Chapter Twenty-Seven

DATA PRIVACY IN THE WORKPLACE

Chapter Twenty-Seven

DATA PRIVACY ISSUES IN THE WORKPLACE

Table of Contents

Chapter Twenty-Seven

DATA PRIVACY ISSUES IN THE WORKPLACE

Michelle Brauer Abidoye, mabidoye@fordharrison.com*, and*
Jessica Asbridge, jasbridge@fordharrison.com*,*
Chapter Editors

I. INTRODUCTION

Privacy issues impacting the workplace can arise in a variety of contexts from the surveillance of employees (such as videotaping, global positioning systems (GPS) monitoring, and monitoring of employees' electronic communications) to protection of employers' financial and business information, trade secrets and customer/client lists to the recent concerns over the protection of employees' personally identifiable information (PII) arising from data security breaches. Many of these issues are magnified when employers adopt bring your own device (BYOD) policies. This chapter discusses U.S. laws relating to data breaches and employee monitoring, as well as the various concerns that can arise in the BYOD workplace.

Additionally, multinational companies must consider not only U.S. laws, but also broader cross-border privacy laws that often vary from jurisdiction to jurisdiction. For example, the European Commission's Directive on Data Protection requires European Union (EU) member countries to create laws restricting the transfer of personal data of EU resident employees to countries (including the U.S.) that are deemed to have inadequate data privacy protections unless certain requirements are met. The U.S. Department of Commerce in consultation with the European Commission previously developed a "safe harbor" framework under which a U.S. company agreed to apply EU-like data protection to EU data subjects. The U.S. company would self-certify that it complied with the U.S.-EU Safe Harbor Framework, which ensured that EU organizations knew the U.S. company provided "adequate" privacy protection, as defined by the Directive. However, the European Court of Justice recently held, in *Schrems v. Data Protection Commissioner*, that the safe harbor framework is invalid, in part, due to its inability to deal with U.S. government access to data in a way that respected EU data protection rights. The decision may impact companies that relied on "EU model clauses." The European data protection authorities could determine that, because of U.S. surveillance practices and the lack of judicial redress for EU citizens, the U.S. does not meet EU standards, and thus, transfers under the EU model clauses should be suspended. The *Schrems* decision is final and not appealable. Prior to this decision, there was little public enforcement of EU transfer obligations. It is expected that transfer compliance will attract much greater scrutiny in the future.

As a result of this decision, U.S. companies that identify the safe harbor as the mechanism relied on to legitimize data transfers should amend their policies and identify an alternative basis. Alternative bases include obtaining explicit opt-in consent from customers in the EU, as consent is allowed in some EU countries as an exemption to the obligation to ensure adequate protection. However, EU regulators set very high standards for obtaining consent, and thus, this may not be a long-term solution.

In place of the safe harbor, a number of companies have utilized a new approach to cross-border data transfer known as Binding Corporate Rules, in which companies customize their data protections and apply in advance for pre-approval for cross-border transfers to enable global data sharing within a group of companies. However, Binding Corporation Rules may not be a workable solution for start-ups or small/medium businesses due to the time and resources involved in obtaining pre-approval.

As illustrated by the *Schrems* decision, the EU data privacy requirements currently are in a state of flux. On October 16, 2015, the Data Protection Working Party, comprised of U.S. and European policymakers, issued a statement urging the EU and U.S. to find a replacement to the safe harbor framework by the end of January 2016. Multinational employers should remain apprised of developments in EU data privacy laws.

II. DATA BREACH NOTIFICATION REQUIREMENTS

A data breach is generally defined as the unauthorized access to or use of records or data containing PII. Highly publicized data breaches over the past few years highlight the public relations nightmare and potential cost that can be created by a data privacy breach. Although breaches of customer data have long dominated the news, breaches of employee PII are becoming increasingly common and can have significant consequences, as illustrated by the 2015 cyberattack on the U.S. Office of Personnel Management (OPM) files, which involved the theft of "sensitive information" of more than 21.5 million former and current federal employees. The OPM's Chief Information Officer has since testified to Congress that state and nonstate actor attacks on government and business entities will become increasingly more sophisticated in the future, and that those entities need to continue to implement innovative protections against such attacks. Testimony of Tony Scott, June 16, 2015, https://oversight.house.gov/wp-content/uploads/2015/06/Scott-CIO-OMB-Statement-6-16-Data-Breach.pdf.

According to the Identity Theft Resource Center, the number of U.S. data breaches tracked in 2014 reached a record high of 784, which is a 27.5 percent increase over the number reported in 2013. *See Identity Theft Resource Center Breach Report Hits Record High in 2014*, January 12, 2015, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html. The Identity Theft Resource Center 2015 Data Breach Summary, released January 4, 2016, showed that the center identified 781 breaches in 2015, with over 169 million records exposed. According to a study by IBM Security Services in April 2014, companies are attacked an average of 16,856 times a year. In fact, one commentator has described it as a "perpetual stage of siege." According to InfoSecurity Magazine, as of August 2014, more than 10 million personal records have been exposed. No industry is secure, with attacks occurring in restaurant chains, retail stores, financial services providers, health care providers and the government.

Currently, the U.S. has a patchwork regime of federal and state-based laws and regulations that vary in their protections and requirements. An employer's obligation for protecting PII, as well as providing notice of data breaches, varies depending on the laws to which the employer is subject.

A. Proposed Personal Data Notification & Protection Act. In March 2015, legislation was introduced into the U.S. House of Representatives seeking to establish a federal data breach law. The legislation was referred to the House Judiciary committee, but it is unclear whether it will be released from committee for a vote by the House. The legislation – the Personal Data Notification & Protection Act, is intended to clarify and strengthen the obligations companies have to notify customers when their personal information has been exposed, including establishing a 30-day notification requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The legislation also seeks to criminalize illicit overseas trade in identities. *See* H.R. 1704, 114th Cong. (2015).

The proposal defines "sensitive personally identifiable information as any information or compilation of information, in electronic or digital form that includes:

1. An individual's first and last name or first initial and last name in combination with any two of the following data elements:

- home address or telephone number;
- mother's maiden name; and
- month, day, and year of birth.

2. A nontruncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number;

3. Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;

4. A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code;

5. A user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account; or

6. Any combination of the following data elements:

- an individual's first and last name or first initial and last name;
- a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or
- any security code, access code, or password, or source code that could be used to generate such codes or passwords."

The proposal permits the Federal Trade Commission (FTC) to amend the definition of sensitive PII "to the extent that such amendment will not unreasonably impede interstate commerce, and will accomplish the purposes of" the proposed law. In amending the definition, the FTC may determine that any particular combinations of information are sensitive PII, or that any particular piece of information, on its own, is sensitive PII.

The proposal would require businesses engaged in interstate commerce that use, access, store, transmit, dispose of or collect sensitive PII regarding more than 10,000 people in a 12-month period to notify any individual whose sensitive PII has been accessed or acquired "unless there is no reasonable risk of harm or fraud to" the individual. As noted above, the proposal generally requires notice within 30 days, with exceptions for law enforcement or national security. The proposal provides for a safe harbor for companies that have conducted a "risk assessment" as defined in the proposal and have determined that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive PII was subject to the security breach. It also provides for a limited exception for companies that participate in certain types of security programs. The law would be enforced by the FTC, and a violation would be treated as an unfair or deceptive trade practice. The proposal would also permit state attorneys general to bring civil actions to enforce the law, including seeking penalties of not more than $1,000 per day per individual whose sensitive PII was accessed or acquired, up to a maximum of $1 million per violation, unless the violation is found to be willful or intentional. The legislation is available at: https://www.congress.gov/bill/114th-congress/house-bill/1704/text.

B. Prevention of a Data Breach. Data breaches can occur in a variety of ways; however, Michael Bruemmer, the vice-president of Experian's data breach resolution group, has stated that more than 80 percent of the breaches his company works with "had a root cause in employee negligence." According to Elizabeth Weise, journalist for USATODAY, "43% of U.S. Companies had a Data Breach in the Past Year," USATODAY, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/. According to Bruemmer, this "could be from someone giving out their password, someone being spear-phished, it could be a lost USB, it could be somebody mishandling files, it could be leaving the door to the network operations center open so someone can walk in." *Id.* Other ways data breaches may occur include the loss or theft of mobile devices or laptops containing records of PII; disclosure through the use of unsecured wireless networks or peer-to-peer networks; breaches of vendors' secure databases; and inadvertent disclosure through e-mail attachments. Data breaches can also occur due to the intentional theft of records by employees. The FBI has issued an alert to U.S. businesses regarding the significant insider threat posed by disgruntled employees. The FBI has concluded that such intentional breaches have caused harm as high as $3 million per incident to the affected companies. *See* http://www.ic3.gov/media/2014/140923.aspx.

Formerly, organizations could easily screen untrustworthy applicants who will have access to sensitive data by asking applicants to check a box as to whether they had ever previously been convicted of a crime. However, numerous states have now enacted "ban-the-box" laws, which prohibit employers from asking such a question. Employers should review their states' laws regarding the permissibility of asking for criminal background information. Most laws do permit an employer to conduct a lawful, post-interview, pre-employment background check. For more information, please see the *Hiring* Chapter of the SourceBook.

III. DATA PRIVACY AND SECURITY LAWS

A. Federal Laws Addressing Data Privacy and Security. As noted above, there currently is no one, generally applicable federal law that imposes data privacy and security obligations on employers. Certain anti-discrimination laws such as the Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act of 2008 (GINA) require employers to keep employees' medical information confidential. Under the ADA, medical information must be kept in separate files, segregated and secured from general personnel files. Certain exceptions may be made to the confidentiality requirement, including for supervisors and managers who may be informed about necessary restrictions on employees with disabilities and accommodations for them; first aid and safety personnel who may be informed if an employee might require emergency treatment related to the disability; and government officials investigating employer compliance with the ADA, who are entitled to be provided with relevant information on request. Generally, however, those without a need to know the information should not have access to the medical information. While the ADA protects the confidentiality of medically related information, it does not contain a data breach notification requirement. GINA restricts the collection and disclosure of genetic information unless the circumstances warrant a limited exception under the statute. For more information, please see the *Americans with Disabilities Act and Other Disability Discrimination Laws* SourceBook Chapter.

Additionally, laws regulating specific industries may impose data privacy requirements, although these often are directed at protecting the privacy of information obtained from consumers or customers rather than employees.

