-for-duty certification at the time the employee seeks reinstatement at the end of FMLA leave.

The U.S. Department of Labor has developed a standard form that an employer may use to obtain medical certification, including second and third opinions, from health care providers. An employer may not obtain information beyond that specified in the standard form. 29 C.F.R. § 825.306(a). In all instances, the request for information must relate only to the serious health condition for which the current need for leave exists. Id. As discussed previously, an employee must authorize disclosure by the health care provider of the employee's medical information to the employer.

Employers must maintain FMLA medical records and certifications as confidential medical records in separate files from the employer's personnel files, and if the ADA is also applicable, such records shall be maintained in conformance with ADA confidentiality requirements. Employers must retain FMLA medical records and certifications for at least three years.

4. Fair and Accurate Transactions Act (“FACTA”)

Under the Fair and Accurate Transactions Act’s amendments to the FCRA, medical information may be included in a consumer report prepared for employment purposes only if: (1) it is relevant to process or effect the employment and (2) the applicant or employee has provided specific written consent that clearly and conspicuously describes the use for which the information may be provided. Medical information is defined broadly to include information in any medium that relates to the medical condition of an individual, the provision of care, or payment for services.

Medical information may also be included in a consumer report if it pertains solely to transactions, accounts, or balances relating to debts arising from the receipt of medical services, products or devices, where the information, other than account status or amounts, is restricted or reported using codes that do not identify, or do not provide information sufficient to infer, the specific provider or the nature of such services, products or devices.

B. Social Security Numbers

1. Generally

Employers collect their employees’ Social Security numbers (“SSNs”) as a matter of course during the employment application process and thereafter. Employers need the SSNs for legitimate purposes, such as reporting employee earnings and payroll taxes. SSNs are, notwithstanding their widespread use, one of the most sensitive pieces of personally identifiable information. No other personally identifiable information plays a greater role in linking to or identifying records that contain sensitive information that employees typically wish to remain confidential. Befitting the special status of SSNs, several states have passed laws that impose special protections for them.

Most of the state laws passed in recent years are directed primarily to the interaction between a business and its customers. Several laws do, however, apply to the collection, use, security and disclosure of SSNs collected from employees. These laws generally prohibit the following types of activities:

- Intentionally communicating, displaying, posting or otherwise making more than 4 digits of an SSN available to the public.
- Printing a SSN on any identification card, membership card, or permit or license.
- Using a SSN as a user identifier or login name.
- Requiring transmission of a SSN over the Internet unless the connection is secure or the transmission is encrypted.
- Requiring use of a SSN to access a Web site or any other computer network, unless a password, PIN or other authentication device is also required to access the site.

- Printing a SSN on any materials that are mailed (even if not visible on the outside of the envelope or otherwise visible without manipulation).

These laws typically contain exceptions for the following activities:

- Collection or use for internal verification or administrative purposes.
- Collection or use of the last 4 digits of the SSN.

Additionally, restrictions on mailing SSNs typically contain exceptions for mailing materials containing an SSN where (a) state or federal law requires the SSN to be on the mailed document or (b) where the materials are sent as part of an application or enrollment process; to establish, amend or terminate an account, contract or policy; or to confirm the accuracy of the SSN.

Note that even when SSNs may be mailed pursuant to an exception, they cannot be printed on the outside of an envelope or on a postcard.

At least one state law requires any person or entity who obtains one or more SSNs in the ordinary course of business to create a privacy policy that does at least all of the following concerning the SSNs that the person possesses or obtains:

- Ensures to the extent practicable the confidentiality of SSNs;
- Prohibits unlawful disclosure of the SSNs;
- Limits who has access to information or documents that contain the SSNs;
- Describes how to properly dispose of documents that contain the SSNs; and
- Establishes penalties for violation of the privacy policy.

Mich. Comp. Laws § 445.84.

Legislation is expected to continue to impose new and increased restrictions upon the use and disclosure of SSNs. For instance, a California law set to take effect on January 1, 2008 will prohibit the printing of more than four digits of an SSN on an employee's pay stub or itemized statement. See Cal. Labor Code § 226.

2. Reasonable Security Measures Required to Protect SSNs

A few states have passed laws requiring businesses that own or license personal information about residents of that state (including SSNs) to (a) implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure; and (b) to require by contract that third parties to whom such personal information is disclosed also implement and maintain such procedures. What is meant by "reasonable security" is discussed in Part C below.