1. Gramm-Leach-Bliley Act (GLBA). The federal Financial Modernization Act of 1999, also known as the GLBA applies to "financial institutions" and prohibits covered entities from disclosing consumers' nonpublic personal information, with certain exceptions, unless the entity has provided notice to the consumer. The notice must be provided at the time a customer relationship is established and at least annually after that. The Federal Trade Commission (FTC) is one of eight federal agencies that enforces provisions of the GLBA. Rules developed under the GLBA include the Financial Privacy Rule, which governs how institutions can collect and disclose of customers' personal financial information; the Safeguards Rule, which requires all financial institutions to maintain safeguards to protect customer information; and another provision designed to prevent individuals and companies from gaining access to consumers' personal financial information under false pretenses, a practice known as "pretexting." More information on this law is available on the FTC's web site at: http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/financial-privacy. There is no private right of action under the GLBA. The FTC also enforces broad consumer protection laws such as the Federal Trade Commission Act (FTC Act), which is a consumer protection law that has been applied to business practices that affect consumer privacy and data security.

2. The Fair Credit Reporting Act (FCRA). The federal FCRA, 15 U.S.C. § 1681a, *et seq.*, governs an employer's request for or use of a "consumer report" or "investigative consumer report" prepared or collected by a "consumer reporting agency." The FCRA's restrictions on the use of consumer reports by employers are discussed in more detail in the *Hiring* Chapter of the SourceBook.

a. The Red Flags Rule. The FCRA was amended by the Fair and Accurate Credit Transaction Act (FACTA), which, among other things, allows consumers to place fraud alerts on their credit histories to reduce the risk of identity theft. FACTA also required the FTC, along with other federal agencies, to develop a Rule (the Red Flags Rule) requiring "creditors" and "financial institutions" with covered accounts to implement programs to identify, detect, and respond to the warning signs, or "red flags," that could indicate identity theft. The rule was issued in 2008. Although primarily created for the purpose of increasing protections against identity theft, the rule imposed new requirements on employers conducting background checks. Specifically, employers must have policies in place for dealing with "red flag" notifications from credit reporting agencies (CRAs). Under the regulations, CRAs must notify employers of a substantial difference between the address for the applicant or employee that the employer provided and the address in the CRA's file. Employers must have procedures in place to form a reasonable belief that the consumer report relates to the applicant or employee about whom the employer has requested the report upon receipt of the "red flag" notice.

The policy could take the form of an internal memorandum to human resources or any other person(s) responsible for conducting the employer's background checks. There are several methods that may be utilized to achieve the necessary reasonable belief that the consumer report relates to the individual about whom the report was requested. The employer may reasonably confirm an address by:

(1) verifying the address with the individual;

(2) reviewing its own records to verify the individual's address;

(3) verifying the address through third parties; or

(4) using reasonable means.

The employer must also provide the CRA with an assurance that it has reasonably confirmed the information is accurate. More information regarding the Red Flags Rule is available at: https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business.

b. Document Destruction Requirements. The FTC's Document Disposal Rule requires employers to take reasonable measures to properly dispose of consumer information derived from "consumer reports" by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. The Disposal Rule was issued pursuant to the requirements of FACTA. The rule is designed to reduce the risk of consumer fraud, including identity theft, created by improper disposal of consumer information. The text of the Disposal Rule is published at 16 CFR Part 682.

The Disposal Rule applies to any person or entity subject to FTC jurisdiction and who, for a business purpose, maintains or otherwise possesses consumer information. Employers who obtain consumer reports for any of the permissible purposes listed in the FCRA (for example, reports from a third party CRA in conjunction with a background check for employment purposes or any compilation of such information) are covered by the Disposal Rule.

While the Disposal Rule does not specify how those covered by the rule should dispose of consumer information, it notes in the Preamble that the FTC expects covered entities to consider the sensitivity of the information, the nature and size of the entity's operations, the costs and benefits of different disposal methods and relevant technological changes. The FTC's website notes that reasonable measures for disposing of consumer report information could include establishing and complying with policies to:

- burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include:

(1) reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule;

(2) obtaining information about the disposal company from several references;

(3) requiring that the disposal company be certified by a recognized trade association; and

(4) reviewing and evaluating the disposal company's information security policies.

See http://business.ftc.gov/documents/alt152-disposing-consumer-report-information-rule-tells-how. The Preamble to the Disposal Rule also notes that reasonable measures likely will require elements such as the establishment of policies and procedures governing disposal and employee training.

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other things, HIPAA restricts the instances in which a "covered entity" can use or disclose "protected health information" (PHI) and imposes a variety of administrative tasks on covered entities that are designed to ensure that PHI is appropriately protected. Provisions of HIPAA relevant to data privacy and protection include the Standards for Privacy of Individually Identifiable Health Information (the HIPAA privacy rule), which governs the collection, use and disclosure of PHI and the Security Standards for the Protection of Electronic Protected Health Information (the HIPAA Security Rule), which provides standards for protecting PHI. Additionally, the Standards for Electronic Transmission (HIPAA Transactions Rule) applies to the electronic transmission of medical data.

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) issued final regulations addressing various aspects of HIPAA compliance, including changes to:

- The HIPAA privacy, security and enforcement rules required under the Health Information Technology for Economic and Clinical Health (HITECH) Act;
- The breach notification rules for unsecured PHI; and
- The HIPAA privacy rules required by the GINA.

The final regulations were effective March 26, 2013. The final rule is available at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

a. Who Must Comply with the HIPAA Privacy and Security Rules? Only three types of "covered entities" must comply with the HIPAA privacy and security rules: (i) a health care provider that transmits health information electronically; (ii) a health care clearinghouse; and (iii) a health plan. An employer is not a covered entity and, for that reason, generally is not subject to the HIPAA privacy and security rules in its capacity as an employer. However, to the extent an employer sponsors or administers a "group health plan" for its employees, it must ensure that its health plan complies with these rules.

For purposes of the HIPAA privacy and security rules, a "group health plan" is a plan that provides, or pays for the cost of, medical care. It includes hospitalization plans, major medical plans, health maintenance organizations (HMOs), dental plans, vision plans, health care flexible spending account plans, long-term care plans, and other types of plans that provide medical care. An employee assistance program is a health plan for HIPAA purposes, unless it is merely a referral service that does not provide medical care. However, a plan providing only accident or disability income insurance is not a health plan under HIPAA, nor is a plan providing only workers' compensation insurance. Only employer plans with 50 or more participants, or that are administered externally, are subject to the HIPAA privacy rules.

In summary, except for health care providers and health care clearinghouses, an employer must comply with HIPAA only if it sponsors a group health plan (as defined above) that covers 50 or more participants or that is administered by an outside third party.

Under the 2013 final regulations issued by HHS, business associates of covered entities are directly liable for compliance with certain of HIPAA's privacy and security requirements. A business associate includes a person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a covered entity where the provision of the service involves the disclosure of protected health information from such covered entity to the person. The final regulations also adopt HHS' proposal to apply the business associate rules to subcontractors, and clarify the definition of subcontractor to mean "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate."

b. What Information Is Protected? Under HIPAA, only the use or disclosure of PHI is regulated. PHI is any individually identifiable health information transmitted or maintained by the covered entity, *other than* employment records held by a covered entity in its role as an employer. *See* 45 C.F.R. § 160.103. To be considered PHI, the information must (i) relate to the physical or mental health of an individual or to the provision of or payment for health care; and (ii) identify or have the potential to identify the individual. The 2013 regulations also clarify that, in accordance with the requirements of GINA, genetic information is health information. The regulations also prohibit group health plans and insurers from using or disclosing genetic information for underwriting purposes.

Note that employment records are not considered PHI under HIPAA. Regulations do not define the type of information that is considered employment records. However, in the preambles to the HIPAA privacy regulations, HHS stated that "medical information needed for an employer to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees, may be part of the employment records maintained by the covered entity in its role as an employer."

c. How May PHI Be Used? An employer that creates or maintains PHI in its capacity as the sponsor of a group health plan must ensure that it uses or discloses PHI only for those purposes permitted under HIPAA. HIPAA permits PHI to be used or disclosed: (i) for treatment, payment or health care operations, (ii) pursuant to a valid HIPAA authorization form, and (iii) in a variety of other enumerated circumstances, such as when required by law, in abuse or neglect situations, for law enforcement purposes, etc., if specified conditions are met. PHI may not be used by an employer to make employment decisions regarding an individual, nor can PHI received under one health plan be used to make benefit decisions under another health plan. For more information on the disclosure of PHI, including to business associates, please see the *Employee Benefits* Chapter of the Sourcebook.

d. What Else Does HIPAA Require? In addition to restricting the use and disclosure of PHI, HIPAA imposes a variety of administrative tasks on covered entities. These tasks are designed to ensure an individual's PHI is appropriately protected. Where employer-sponsored group health plans are concerned, the level of an employer's involvement in the administration of the plan and, in particular, the types of PHI the employer maintains or receives, will determine the extent to which it must comply with these administrative requirements. For example, an employer who sponsors a fully insured group health plan and receives no more than summary health information will have few administrative compliance tasks. On the other hand, an employer who receives more than summary health information from an insurer, or that sponsors a self-funded health plan, must comply with all of the administrative requirements of HIPAA. Those requirements include designating a privacy official; providing training to employees on the HIPAA privacy rules; implementing appropriate physical, administrative and technical safeguards to protect PHI; establishing a process for privacy complaints; establishing sanctions for HIPAA violations; mitigating the effects of wrongful uses or disclosures; refraining from intimidating or retaliatory acts; not conditioning treatment or payment, enrolling in the plan, or being eligible for benefits on a waiver of HIPAA rights; implementing privacy policies and procedures, implementing security standards for electronic PHI; maintaining written documentation; and drafting and distributing a notice of privacy practices. In addition, all group health plans must contain language that, among other things, describes the ways in which PHI will be used or disclosed and identifies those employees who will have access to PHI. Access to PHI must be limited to those employees identified in the health plan document. For more information, please see the *Employee Benefits* Chapter of the SourceBook.

e. Notification of Security Breaches. In the event of a breach of unsecured PHI, the 2013 regulations impose certain notification requirements on covered entities and business associates. Unsecured PHI is defined as protected health information that is not secured using Secretary of HHS-approved standards. The covered entity or business associate must provide notification of a breach of unsecured PHI "without unreasonable delay," and in no case later than 60 days, after discovery of the breach.

The 2013 final regulations revise and clarify the definition of breach and a risk assessment approach (used to determine if there was a significant risk of harm to an individual due to an impermissible use or disclosure), both of which were addressed in earlier regulations. Under the amended definition of breach, an impermissible use or disclosure of PHI is presumed to be a breach unless a covered entity or business associate can demonstrate that there is a low probability that the PHI was compromised.

The final regulations removed the harm standard under earlier guidance providing that breach notification was not required if it could be demonstrated that there was no significant risk of harm to the individual. Instead of assessing the risk of harm to an individual, covered entities and business associates must assess the probability that PHI was compromised, based on a risk assessment that considers at least the following factors:

- the nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI was mitigated.

A business associate who discovers a breach must report it to the covered entity. In the case of a breach discovered by the covered entity, the notice is to be provided directly to the individual impacted or to prominent media outlets of a state or jurisdiction if 500 or more residents are impacted. Additionally, for a breach involving 500 or more individuals, notice must be provided immediately to the Secretary of HHS.

The notification of breach must include the following information (to the extent possible):

- a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- a description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number (SSN), date of birth, home address, account number, or disability code);
- the steps individuals should take to protect themselves from potential harm resulting from the breach;
- a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

More information is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

B. State Data Privacy Laws. At the state level, various states have enacted comprehensive employee data privacy laws that protect health information and certain identifiable information, such as employee SSNs.

1. Data Breach Notification Laws. According to the National Conference of State Legislatures (NCSL), 47 states as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted legislation requiring private or governmental entities to notify individuals of security breaches involving PII. *See Security Breach Notification Laws,* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, which includes a list of state security breach notification laws. The list is set forth below; however, employers may want to check the NCSL web site for any updates that may have occurred since the publication of this edition of the SourceBook.

State	Citation
Alaska	Alaska Stat. § 45.48.010, *et seq.*
Arizona	Ariz. Rev. Stat. Ann. § 44-7501
Arkansas	Ark. Code § 4-110-101, *et seq.*
California	Cal. Civ. Code § 1798.29; *id.* § 1798.80, *et seq.*
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b
Delaware	Del. Code Ann. 6 § 12B-101, *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code Ann. §§ 10-1-910, *et seq.*; *id.* § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1, *et seq.*
Idaho	Idaho Code Ann. §§ 28-51-104 to -107
Illinois	815 Ill. Comp. Stat. 530/1, *et seq.*
Indiana	Ind. Code §§ 4-1-11-1, *et seq.*; *id.* §§ 24-4-14-1, *et seq.*
Iowa	Iowa Code §§ 715C.1; 715C.2
Kansas	Kan. Stat. Ann. §§ 50-7a01, *et seq.*
Kentucky	Ky. Rev. Stat. Ann. § 365.732; *id.* § 61.931 to 61.934
Louisiana	La. Rev. Stat. Ann. §§ 51:3071, *et seq.*; *id.* §§ 40:1300.111-.116 (Health Care Consumers' Right to Know)
Maine	Me. Rev. Stat. tit., 10 §§ 1347, *et seq.*
Maryland	Md. Code Ann., Com. Law §§ 14-3501, *et seq.,* Md. Code Ann., State Gov't §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws ch. 93H §§ 1, *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63; 445.72
Minnesota	Minn. Stat. §§ 325E.61; 325E.64
Mississippi	Miss. Code Ann. § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code Ann. §§ 2-6-1501 to -1503; *id.* §§ 30-14-1701, et seq.; *id.* § 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801, et seq.
Nevada	Nev. Rev. Stat. §§ 603A.010, et seq.; *id.* § 242.183
New Hampshire	N.H. Rev. Stat. Ann. §§ 359-C:19, et seq.; *id.* § 189:66
New Jersey	N.J. Stat. Ann. §§ 56:8-161, -163

State	Citation
New York	N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law § 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	N.D. Cent. Code §§ 51-30-01, et seq.
Ohio	Ohio Rev. Code Ann. §§ 1347.12, 1349.19, 1349.191-92
Oklahoma	Okla. Stat. 74 § 3113.1; Okla. Stat. 24 §§ 161-166
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628; 2015 S.B. 601, Chap. 357 (effective January 1, 2016)
Pennsylvania	73 Pa. Con. Stat. §§ 2301, et seq.
Rhode Island	R.I. Gen. Laws §§ 11-49.2-1, et seq.; 2015 S.B. 134, Public Law 2015-138, 2015 H.B. 5220, Public Law 2015-148
South Carolina	S.C. Code Ann. § 39-1-90
Tennessee	Tenn. Code Ann. §§ 47-18-2107, 8-4-119
Texas	Tex. Bus. & Com. Code Ann. §§ 521.002; 521.053; Tex. Educ. Code § 37.007(b)(5); Tex. Pen. Code § 33.02
Utah	Utah Code Ann. §§ 13-44-101, et seq.; *id.* § 53A-13-301(6)
Vermont	Vt. Stat. Ann. tit. 9, §§ 2430, 2435
Virginia	Va. Code Ann. §§ 18.2-186.6, 32.1-127.1:05 (breach of medical information by state agency), § 22.1-20.2
Washington	Wash. Rev. Code §§ 19.255.010; 42.56.590 (public officers and agencies)
West Virginia	W. Va. Code §§ 46A-2A-101, et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. Ann. §§ 6-3-901, 40-12-501, et seq.
District of Columbia	D.C. Code §§ 28-3851, et seq.
Guam	9 Guam Code Ann. §§ 48.10, et seq.
Puerto Rico	P.R. Laws Ann. 10 §§ 4051, et seq.
Virgin Islands	V.I. Code Ann. 14, § 2208

2. Issues Frequently Addressed in State Data Breach Laws. State laws addressing data breach notification can vary greatly, with some providing very limited protection while others impose much tougher standards such as requiring companies to offer affected individuals at least a year of free credit protection or permitting the recovery of damages. *See* Seth Rosenblatt, *Obama's Data Breach Initiative Has Privacy Advocates Optimist, Cautious,* January 13, 2015, http://www.cnet.com/news/obama-data-breach-plan-has-privacy-advocates-optimistic-cautious/. Following are some of the more common issues addressed by these laws.

a. Who Must Comply With the Law? A state law may apply only to government agencies or may also cover businesses, sometimes with a minimum size threshold, as well as information collectors/data brokers. Laws often distinguish between those who own or license the data that has been breached and those who have data in their possession, such as vendors. Most laws require a nondata owner to notify the data owner of a breach immediately or as soon as practicable following discovery. Florida, however, requires such notice no later than 10 days after discovery of the breach.

b. Definition of PII. Most laws define this as the individual's name (first and last or first initial and last name) combined with some type of informational/data element when the element is not encrypted or redacted such as:

- SSN;
- Driver's license, voter identification or other official state identification number;
- Account, credit card or debit card number in combination with (Massachusetts and Kansas laws provide **alone** or in combination with) a security code, access code or password (Iowa's recently amended law adds expiration dates of credit and debit cards combined with the credit or debit card number.); and
- Passwords, personal identification numbers, or other codes for financial accounts.

Laws generally exclude publicly available information from the definition of personal information. State laws should be reviewed carefully because a specific state may define personal information to include information not found in other states' statutes. For example, North Dakota includes an individual's employee identification number, and both North Dakota and Texas include mother's maiden name, as does the proposed Personal Data Notification & Protection Act discussed above. *See* Tex. Bus. & Com. Code Ann. § 521.002. Wyoming includes an individual's tribal identification card. *See* Wyo. Stat. Ann. § 6-3-901.

Iowa's recently amended law redefines personal information to include encrypted or redacted personal information if the keys to unencrypt, unredact or otherwise read the data have been obtained. Chabrow, *supra,* http://www.bankinfosecurity.com/states-advance-breach-notification-laws-a-6762/p-2. Oregon has a similar provision. *See* Or. Rev. Stat. § 646A.602. Oregon's law further defines personal information to include any of these data elements when **not** combined with the consumer's first name or first initial and last name and when the data elements are **not** rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. *Id.* (emphasis added).

Additionally, the following elements are sometimes included in the definition of personal information:

(1) Medical Information. As noted above, HIPAA protects personally identifiable health information, but some states also include this in the definition of personal information. *See* Arkansas, Ark. Code § 4-110-103 (medical information); California, Cal. Civ. Code § 1798.29 (medical and health insurance information); Florida, Fla. Stat. § 501.171 (medical and health insurance information); Texas, Tex. Bus. & Com. Code § 521.002 (information relating to the individual's health, the provision of health care, and the payment for health care); Missouri, Mo. Rev. Stat. § 407.1500 (medical and health insurance information); North Dakota, N.D. Cent. Code § 51-30-01 (medical and health insurance information); and Puerto Rico, P.R. Laws Ann. 10 § 4051 (medical information protected by HIPAA). Wisconsin includes DNA in its definition of "personal information." Wis. Stat. § 134.98.

(2) Biometric data. A few states, Nebraska, Neb. Rev. Stat. § 87-802; Iowa, Iowa Code § 715C.1; and Wisconsin, Wis. Stat. § 134.98, include biometric data in the definition of personal information.