Some states impose security measures specific to SSNs. A New York statute, for instance, requires reasonable measures to ensure that no officer or employee has

access to SSNs for any purpose other than a legitimate or necessary business related to the conduct of its business or trade. It also requires the business to provide safeguards necessary or appropriate to preclude unauthorized access to SSNs and to protect their confidentiality.

To address the “reasonable measures” requirement, companies should review their user policies to ensure that access to SSNs is properly restricted. The policies should show that unauthorized access to SSNs has been considered and addressed in order to limit access to that which is necessary for the accessing person to perform a legitimate business function. Technical measures, such as audit trails and attribution methods that tie access to databases containing SSNs to particular user identities (among other things), are necessary to meet the requirement of “necessary or appropriate” safeguards. A lack of appropriate technical measures would violate the New York statute if scrutinized.

3. Secure Disposal of SSNs

Several states have laws under which personal information, including SSNs, must be disposed of properly (e.g., by shredding or burning in the case of paper records, and unrecoverable deletion in the case of electronic records). These obligations are, with minor exception, analogous to the FCRA’s requirements for the disposal of information obtained from credit reports.

C. Security Obligations

1. General Obligation to Secure Personal Information

In addition to specific obligations to protect personal information of consumers and employees found in subject matter-specific statutes, general statutes imposing data security obligations, and other regulations, rules and orders, many commentators have argued that there exists a common law duty to secure personal information of consumers, employees and others that may be in a company’s control at any given time. The extent to which data must be secured is typically expressed in statutes and by enforcement authorities as the use of “reasonable” security measures to prevent the unauthorized use and disclosure of, and access to, personal information.

Attempts to define the general standard of “reasonable security” must take into account all factors relevant to the company’s situation, including the nature of its business, whether the company is in a regulated industry, the size, sophistication and budget of the company, and the amount and nature of the personal information that it collects and maintains. That is, it must be a “process oriented” approach. This is the approach endorsed by the Federal Trade Commission (“FTC”) as a general best practice for all industries. See Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, [available at www.ftc.gov/acoas/papers/finalreport.htm](http://www.ftc.gov/acoas/papers/finalreport.htm).

Characterized generally, a process-oriented data security program that provides reasonable security measures will be comprised of the following:

- **Tailored measures.** Development and implementation of security measures designed or otherwise appropriate to manage and control the specific risks to the security of personal information identified by the company. Risks should be assessed by the likelihood that they will materialize, the potential damage that

would result in that event, and the sufficiency of current safeguards in place to prevent the risk.

- **Oversight of third parties.** If vendors, service providers or other independent contractors have access to personal information, those contractors should be subject to strict contractual restrictions and appropriate oversight.
- **Training and education.** As in the electronic communications context, the best policies are of little value if they are not inculcated into the workforce. Employees should be aware of the importance of data security measures and receive training in how to comply with information security policies.
- **Monitoring and testing.** An information security program should be monitored and tested as appropriate to ascertain its ongoing effectiveness.
- **Review and adjustment.** Reasonable security measures are constantly evolving. They should be questioned, reviewed and, if appropriate, modified to meet new threats while continuing to protect personal information.

As implied by the above requirements, businesses cannot simply argue that their security measures are “consistent with industry standards.” Regardless of what other companies are doing, “reasonable security” requires that proper security measures be implemented to address identified risks.

If the security measures implemented pursuant to this process are insufficient to protect personal information from unauthorized access, one or more state breach notification statutes will require notice to affected consumers. Breach notification requirements are discussed in the next section.

2. **Security Breach Notification: Lost Laptops, Stolen Storage Media, and Hacking Incidents**

a. **Overview of Breach Notification Statutes**

An appropriate security breach mitigation and notification program is a key component of a company’s information security program. California was the first state to require notice to consumers in the event of a security breach in which their personal information may have been compromised. Just a few years later, thirty-seven state laws require notification to affected persons in the event that unencrypted personally identifiable information maintained by a company is, or is reasonably believed to have been, acquired by an unauthorized person. These laws also require notice to the owner of the information (i.e., another company) if the entity suffering the breach is not the owner of the personal information. The material provisions of these laws are summarized in a Perkins Coie chart at www.perkinscoie.com/statebreachchart/chart.pdf.

To characterize the laws generally, the personal information that triggers notice obligations under these statutes typically defined as consisting of a person’s first name or initial and last name, plus any of that person’s SSN, driver’s license or state ID card number, or financial account number or credit or debit card number, together with any required PIN or access code that is

needed to access those accounts. Some states include additional types of information, including ID numbers assigned by employers, electronic signatures, passwords, biometric information, medical information, insurance information, and other, similar information.