(3) Username or e-mail with a password. Currently only Florida and California include user name or e-mail with password in the definition of personal information. *See* Fla. Stat. § 501.171; Cal. Civ. Code § 1798.29. Puerto Rico includes "[n]ames of users and passwords or access codes to public or private information systems." *See* P.R. Laws Ann. 10 § 4051(a)(4).

c. Trigger for Notification Requirement. State laws vary with regard to what circumstances trigger the requirement to provide notification of a breach of data security. Many require some "risk of harm" before notice is required. For example, Ohio's statute requires notice if a breach "causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state." Ohio

Rev. Code Ann. § 1349.19. Florida law states that notice to affected individuals is not required if, "after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years." Fla. Stat. § 501.171(4)(c). Other state laws do not include such "risk of harm" provisions. *See* Ga. Code Ann. § 10-1-912.

d. Who Must be Notified of the Breach? In addition to the affected person, many laws require notification be provided to other entities such as law enforcement, state regulators, the media and/or consumer reporting agencies. Some laws impose additional notification requirements depending on the number of people affected by the breach. For example, in 2014, Iowa amended its breach notification law to require notice be sent to the Consumer Protection Division of the Office of Attorney General within five business days of notifying consumers of a breach if the breach affects more than 500 people. *See* Eric Chabrow, States Advance Breach Notification Laws, April 18, 2014, http://www.bankinfosecurity.com/states-advance-breach-notification-laws-a-6762/p-2. Similarly, California's general breach notification law requires notification be provided to the state attorney general if a breach requires notice to more than 500 California residents. Missouri requires notice to the attorney general if 1,000 or more people are affected by a breach.

e. Time Frame for Providing Notice. Many state laws require notice be provided as expediently as possible, without unreasonable delay, etc., but some states require notice be provided within a specific time frame. For example, in Maine, once it is determined that notification is required, it must be provided no later than seven days after law enforcement concludes that such notification will not jeopardize a criminal investigation. Maine Rev. Stat. tit. 10 § 1348. In Vermont, notice must be provided as expediently as possible but no later than 45 days after discovery of the breach. Vt. Stat. Ann. tit. 9, § 2435.

f. Method of Notification. State laws vary with regard to the type of notification they permit. Most states permit written and e-mail notification, although some states impose specific requirements before e-mail notification can be used. Some states permit notice to be made by telephone, although they may impose restrictions such as prohibiting prerecorded messages or requiring written notice if telephone notice cannot be provided through a live conversation. Most states also permit substitute notice, although this may be limited to situations involving information brokers/data collectors and may require them to demonstrate that the cost of providing notice would exceed a certain amount or that the number of individuals who must receive notice exceeds a certain threshold. Substitute notice may include e-mail notification, conspicuous posting of the notice on the information broker/data collector's web site or notification to media. Additionally, some states, such as California, require particular content for the notification.

g. Penalties/Enforcement. Approximately half of the state data breach laws provide for some sort of penalty; however, the basis for the penalty varies. In some states, the penalty is per breach, while others base it on the number of individuals affected by the breach. Other states, such as Florida and Ohio, calculate the penalty based on the length of delay in notification. *See* Fla. Stat. § 501.171; Ohio Rev. Code Ann. § 1349.192. Some laws also permit the state attorney general to bring an action against a company based on a violation of the breach notification statute.

h. Private Right of Action. Several states permit individuals injured by a data breach to bring a lawsuit against the company, including: Alaska, California, Hawaii, Louisiana, Maryland, Massachusetts, Minnesota, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas (under the Deceptive Trade Practice Act), Virginia, Washington State, and the District of Columbia.

3. State Laws Restricting the Use of SSNs. In addition to data breach notification laws, in another effort to protect citizens from identity theft, some states have enacted laws restricting the use of SSNs. While the provisions of the laws vary from state to state, they commonly include prohibitions or limitations on the display and use of SSNs, limitations on a company's ability to require SSNs to be transmitted over the internet, and, in some states, a notification requirement if the privacy of an SSN has been breached. Employers should consult the laws of the states in which they have operations to determine whether those states have enacted laws regulating the use or disclosure of SSNs.

4. Policy Considerations. Safeguards a company should have in place to minimize risk of a breach include:

- create and maintain data security policies and procedures;
- classify and segregate sensitive data;
- designate Chief Privacy and Information Security Officer(s);
- implement IT and other physical controls (e.g., encryption, secure areas, locked file cabinets);
- establish personnel controls (e.g., background checks, restricted access);
- train employees on data security policies and stress the importance of internal reporting;
- conduct data privacy and security risk assessments and audits; and
- develop and maintain data privacy and security standards for third party vendors and contractors.

Additionally, the following steps can help prepare for a breach before it happens:

- create a data incident response team with clear assigned roles;
- outline key steps to take within 24 hours of a suspected breach;
- train employees on how to spot and report a suspected breach;
- have litigation and media plans in place in the event of a breach;
- maintain relationships with outside advisors who may be needed soon after report of a suspected breach (e.g., IT technicians, lawyers, data recovery and other forensics experts);
- track data breach laws, rules and notification mandates for all relevant jurisdictions (e.g., various US states or any countries where your company does business); and
- conduct breach response drills to improve effectiveness.

IV. EMPLOYEE MONITORING

Employers may have any number of reasons to monitor an employee, from assessing productivity to ensuring the security of confidential business information to investigating allegations of misconduct, including harassment, discrimination or theft. The most common forms of employee monitoring include closed circuit or video cameras, the monitoring and recording of telephone conversations, monitoring or recording verbal communications, monitoring communications through computer networks, utilizing computer programs designed to track productivity, and using tracking technology such as GPS on vehicles or mobile devices used for work.

A. Monitoring Electronic Communications, Internet and Computer Usage. As e-mail increasingly becomes the primary form of communication in many organizations, employers have recognized the need to monitor e-mail content. Most lawsuits challenging the legality of an employer's monitoring of an employee's electronic communications on a company-owned computer or device have been unsuccessful. Generally, courts have found that if an employer has notified employees that company-owned equipment is the property of the employer and it reserves the right to inspect the equipment or monitor employee activities at any time, such notice eliminates any expectation of privacy an employee may have with regard to activities conducted on that equipment. The Seventh Circuit has noted that "abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002). However, there may be a greater likelihood of liability if employer monitoring ventures into personal accounts or websites.

Two primary sources of legal liability resulting from monitoring employees' e-mails are: (1) claims arising under the Electronic Communications Privacy Act of 1986 (ECPA); and (2) state law invasion of privacy claims. However, employers should review the laws of the states in which they have employees because some state statutes may also regulate the monitoring of employee e-mail or other on-line activity.

1. ECPA. In 1986, ECPA amended the federal Wiretap Act,[1] which previously only addressed the interception of wire (i.e. telephone) and oral communications, to also address the interception of electronic communications. *See U.S. v. Steiger*, 318 F.3d 1039, 1046 (11th Cir. 2003); 18 U.S.C. §§ 2510-2522.

The ECPA also created the Stored Communications Act (SCA), which protects against unauthorized access to stored electronic communications and records. *See* 18 U.S.C. §§ 2701-2711. Additionally, the ECPA created provisions applicable to pen registers and trace and trap devices. *See* 18 U.S.C. 3121-3127; *Privacy, An Overview of the Electronic Communications Privacy Act,* Congressional Research Service, October 9, 2012, https://www.fas.org/sgp/crs/misc/R41733.pdf.

Although the ECPA does not specifically mention e-mail in the definition of "electronic communication," the legislative history clearly shows Congress' intent to include it within the definition of "electronic communications." *See* Sarah DiLuzio, *COMMENT: Workplace E-Mail: It's Not as Private as You Might Think*, 25 Del. J. Corp. L. 741, 745, n.25 (2000). However, the ECPA was written prior to the advent of the Internet and has been criticized for its ambiguity. *See* Leonard Court, *The Workplace Privacy Myth: Why Electronic Monitoring is Here to Stay*, 29 Okla. City U. L. Rev. 15 (2004); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) ("the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website.") Additionally, as discussed below, while courts have applied its provisions to employer monitoring of employee e-mail, few employers have been found liable under the Act.

a. Interception under the Federal Wiretap Act. The Wiretap Act prohibits the unauthorized interception of electronic communications. Federal courts generally have held that for electronic communications to be intercepted within the meaning of the Wiretap Act, they must be acquired contemporaneously with transmission. *See, e.g. Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission," thus, the employer did not violate the Wiretap Act when it examined a former employee's e-mails stored on its central file server), *as amended* (Jan. 20, 2004). *See also Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (reiterating its holding in *Konop v. Hawaiian Airlines*, that Congress did not intend for "intercept" as used in the Wiretap Act to apply to electronic communications when those communications are in electronic storage); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (finding that, to constitute an interception, an electronic communication must be captured contemporaneously with transmission); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) ("for a website such as Konop's

1 The Federal Omnibus Crime Control and Safe Streets Act of 1968 (popularly known as Title III).

to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."); *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F. Supp. 2d 417, 431 (S.D.N.Y. 2010) ("the law in the majority of the courts to have examined the issue, is that electronic communications cannot be intercepted for purposes of the ECPA after they have been delivered, at which point they become 'stored communications' regulated by the SCA"; rejecting the argument that the e-mails in question were intercepted within the meaning of the Act because they were read at or very near the time the messages arrived in the recipients accounts); *NovelPoster v. Javitch Canfield Grp.*, 2014 WL 3845148, at *11 (N.D. Cal. Aug. 4, 2014) (allegations that defendants wrongfully accessed the accounts at issue and, by changing passwords, prevented the plaintiff from accessing certain ones did not allege an interception of electronic communications as understood under the Wiretap Act).

In *Shefts v. Petrakis*, 2012 WL 4049484 at *6 (C.D. Ill. Sept.13, 2012), the court addressed claims under the federal Wiretap Act and the SCA by the president and CEO of a telecommunications company against the company's board of directors. As part of its investigation of harassment claims against the plaintiff, the Board: (1) had the plaintiff's work e-mail messages forwarded to a "dummy" account; (2) installed spyware on his work computer, which transmitted screen shots of his computer activity to Board members; and (3) enabled the company's Blackberry Enterprise Server to capture and store text messages from the plaintiff's personal Blackberry device, which he also used for work. The plaintiff claimed these actions violated the ECPA by enabling the defendants to intercept e-mail from his work account as well as his personal Yahoo! e-mail account, and text messages on his Blackberry.

First, the court held that the use of automatic routing software to forward the plaintiff's work e-mails to the "dummy" account was an interception under the Wiretap Act because it enabled the defendants to acquire the plaintiff's messages when he acquired them. *Id.* at *7. Second, the court found that the actions of the spyware installed on the Plaintiff's work computer, which transmitted screen shots of Plaintiff's computer activity to Board members, were interceptions under the Wiretap Act. *Id.* at *9. "Notably, any emails sent by Plaintiff on his Yahoo! account via his desktop computer would have been captured by SpectorPro *as they were transmitted* to Yahoo! via the internet." *Id.* (emphasis in original). The court also rejected the defendants' argument that the spyware did not intercept communications within the meaning of the Wiretap Act because the operation of the spyware did not affect interstate commerce. *Id.* at *8. The court held that the definition of intercept under the Wiretap Act does not require any effect on interstate commerce; rather, the communication itself must affect interstate commerce. *Id.* The court distinguished decisions finding keylogger devices do not impact interstate commerce because the transmission in question for a keylogger is only the transmission of signals from the keyboard to the computer, while the spyware captured electronic communications that affect commerce. *Id.* Finally, the court held that the Blackberry server did not intercept the plaintiff's text messages because it was scheduled to sync with the Blackberry device at certain intervals; syncing was not triggered by the receipt of a message

In *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011), the court addressed an employee's claim that her employer violated the federal Wiretap Act, the Indiana Wiretap Act and the SCA when it installed a keystroke logger on her work computer, obtained the passwords for her e-mail and checking accounts, accessed these accounts and viewed, forwarded and discussed some of the employee's e-mails. The court dismissed the federal Wiretap Act claim, holding that the keystrokes intercepted by the logger were not "electronic communications" under the Act because the systems through which the signals traveled did not affect interstate or foreign commerce. *Id.* at 1094. "Because the intercepted keystrokes were not electronic communications, they could not be 'intercepted' as that term is defined in the [Federal Wiretap Act]." *Id.* The court also held, however, that the plaintiff had stated a claim under the Indiana Wiretap Act, which is similar to the federal Wiretap Act but does not include the requirement that the transmission occur by a system affecting interstate commerce. Additionally, the court held that the employee sufficiently stated a claim under the SCA to survive the defendants' motion to dismiss. *But see Luis v. Zang*, 2013 WL 811816, at *6 (S.D. Ohio Mar. 5, 2013), *report and recommendation adopted,* 2014 WL 2804035 (S.D. Ohio June 20, 2014) (noting that keylogger software would qualify as an "interception" under the federal Wiretap Act, reasoning that "it is the communication itself that must affect commerce, not the means of interception").

b. Exceptions to the federal Wiretap Act. Although the Wiretap Act does not, by its terms or legislative history, limit its applicability to employer monitoring of employees' e-mail, the Act does contain three exceptions that often have the same practical effect. *DiLuzio*, *supra* at 746. These exceptions are: the provider exception; the ordinary course of business exception; and the consent exception. *Id.*

(1) The Provider Exception. The federal Wiretap Act specifically authorizes "an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service…" 18 U.S.C. § 2511(2)(a)(i). It is likely most private employers will be exempt from the Wiretap Act under this exception if they provide their employees with e-mail service through a company-owned system. *See* DiLuzio, *supra,* at 746. It is less clear whether the provider exception applies to employers who provide e-mail capabilities through common carriers. *Id.*

To meet the provider exception, the provider must be able to show that the interception occurred in the normal course of employment while engaged in an activity that is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service. *Schmidt v. Ameritech Ill.*, 768 N.E.2d 303, 306-08b 314-15 (Ill. App. 2002) (reversing five million dollar jury verdict awarded against the provider of telephone services who examined the telephone records of one of its employees, the employee's wife, and the wife's employer to determine whether the employee had taken a prohibited vacation while he was on disability leave; the employer's conduct was protected under the ECPA because the employer was attempting to protect its property rights by determining whether the employee took two vacations when he was only entitled to one).

(2) Ordinary Course of Business Exception. To find liability under the federal Wiretap Act, the violator must intercept the communication with an "electronic, mechanical or other device." 18 U.S.C. § 2511(1)(b). The phrase "electronic, mechanical or other device" excludes from its definition any "telephone or telegraph instrument, equipment or facility, or any component thereof," which is used by a provider of wire or electronic communication service "in the ordinary course of its business." *Id.* § 2510(5)(a). Despite the language seemingly limiting the ordinary course of business exception to a "telephone or telegraph instrument, equipment, or facility, or any component thereof," the exception has been interpreted as applying to monitoring of electronic communications. *See In re Google Inc. Privacy Policy Litigation*, 2013 WL 6248499, at *10 (N.D. Cal. Dec. 3, 2013) (concluding that, "as a provider of electronic communication services, Google is immune from claims alleging interception by a 'device' based on equipment used 'by a provider of wire and electronic communication service in the ordinary course of business'" and finding that the complaint failed to allege any interception by Google that fell outside "the scope of this broad immunity"); *but see Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014) (concluding that, to fall within the ordinary course of business exception, "there must be 'some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good'" and "[b] ased on the current record, the court cannot find any facts alleged in the complaint or facts presented by Facebook that indicate a nexus between Facebook's alleged scanning of users' private messages for advertising purposes and its ability to provide its service"). See the discussion below of the ordinary course of business exception with regard to monitoring telephone conversations.

(3) Consent Exception. The consent exception applies when one party to the communication has given prior consent to the interception or access. 18 U.S.C. § 2511(2)(d) (Wiretap Act). *See Borninski*, 2005 WL 1206872 at *13 (employee's signature on form advising employees that their Internet access should be for business purposes only, that the company logged and archived incoming and outgoing data communications through its gateway system, and that use of the gateway implied consent to such monitoring constituted express consent to the monitoring of the employee's Internet activity). Thus, not only can a properly worded disclosure establish that an employee had no reasonable expectation of privacy in his or her electronic communications or Internet usage, it can help establish consent in a claim under the federal Wiretap Act.

B. The SCA. Plaintiffs often bring claims under both the Wiretap Act and the SCA. The SCA prohibits unauthorized access to wire and electronic communications in temporary and back-up storage and further provides:

> [W]hoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701(a).

Issues that often arise in SCA cases include the definition of storage and "facilities" as those terms are used in the Act.

1. Storage under the SCA. The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17). The Department of Justice has interpreted this provision to mean a communication is in electronic storage under the SCA only if both (a) temporary and intermediate storage incident to the transmission of the communication; and (b) storage for the purposes of backup protection are met. *See Jennings v. Jennings,* 736 S.E.2d 242, 244 (S.C. 2012) (nonemployment case). However, a number of courts have held that e-mail can be in storage if it meets either (A) or (B). *Id.* at 244 (citing cases, but not deciding the issue). Additionally, many courts have held that e-mails that have been open and read by the recipient and left on the service provider's server are not in storage for the purposes of "backup protection" as used by the SCA. *See, e.g., id.* (because the e-mails in question had been opened by the recipient and left on the Yahoo! server they were not in storage for the purposes of "backup protection" under the SCA); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013) (discussed in more detail below) (holding, "in light of the restriction of 'storage' in § 2510(17)(B) solely for 'backup protection,' e-mails which the intended recipient has opened, but not deleted (and thus which remain available for later re-opening) are not being kept 'for the purposes of backup protection'"). *But see Cheng v. Romo,* 2013 WL 6814691, at *4 (D. Mass. Dec. 20, 2013) (disagreeing with *Jennings,* holding that when the defendant accessed the e-mails in question on the Yahoo! server, the text of the messages was transmitted to her own internet browser and the Yahoo! server continued to store copies of those e-mails, which the court found to be in backup storage for the purposes of the SCA).

Additionally, courts have held that e-mails stored on a computer hard drive or cell phone are not in electronic storage under the SCA. *See Rajaee v. Design Tech Homes, Ltd.*, 2014 WL 5878477, at *2 (S.D. Tex. Nov. 11, 2014) (citing *Garcia v. City of Laredo, Tex.,* 702 F.3d 788, 791 (5th Cir. 2012)) (The court granted summary judgment in favor of employer on former employee's claims that the employer violated the SCA when, after the employee's discharge, it remotely wiped his personal iPhone, which he also used in his employment. Relying on Fifth Circuit precedence, the court held "information that an individual stores to his hard drive or cell phone is not in electronic storage under the statute.").

2. Facilities under the SCA. In *Garcia v. City of Laredo,* 702 F.3d 788 (5th Cir. 2012), the Fifth Circuit rejected an employee's claim that her employer violated the SCA by accessing text messages and images stored on her personal cell phone without her permission, holding that the cell phone was not a facility with the meaning of the SCA. The plaintiff in this case was a police dispatcher who was fired as a result of text messages and images on her personal cell phone, which the employer viewed without her consent. The plaintiff claimed the employer's access of these images and text messages on her personal cell phone violated the SCA; however, the Fifth Circuit held that the SCA did not apply to this case. The court for held that for "Defendants to be liable under the SCA, they must have gained unauthorized access to a facility through which electronic communication services are provided (or the access must have exceeded the scope of authority given) and must thereby have accessed electronic communications while in storage." *Id.* at 791. The court noted that the Eleventh Circuit has held that "'the SCA clearly applies ... to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system,' but does not, however, 'appear to apply to the source's hacking into [plaintiff]'s computer to download images and identifying information stored on his hard-drive.'" *Id.* at 792 (citing *United States v. Steiger,* 318 F.3d 1039, 1049 (11th Cir.2003)). The Fifth Circuit also noted that a number of federal district courts have also concluded that the facilities the SCA is designed to protect "'are not computers that *enable* the use of an electronic communication service, but instead are facilities that are *operated by* electronic communication service providers and used to store and maintain electronic storage.'" *Id.* (citing *Freedom Banc Mortg. Servs., Inc. v. O'Harra,* 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012) (emphasis in original). The court noted that this interpretation is consistent with legislative history, as the discussion of the SCA "'deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers ...'" *Id.* at 793 (citations omitted). Thus, the court held, "An individual's personal cell phone does not *provide* an electronic communication service just because the device *enables* use of electronic communication services, and there is no evidence here that the Defendants ever obtained any information from the cellular company or network. Accordingly, the text messages and photos stored on Garcia's phone are not in 'electronic storage' as defined by the SCA and are thus outside the scope of the statute." *Id.* (emphasis in original). *See also K.F. Jacobsen & Co. v. Gaylor,* 947 F. Supp. 2d 1120, 1122 (D. Or. 2013) (employer-issued computers are not facilities through which "electronic communication services" are provided for purposes of the SCA).