The statutes typically require notice to affected persons “in the most expedient time possible, and without unreasonable delay,” in the event that a company discovers or learns of a security breach in which personal information is, or is reasonably believed to have been, compromised. All states allow some form of delay of notification where a law enforcement agency requests it.

The state statutes all specify the means by which notice may be provided. All allow notice via postal mail, but they vary as to whether they allow telephonic, email, “substitute notice” (i.e., publicizing the breach in specified media and/or posting on company’s Web site) or other forms of notice. Only a few specify the content of the notice.

As critical here, these statutes require notice to employees if their personal information is, or is reasonably believed to have been, compromised. Moreover, some state attorneys general may consider it an unfair practice to fail to notify employees whose information may have been compromised (regardless of whether applicable statutes require notice to those employees).

b. Security Breach Mitigation and Response

i. Pre-Breach Planning

Security breaches may occur due to outside hackers, rogue employees, economic espionage, physical intrusion, inadvertence, and the negligence of third-party vendors. Look at the lifecycle of collection, use, storage and disclosure of personal information to understand vulnerabilities. Ensure contractual protections are in place with all third party vendors that have access to or possession of personal information.

Companies should organize a security breach response team and prepare an incident response team now. When a breach occurs, there will be little time to organize and marshal resources effectively. Companies should ensure that the incident response plan identifies the key personnel who will have the responsibility for responding to each item below. After the incident response team is identified, they should undergo training and planning as appropriate to prepare them to implement the plan.

ii. Initial Breach Response

When a company discovers a breach, it should:

- take immediate steps to correct the security failure and ensure that the breach is contained;

- initiate its incident response plan;
- commence the process of gathering and preserving evidence (specific procedures must be followed to preserve evidence properly, so consider legal help if not familiar with them); and
- document response efforts and the costs of remediation (for insurance purposes or to prove damages if necessary).

iii. Notify Law Enforcement

If the breach is ongoing, or consists of hacking, viruses, malware or other malicious or illegal activity, a company should strongly consider notifying law enforcement immediately. A company's local U.S. Attorney can assist in coordination with law enforcement. A company may instead contact the local FBI branch office or the Secret Service.

A company's IT department can invite law enforcement on premises during an attack to assist in the monitoring of communications. See 18 U.S.C. 2511 for computer trespass requirements.

Companies should almost always also notify local authorities. Your employees may need a police report to obtain credit protection or deal with ID theft.

iv. Determine Whether, and to Whom, Notice is Required or Desirable

The triggers for notification under state security breach statutes are detailed in the above-mentioned chart. The decision regarding whether to notify employees will hinge not only upon statutory requirements but also upon the likely effects of the breach on employee morale and public relations. If a company chooses not to disclose the breach, consider the likely effects if that choice was to be discovered later.

A company must also choose whether to notify all employees or only those in states in which notice to employees is required. As noted in the introduction to this section, some state attorneys general believe that it is an unfair practice to fail to notify residents in their state, even if their state does not have a specific notice requirement. It will typically make sense to notify all employees.

If a company maintains personal information on behalf of its owner (i.e., if the company is acting as a vendor or service provider), it will be obligated under the breach notification statutes to notify the owner of the personal information if the personal information is, or is likely to have been, compromised in the breach. The company may also be obligated to notify other persons under its contracts and other agreements.

v. Pre-Notice Planning / Preparation

Employers who suffer a breach and notify employees should prepare for a high volume of calls to customer service, management or other contacts for employees. Companies should draft a script and obtain outside call center services if needed. Depending upon the size and visibility of the company involved, its public relations department and spokespersons should be prepared to answer questions about the breach from the media.

vi. Notify Credit Reporting Agencies

Breach notification statutes require notice to credit reporting agencies if certain thresholds of affected persons are met. Contact the credit bureaus before notifying employees. Include a copy of the notice to consumers and provide information regarding the timing, content and distribution of the notices. As a practical matter, the first credit reporting agency to be notified will notify the other two.

vii. Notify Employees

Determine whether to notify employees individually or to use substitute notification procedures (if available under applicable statutes). Substitute notification procedures are not recommended except where individual notification would be cost-prohibitive or unavailable. This is not typical in the employment context, but can arise if a large number of former or retired employees must be notified.