3. Authorization. In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008), the court held that a former employer's actions would have been a violation of the SCA if a claim had been brought under that statute and, based on its findings, precluded the former employer from using its former employee's e-mails as evidence in a theft, breach of fiduciary duty and trademark infringement lawsuit filed against the former employee[2]. These actions included using the employee's user name and password for his personal e-mail account (which he stored on the employer's computer) to access his private e-mail accounts on three separate third-party providers. The court rejected the employer's argument that it was authorized to view these e-mails because: (a) its e-mail policy put the employee on notice that his

2 Subsequently, the defendants amended the complaint to allege a breach of the SCA, and the court granted summary judgment in their favor, finding plaintiffs accessed the e-mails in violation of the SCA. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp.2d 417 (S.D.N.Y. 2010).

e-mails could be viewed by the employer, thus he had no expectation of privacy in the e-mails; and (b) he gave implied consent for the employer to access his accounts by leaving his user name and password on the employer's computer. The court found that the employer's policy did not eliminate the employee's reasonable expectation of privacy in his personal e-mail accounts stored on third-party computer systems because the policy was limited to matters stored on, created by, received from or sent through the company's system. The court acknowledged that "[c]ourts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, where the employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored." *Id.* at 559-60 (citing *United States v. Simons,* 206 F.3d 392, 398 (4th Cir.2000); *Thygeson v. U.S. Bancorp,* 2004 WL 2066746, *21 (D. Or. Sept.15, 2004); and *Muick v. Glenayre Electronics,* 280 F.3d 741, 743 (7th Cir. 2002)). However, the court distinguished these cases because in *Pure Power* there was no evidence the employee stored the e-mail communications on the employer's computers, servers or systems, "nor were they sent from or received on the company e-mail system or computer." Instead they were "located on, and accessed from, third-party communication service provider systems." *Id.* at 560. The court also held that the employee did not give implied consent to the employer to access his personal e-mail accounts by leaving his password and user name stored on the employer's computer. The court held that "[i]mplied consent, at a minimum, requires clear notice that one's conduct may result in a search being conducted of areas which the person has been warned are subject to search." In this case, the employee only had notice that the employer's computers could be searched for evidence of personal e-mail use, not that his third party accounts could also be searched.

4. Exceptions to the SCA. The SCA, like the federal Wiretap Act, contains two exceptions that effectively limit its applicability to employer monitoring of employees' emails. *DiLuzio*, *supra* at 746.

a. The Provider Exception. The SCA exempts persons or entities providing a wire or electronic communications service from its prohibition against the unauthorized access of stored communications. In *Fraser,* 352 F.3d at 114-15, the court held that because the employee's e-mail was stored on the employer's system, which the employer administered, the employer's search of the employee's e-mail fell within the provider exception to the SCA. *See also Borninski v. Williamson*, 2005 WL 1206872 (N.D. Tex. May 17, 2005) (employer did not violate the SCA by accessing employee's e-mails that were stored on a company-issued computer hard drive because the hard drive did not qualify as "temporary or immediate storage of a wire or electronic communication incidental to the electronic transmission" not did it qualify as "storage by an electronic communication service for purposes of backup protection of such communication"). The court in *Borninski* also noted that the employer did not access Borninski's computer without authorization for the purposes of the SCA, since it provided the computer and exercised control over its network and the computers attached to the network.

b. Consent Exception. The consent exception under the SCA applies when one party to the communication has given prior consent to the access. 18 U.S.C. § 2702(b)(3). *See Borninski*, 2005 WL 1206872 at *13. As noted above, a properly worded disclosure can help establish consent in a claim under the SCA.

5. Damages Under the SCA. The SCA, 18 U.S.C. § 2707(b), provides for the award of equitable or declaratory relief, a reasonable attorneys' fee and other costs and damages under subsection (c) which include actual damages, including lost profits, but in no case less than $1,000, and punitive damages where there is a willful violation. There are differing opinions about whether actual damages are necessary before an entitlement to statutory damages. *Compare Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009) (statutory damages under the SCA are only recoverable where a plaintiff has also suffered actual damages) with *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F. Supp. 2d 417, 428 (S.D.N.Y. 2010) (defendants need not allege actual damages because Congress clearly intended that damages under

§ 2707(c) be at least $1,000 per violation), *judgment entered by Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 813 F. Supp. 2d 489 (S.D.N.Y. 2011).

C. Employees' Privacy Rights.

1. Fourth Amendment Claims. Because the Fourth Amendment's protection against unreasonable searches and seizures protects private citizens against governmental intrusions, most searches by private employers do not implicate constitutional concerns. *See Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). However, the U.S. Supreme Court's decision in a Fourth Amendment lawsuit filed against a city based on the city's review of text messages sent from the employee's city-provided pager provides guidance for private employers as well as governmental employers. In *City of Ontario v. Quon*, 560 U.S. 746 (2010), the Supreme Court held that the city of Ontario did not violate its employees' Fourth Amendment right to be free from unreasonable searches by reviewing the employees' text messages sent on pagers provided by the city. The Court did not rule on whether the employees had a privacy interest in the text messages, but instead assumed that they did and ruled on the issue of whether the city's search violated the Fourth Amendment.

In this case, the city had a policy informing employees that it reserved the right to monitor and log all network activity including e-mail and Internet use, with or without notice. *Id.* at 751. The policy further stated, "Users should have no expectation of privacy or confidentiality when using these resources." *Id.* Although the policy did not specifically mention text messages sent from city-issued pagers, the plaintiff was informed that text messages would be treated like e-mails, meaning they would be treated as public information and would be eligible for auditing. *Id.*

The city subsequently reviewed the plaintiff's text messages as part of an effort to evaluate its policy limiting text message characters. *Id.* at 752. As part of that review, the city discovered that many of the plaintiff's text messages were not work related and some were sexually explicit. *Id.* at 752-53. The situation was investigated by internal affairs, which reviewed only the messages the plaintiff sent during work hours. *Id.* at 753. The internal affairs report determined that the plaintiff sent or received 456 messages during August 2002, of which only 57 were work related. *Id.* The plaintiff was disciplined and subsequently sued the city and the police department, claiming the review of his text messages violated the Fourth Amendment. *Id.* at 753-54. The Supreme Court granted certiorari and overturned the Ninth Circuit's determination that the city violated the Fourth Amendment by reviewing the plaintiff's text messages.

The Court did not determine whether the employees had a reasonable expectation of privacy in the text messages, noting that it must "proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer." *Id.* at 759. Recognizing that a broad holding addressing employees' expectations of privacy in employer-provided technological equipment might have implications for future cases that it could not predict, the Court stated that it preferred to dispose of the case on narrower grounds. *Id.* at 760. Accordingly, the Court made several presumptions before reaching a decision: (1) the plaintiff had a reasonable expectation of privacy in text messages sent on the pagers provided to him by the city; (2) the city's review of the text messages constituted a search within the meaning of the Fourth Amendment; and (3) the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere. *Id.*

The Court held that even if the plaintiff had a reasonable expectation of privacy in the text messages, the City did not violate the Fourth Amendment by reviewing transcripts of the text messages. *Id.* Applying the standard set forth by earlier Supreme Court cases, the Court held when a search is conducted for a noninvestigatory work-related purpose or to investigate work-related misconduct, a government employer's warrantless search is reasonable if it is "justified at its inception" and if the measures adopted are "reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search." *Id.* at 761.

The Court held that the city's review of the text messages satisfied this standard. *Id.* In addition to finding the search justified and the City's methods reasonably related to the purpose of the search and not unduly intrusive, the Court noted that it was not reasonable for the plaintiff to conclude that his messages were in all circumstances immune from scrutiny. *Id.* at 762. Given that the City issued the pagers to the plaintiff and other SWAT Team members in order to help them more quickly respond to crises, and they had received no assurances of privacy, the plaintiff could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations. *Id.*

Based on this decision, an employer's search of an employee's electronic communications should be deemed reasonable where the employer can justify the search based on work-related needs and where the search is not excessively intrusive. The Court noted the importance of having clear and well-communicated electronic usage policies, which may reduce any expectation of privacy an employee may have in communications on employer-provided electronic equipment. *Id.* at 760. *But see Adkisson v. Abbott,* 2014 WL 2708424 (Tex. App. June 13, 2014) (declining to extend *Quon's* holding that a federal right to privacy exists in a governmental workplace by noting that *Quon* does not establish so broad a right to privacy that it would protect public information stored in a public official's personal e-mail account).

2. State Law Invasion of Privacy Claims. Employees may also bring invasion of privacy claims under law state based on employer monitoring of their electronic communications and activities. Some states include a right of privacy in their constitutions, while such claims are based on common law in other states. Suits based on state common law are often phrased as unreasonable intrusion upon the seclusion of another, but may also include appropriation of another's name or likeness, the public disclosure of private facts, or publicity that unreasonably places another in a false light. Depending on the state law and the specific claim, the employer may be able to defend these lawsuits by showing that the information contained in an e-mail or other electronic communications is not private or that the employee had no reasonable expectation of privacy. Having employees acknowledge in writing that they understand their electronic communications will be monitored by the employer helps establish that the employee had no reasonable expectation of privacy. *See, e.g., Thygeson v. U.S. Bancorp,* 2004 WL 2066746 (D. Or. Sept. 15, 2004) (unpublished decision) (employee had no reasonable expectation of privacy in e-mails sent and received on the employer's e-mail system, some of which were saved in personal folders on the employer's computer network. The employer's policy stated that the company's computers, including e-mail, were intended for business purposes only and that the employer reserved the right to monitor employee's e-mails and computer files, which nullified any expectation of privacy the employee might have in his e-mail or in the addresses of the web sites he visited using the employer's Internet access); *Garrity v. John Hancock Mut. Life Ins. Co*., 2002 WL 974676 at *2 (D. Mass. May 7, 2002) (The use of password-protection and personal folders on the company intranet system to save e-mails sent using an office e-mail system, including sexually explicit e-mails from Internet joke sites, were insufficient to create a reasonable expectation of privacy). (unpublished decision); *Kelleher v. City of Reading,* 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (unpublished decision) (plaintiff had no reasonable expectation of privacy in e-mail on the employer's e-mail system, where the employer's policy specifically stated that e-mails created or sent using the employer's e-mail system were the property of the employer, the employer reserved the right to access and disclose the contents of e-mails, and the e-mail system was strictly for official use).

However, at least one court has held that "[a]bsent clear knowledge of the extent of what could be searched, and the opportunity to refuse or withdraw his consent," implied consent has not been given. *See Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp 2d 548, 562 (S.D.N.Y. 2008). Additionally, many courts will conduct a balancing test to weigh the employer's need to monitor employee computer use against the employee's expectation of privacy. *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100-01 (E.D. Pa. 1996) (employee who was fired for making threatening comments about management over the company's e-mail system had no reasonable expectation of privacy in the e-mail messages, even though the employer repeatedly reassured employees that management would not intercept such communications).