For individual notices, determine whether email, phone, written or fax notices are most appropriate. Make sure that notice method is allowed in the state in which you use it and be aware of other restrictions (e.g., email notice typically requires E-SIGN compliance).

Most statutes do not specify the notice's content, but a few have minimum requirements. Be careful to word the notice carefully, as it will be widely circulated and is likely to be posted online and/or given to the media.

Some statutes require you to include in the breach notification information regarding credit freezes. Credit freezes, if requested by a customer, prevent credit reporting agencies from releasing the consumer's credit report or any information in it without the express authorization of the consumer. Companies may also wish to touch upon "fraud alerts" and "victim alerts" in their notices to consumers. Employees can contact credit bureaus to add a fraud alert message to their credit reports free of charge. If a fraud alert is in place, a credit provider will require positive ID before extending credit. Employees may request an Extended Fraud Victim Alert by submitting a copy of a valid ID theft report filed with any law enforcement agency. An alert will remain on the report for 7 years and may cause delay in obtaining credit during that period.

viii. Other Notices

If the breach involves credit card information, the company will need to comply with its merchant agreement, Payment Card Industry (PCI) standards and other pertinent rules. The company should notify its merchant bank and its card issuer.

If financial or credit card payment information was compromised, the Secret Service should also be notified.

If a company does business in certain states, or if employees who reside in certain states are affected, certain officials/agencies of and within those states must be notified. Details are contained in the above-mentioned chart of state laws.

ix. Responding to Employee Concerns

Some companies suffering breaches purchase one-year fraud protection insurance from credit reporting agencies for affected persons. Consider this insurance as an employee goodwill gesture.

Ensure that all complaints or concerns that your employees raise are addressed. Be prepared to assist employees who claim identity theft from the breach and know what information you have to release upon request. Maintain a record of response to concerns and any investigation of identity theft.

x. Potential Remedies

As a victim of a security breach, the company may have remedies against the perpetrator, if known. If any individual is prosecuted, the company will have the right to restitution under the Victim and Witness Protection Act.

Companies should understand their role in any criminal prosecution or sentencing of a computer hacker or other data thief. They should ensure that their security procedures and intellectual property do not become part of the evidence in the case and subject to further public disclosure.

Fair Credit Reporting Act (FCRA)

Compliance Chart

	<u>Before Obtaining Report</u>	<u>Before Adverse Action</u>	<u>After Adverse Action</u>
<p>Consumer Report <i>(unrelated to workplace misconduct)</i></p>	<ul style="list-style-type: none"> • Give notice • Obtain written consent • Provide description of rights under FCRA** <p>**NOTE: The description of rights form (available on the FTC website http://www.ftc.gov/bcp/online/pubs/credit/fcrasummary.pdf) has been amended recently. Employers should be sure to update their forms if they have not already done so.</p>	<ul style="list-style-type: none"> • Provide copy of report • Provide description of rights under FCRA 	<ul style="list-style-type: none"> • Disclose nature of adverse action taken • Disclose name, address, and phone number of third party investigator • Disclose that third party investigator did not take the adverse action and cannot explain why it was taken • Disclose right to obtain another copy of the report and dispute it

	<u>Before Obtaining Report</u>	<u>Before Adverse Action</u>	<u>After Adverse Action</u>
<p><u>Investigative Consumer Report</u> (unrelated to workplace misconduct)</p>	<p>In addition to above:</p> <ul style="list-style-type: none"> • Within 3 days of request, employer must mail/deliver: (1) disclosure that investigative report may be made, (2) statement that employee may request additional information on nature and scope, and (3) summary of rights under FCRA. <p>NOTE: If employee requests additional information, employer must disclose nature and scope no later than 5 days after receiving request (or 5 days after ordering report, if later)</p>	<ul style="list-style-type: none"> • Provide copy of report • Provide copy of rights under FCRA 	<ul style="list-style-type: none"> • Disclose nature of adverse action taken • Disclose name, address, and phone number of third party investigator • Disclose that third party investigator did not take the adverse action and cannot explain why it was taken • Disclose right to obtain another copy of the report and dispute it
<p><u>Report sought in connection with investigation of workplace misconduct</u> (or compliance with Fed/State/Local law or policies of employer)</p>	N/A	N/A	<ul style="list-style-type: none"> • Disclose a summary containing the nature and substance of the communication upon which the adverse action was based • <i>Except</i> that sources of information acquired solely for use in preparing the report need not be disclosed