3. Importance of Employer Policies. As noted above, employers can reduce employees' expectation of privacy in their computer use by implementing clear e-mail and Internet usage policies. Additionally, employees should be required to acknowledge that they have received the policy and agree to abide by it. The policy should be included in the employee handbook and should be redistributed on a regular basis. Employers may also consider having the policy appear on the computer whenever e-mail is accessed. Employers should take care to ensure they do not act inconsistent with their policies, as this could give rise to an employee having an expectation of privacy in their computer use. Policies must be tailored for the employer's specific business, but the following issues should be addressed in most policies:

- All computers, telephones, and other electronic equipment are the property of the organization.
- The organization reserves the right to monitor or access all employee Internet, e-mail, computer, voicemail, and telephone usage for any business-related purpose.
- The organization will maintain copies of Internet, e-mail, and voicemail passwords, and the existence of such passwords is not in any way an assurance of the confidentiality of the communications.
- The transmission of any discriminatory or harassing messages via e-mail, voicemail, or the Internet is prohibited and will be considered a violation of the organization's equal employment opportunity policy.
- Instructions as to when, if at all, e-mail, the Internet, and telephones may be accessed for personal use should be provided.
- Any violation of the electronic communications or technology use policy may result in disciplinary action, up to and including termination.
- Further, the scope of the electronic communications or technology use policies should be tailored to include the various types of equipment used by the employer and provide notice of the methods by which the employer may monitor employees.
- Before adopting a policy requiring employer e-mail be used for business purposes only, consider consulting experienced labor counsel, as the National Labor Relation Board (NLRB) has held that "employee use of email for statutorily protected communications on nonworking time must presumptively be permitted by employers who have chosen to give employees access to their email systems." *Purple Communications, Inc.*, 361 NLRB No. 126 (2014) (overturning *Register Guard*, 351 NLRB 1110 (2007), *enf'd in part*, *Guard Publishing v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009), which had held that employees have no statutory right to use their employers' e-mail system for Section 7 purposes[3]). For a further discussion of this issue, please see the *NLRA's Impact on the Workplace* and *Coping with Unions* SourceBook chapters.

D. State Laws Restricting Employer Access to Employees' Social Media. At least 21 states now restrict an employer's access to employees' personal social media (in 2015, Connecticut, Montana, Virginia, and Oregon's legislatures enacted such legislation, and legislation is pending in several other states). These states' laws generally prohibit employers from requiring or requesting that a current or prospective employee disclose a username or password to his or her personal online account or access a personal online account in the presence of the employer. Further, employers may not take adverse action against a current employee who refuses to engage in these activities or

3 Section 7 of the National Labor Relations Act (NLRA or the Act) gives employees the right to form, join or assist unions and to engage in other concerted activities for mutual aid and protection. Section 7 protects activities on behalf of a group of employees that could include criticism of a company's policies and procedures or its management, or other terms and conditions of employment.

refuse to hire a prospective employee because he or she refuses to engage in such activities. These laws generally do not restrict the employer's ability to monitor data that is stored on a computer or phone provided to the employee by the employer for business use.

E. Monitoring Telephone Conversations. The federal Wiretap Act, as amended by the ECPA, restricts monitoring and recording of employee telephone calls or other conversations. Additionally, almost every state has enacted legislation that regulates telephone monitoring or recording of conversations.

The Wiretap Act prohibits employers from intentionally intercepting an employee's telephone or electronic communications. *See Anderson v. City of Columbus,* 374 F. Supp. 2d 1240, 1242-43, 1247 (M.D. Ga. 2005) (finding issue of fact regarding whether an individual supervisor intentionally intercepted the plaintiff's telephone conversations where the supervisor knew of a glitch in the recording system when headphones were used and failed to tell the plaintiff how to prevent the recording). The Act also prohibits an employer from using or disclosing the intercepted communications. Criminal penalties may be imposed, and aggrieved employees may bring civil action. *See McCann v. Iroquois Mem. Hosp.,* 622 F.3d 745, 752-53 (7th Cir. 2010) (Federal Wiretap Act requires intentional interception, finding issue of fact regarding whether conversation was intentionally intercepted; also finding no evidence that hospital CEO and trustees knew conversation was recorded illegally).

1. **Exemptions Under the Wiretap Act.**

   a. One Party Consent. The Wiretap Act allows an employer to intercept and use a communication when interception is consented to by at least one of the parties, unless the communication is intercepted for the purpose of committing a crime or tortious act. A party to a communication is one who actually participates in the communication even if that person may not have been the intended recipient of the call. *See, e.g., United States v. Campagnuolo*, 592 F.2d 852, 862 (5th Cir. 1979).

   b. Telephone Extension Exception. An employer can use this exception where: (1) the intercepting equipment was furnished to the user by the phone company or connected to the phone line; and (2) it was used in the ordinary course of business. *Hay v. Burns Cascade Co.*, 2009 WL 414117, at *12 (N.D.N.Y. Feb. 18, 2009). The "extension" exception allows employers to monitor calls in the ordinary course of business, i.e., when all calls are monitored. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (a personal call may not be intercepted in the ordinary course of business "except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal not"; "a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents"). *But see Burrow v. Sybaris Clubs Int'l, Inc.*, 2013 WL 5967333, at *2 (N.D. Ill. Nov. 8, 2013) (business extension exception did not apply because the recording system did not further the use of the telephone, as (1) system did not record the conversations on the telephone but instead was linked to computer servers and archived the recordings in a system separate from the telephone itself; (2) the recordings were available on a web interface that management and employees could freely access).

   Some courts have held that this exception requires notice to the employees that telephone calls are being monitored. *See Anderson v. City of Columbus*, 374 F. Supp. 2d 1240, 1521 (M.D. Ga. 2005) (telephone extension exception does not mean that in the ordinary course of business an employer may surreptitiously intercept everything an employee says while wearing a headset at his or her desk); *but see Arias v. Mutual Cent. Alarm Serv.*, 202 F.3d 553, 559 (2d Cir. 2000) (An alarm company that monitored all telephone calls coming in and going out of its central station 24 hours a day did not violate the Act, even though the employees were told their telephone conversations were not being recorded when they were. The court held that the 24-hour recording was within the ordinary scope of business and that employee consent was not required.).

2. Oral Communications. The Wiretap Act prohibits the use of listening devices to intercept spoken communications "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2). This incorporates the reasonable expectation of privacy law developed under the Fourth Amendment. The same exception for one-party consent applies to oral communications. *See Pitts Sales, Inc. v. King World Products*, 383 F. Supp. 2d 1354, 1360-61 (S.D. Fla. 2005) (individual who videotaped and recorded conversations that occurred in his presence but in which he did not participate was, nevertheless, a party to the communications for the purposes of the one party consent exception), *findings of fact, conclusions of law at* 2005 WL 4038673 (S.D. Fla. July 29, 2005). In addition to the Wiretap Act, certain states prohibit audio recordings in certain areas, such as restrooms or locker rooms. *See, e.g.*, Cal. Lab. Code § 435. Employers should review state law regarding audio recordings.

3. Penalties. The Wiretap Act provides for criminal prosecution with up to five years in prison and fines up to $250,000 for individuals and $500,000 for organizations. The Wiretap Act also authorizes civil actions for actual damages with a statutory minimum, punitive damages, and attorney fees.

F. Video Monitoring of Employees. Some state statutes restrict camera surveillance of employees. In a state with no such statute, however, the employer can defend the use of cameras as an extension of management authority to observe employees. The following guidelines are relevant to camera surveillance: (1) the cameras should be visible, if this will not jeopardize the investigation; (2) employers should give employees written notice of camera surveillance; and (3) avoid or narrowly restrict the use of cameras in restrooms or other areas that might raise privacy concerns. Limit camera angles to avoid needless problems and control access to the tapes. Finally, if the cameras record voices as well as pictures, the employer must comply with state and federal statutes and regulations applicable to the interception of verbal communications. *See La Porte v. State*, 512 So. 2d 984, 986 (Fla. 2d DCA 1987) (affirming the conviction of an operator of a modeling business for video recording modeling clients without their knowledge). Following these guidelines should reduce the likelihood of invasion of privacy claims.

G. Employee Tracking Devices. Advances in technology have increased the ways an employer can monitor its employees, which can serve valid, business related purposes. For example, using GPS devices on company vehicle can enable the employer to track the location of employees during the day and ensure the safety of the vehicles. Smart identification and clothing technology can enable employers to monitor employee location in the workplace. This can enable hospitals, for example, to determine how long an employee stays in a patient's room. Infrared technology on bathroom sinks can enable employer to monitor how long health care and food service workers spend washing their hands. The use of this technology, however, may also open the door for new types of invasion of privacy claims. *See* Rachel Emma Silverman, *Tracking Sensors Invade the Workplace*, The Wall Street Journal (March 7, 2013), *available at* http://www.wsj.com/articles/SB10001424127887324034804578344303429080678.

For example, in *U.S. v. Jones*, 132 S. Ct. 945 (2012), the U.S. Supreme Court held that the government's actions in installing a GPS device on a criminal suspect's vehicle and using that device to monitor the vehicle's movements constituted a search within the context of the Fourth Amendment. While *Jones* is a criminal case, and the Fourth Amendment is not applicable to private (nongovernmental employers), the language in the decision, especially in Justice Sotomayor's concurrence, reflects concern for the potential impact on an individual's privacy presented by the use of GPS devices:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations … I would take these attributes of GPS monitoring into account when considering the existence of a reasonable

> societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on … More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. … This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

Id. at 955-957 (citations omitted). Justice Sotomayor's reference to the reasonable expectation of privacy may be especially relevant in invasion of privacy claims against nongovernmental employers based on the use of GPS or other types of tracking technology. While employees generally are not viewed as having a reasonable expectation of privacy in an employer-owned vehicle, it is a good idea to have a written policy informing employees of the use of GPS technology on company vehicles for business purposes. Employees should acknowledge in writing that they have received and read the policy and consent to the employer's use of GPS technology. Employers should also ensure that data obtained from tracking devices is kept secure and treated as confidential, to help minimize the risk of an invasion of privacy claim.

Although employers may be able to justify the use of GPS technology for business-related purposes, an invasion of privacy claim may be much more likely if the employer monitors an employee during nonworking hours. In *Cunningham v. New York State Dept. of Labor*, 997 N.E.2d 468, 471(N.Y. 2013), the high court for the state of New York held that a government employer was not required to obtain a warrant prior attaching a GPS device on an employee's private vehicle without his knowledge, as part of an investigation of the employee's suspected misconduct (pursuant to the workplace exception to the warrant requirement under both the U.S. and New York state constitution). However, because the employer monitored the employee's off-duty hours as well as his working time, the court held that the search was not reasonable in scope. *Id.* at 473. Accordingly, the employer was prohibited from using any evidence obtained from the GPS tracking in the employee's discharge hearing. *Id.* at 473-74. Employers should consider utilizing applications that automatically disable the tracking of an employee when that employee is off the clock.

Employers should be aware of the laws of the states in which they have operations, because some states have enacted laws regulating or prohibiting the use of electronic tracking devices. For example, California's penal code prohibits using "an electronic tracking device to determine the location or movement of a person," but does provide an exception where the "registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle." Cal. Penal Code § 637.7. Similarly, Texas law prohibits the placement of "electronic or mechanical tracking devices" on the vehicles of other individuals without consent. Tex. Penal Code Ann. § 16.06. Connecticut law requires employers to provide notice to employees before conducting any kind of electronic monitoring. *See* Conn. Gen. Stat. Ann. § 31-48d; *Gerardi v. City of Bridgeport*, 985 A.2d 328, 334 (Conn. 2010) (The statute did not provide a private right of action for fire inspectors who sued the city after it installed GPS devices in city-owned vehicles to track the movements of the fire inspectors. The court held, "we conclude that the legislature intended the enforcement mechanism of § 31–48d to be limited to proceedings before the labor commissioner, and not to allow employees to bring civil actions."). Delaware law also prohibits installing a tracking device on a motor vehicle without the owner's consent. *See* 11 Del. Code Ann. § 1335. State privacy laws changes frequently, so employers should ensure they are in compliance with the laws of the states in which they have operations.

In addition to monitoring developments in state and federal law regarding tracking devices, employers should take the following steps:

- Ensure that the use of the employee tracking device is justified by a legitimate business need, such as the need to monitor the use of an employer's resources, security and safety concerns, etc.

- Ensure that the tracking device policy clearly sets forth the purpose of the company's use of tracking technology, the manner in which the employer monitors its employees, when employees may disable the tracking technology, when employees should expect to be monitored, and other logistics related to the tracking technology. The policy should also set forth any discipline related to an employee disabling the tracking technology.
- Ensure that the policy has been communicated to all employees and that employees have consented to the use of the tracking technology.

V. BYOD PROGRAMS

More and more employers are permitting their employees to BYOD to work, a trend that is likely to continue to gain in popularity. According to a Samsung survey, 61 percent of all companies currently have some form of BYOD policy in place, while only 15 percent of companies explicitly prohibit the use of personal mobile devices. *See* http://www.samsung.com/us/pdf/byod/2013_BYOD_Index_20130103c.pdf. Further, a global survey of CIOs by Gartner, Inc.'s Executive Programs, shows that 38 percent of companies expect to stop providing devices to workers by 2016. *See Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes*, May 1, 2013, http://www.gartner.com/newsroom/id/2466615. Additionally, even employers who have not adopted BYOD policies may find that their employees use personal devices for business.

BYOD policies have many benefits, including increased productivity, increased employee satisfaction, flexibility, the ability to adopt cutting-edge technology, increased innovation and potentially decreased hardware costs (although some employers may find that the cost of supporting multiple platforms on different devices offsets any cost savings). There are downsides as well including data security issues – compliance with state and federal laws protecting employee and customer PII can be much more difficult when employees can access, transmit or store this information on their personal electronic devices. The use of personal electronic devices can also make it more difficult to protect proprietary or confidential business information and to comply with e-discovery requirements during litigation. Additionally, the use of personal mobile devices can create employment-law related issues such as minimum wage and overtime concerns, discrimination, harassment, and safety issues. Finally, employees may have privacy concerns over employer e-mail monitoring and the use of tracking devices or location services on mobile devices. Developing and maintaining effective BYOD policies can be an on-going challenge for employers, requiring coordination with human resources, IT specialists, and department managers (as well as collective bargaining representatives if the company is unionized).

A. Data Security Issues. Security issues arising from the use of personal devices at work may arise in a variety of ways, including lost or stolen devices, malware, hacking, the use of insecure cloud accounts to store sensitive data, the use of insecure mobile apps, transmitting information through the use of insecure WiFi, Bluetooth or peer-to-peer networks, and sharing devices with friends and family. Employers can take basic security steps to help protect against the loss of confidential and proprietary information as well as PII, including:

- require password-protection on all employee devices;
- require employees agree to secure the devices with the most current technology and install any available security updates;
- encrypt sensitive data;
- restrict the type of data that can be accessed by personal devices;
- restrict which employees can use personal devices for work;
- require immediate notification if the device is lost or stolen;

- require installation of remote-wipe technology so that sensitive data can be wiped from a lost or stolen device (obtain written authorization from the employee, as discussed below);
- prohibit employees from:
    - jail-breaking devices;
    - installing applications from unapproved sources;
    - connecting to unknown wireless networks;
    - transmitting company data via public or unsecured WiFi networks;
- develop procedures for responding to data loss or breach (see the discussion of breach notification laws, above); and
- consider requiring the use of technology that permits compartmentalizing or "sandboxing" company data from personal data. *See Bring Your Own Device, Security Risk Considerations for your Mobile Device Program,* EY, September 2013, http://www.ey.com/Publication/vwLUAssets/EY - Bring your own device: mobile sec urity and risk/$FILE/Bring your own device.pdf.

1. Encryption. Encrypting sensitive data can help reduce the risk of loss or disclosure of sensitive information in the event of a security breach. Many state data breach notification laws provide a "safe harbor" for encrypted information. See the discussion of state data breach notification laws above. Additionally, some state laws, such as Massachusetts' information security regulations, specifically require encryption of personal information stored on portable devices.

2. Remote Wiping. Employers may also want to consider requiring the installation of technology that permits remote locking or remote wiping of devices. According to a 2013 survey conducted by data protection firm Acronis, 21 percent of all companies perform remote wiping of devices. *See* Chris Smith, Jan. 22, 2014, http://bgr.com/2014/01/22/byod-remote-wipe/. Mobile Device Management (MDM) software suites can enable employers to manage the entire mobile device, including the ability to remote lock and remote wipe. *See* Ken Hess, *5 Mobile Device Management Features that Matter,* June 5, 2014, http://www.tomsitpro.com/articles/mdm-solutions-comparison,2-745.html. Employees should be notified of the requirement that such technologies be used and should provide written consent to their use. Failure to do so could result in claims against the employer under state computer-trespass statutes, originally designed to prosecute hackers. Additionally, the use of remote wiping, blocking or bricking technologies could damage the employee's device and/or data stored on the device. For example, remotely wiping a device to remove sensitive company data could wipe out the employee's personal information, including e-mails, photographs, videos, books, documents, and software. Employers should explain these risks to the employee and obtain a written waiver consenting to these activities and holding the employer harmless for any such damage or loss.

Obtaining such consent/waivers, as well as developing and promulgating a BYOD policy that reiterates the risks of using personal devices at work, can help defend lawsuits based on remote wiping of a personal device or otherwise accessing the personal device. Employees may bring such lawsuits under the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, the SCA, or various state laws.

The CFAA generally prohibits accessing a protected computer without authorization or in excess of authorization, but requires a showing of at least $5,000 in losses due to the cost of investigating and responding to a violation or as a result of a service interruption. As discussed above, the SCA is part of the ECPA and prohibits the unauthorized access to stored electronic communications and records.

A federal district court in Texas recently granted summary judgment to an employer on a former employee's CFAA, SCA, and state law claims based on the employer's remote wiping of the plaintiff's personal iPhone after his discharge. In *Rajaee v. Design Tech Homes, Ltd.*, 2014 WL 5878477, at *1 (S.D. Tex. Nov. 11, 2014), a sales and marketing employee used his personal iPhone to connect to the employer's Microsoft Exchange Server, enabling him to remotely contact the e-mail, contact manager and calendar provided by the employer. When the employee gave two weeks' notice of his intent to resign, the employer immediately discharged him and, a few days later, remotely wiped his iPhone. The remote wipe restored the iPhone to factory settings, deleting all personal and work related data. The employee sued under the CFAA, SCA, and various state laws, claiming the employer's actions caused him to lose more than "600 business contacts collected during the course of his career, family contacts (many of which are located overseas and some are related to family business), family photos, business records, irreplaceable business and personal photos and videos and numerous passwords." *Id.* at *1. The court granted summary judgment in favor of the employer on the SCA claim, relying on Fifth Circuit precedence holding that "information that an individual stores to his hard drive or cell phone is not in electronic storage under the statute." *Id.* at *2 (citing *Garcia v. City of Laredo,Tex.,* 702 F.3d 788, 791 (5th Cir.2012)). The court also granted summary judgment on the CFAA claim, holding that the plaintiff failed to show he sustained $5,000 in cognizable loss under the CFAA. Although the court ruled in favor of the employer in this case, a signed consent/waiver addressing remote wiping technology would have made defending the lawsuit much easier.

The CFAA is discussed in more detail in the *Employer Challenges and Potential Liability in the Electronic Workplace* Chapter of the SourceBook.

B. E-Discovery Issues. The Federal Rules of Civil Procedure require employers to preserve and produce documents and electronically stored information (ESI) which are in their possession, custody or control. *See* Fed. R. Civ. P. 34. While case law makes it clear that employers have an obligation to preserve and produce relevant ESI stored on mobile devices, employers may have difficulty identifying, preserving and collecting information stored on employees' personal devices. Additionally, the examination of personal devices may lead to the discovery of employees' personal data, and personal data may be inadvertently transmitted to an e-discovery vendor that lacks sufficient security protections. This may lead to invasion of privacy claims by employees whose personal information has been accessed.

Another issue that arises under BYOD policies is whether an employer has control over information stored on an employee's personally-owned mobile device. The federal rules do not define control, and the definitions of that term can vary by court. Some courts have required employers to have actual possession or control while others require either actual control or the legal right to obtain production of documents on demand. At least one court has found that an employer did not have control over information on an employee's personal cell phone which was not used for work related purposes. *See Cotton v. Costco Wholesale Corp.*, 2013 WL 3819974, at *6 (D. Kan. July 24, 2013). In *Cotton,* the court denied the plaintiff's motion to compel the production of text messages from employees' personal cell phones that mentioned the plaintiff or his discrimination claim. The court noted, "documents are deemed to be within the possession, custody, or control if the party has actual possession, custody, or control or has the legal right to obtain the documents on demand." *Id.* at *6 & n.19 (citing *Noaimi v. Zaid,* 283 F.R.D. 639, 641 (D. Kan. 2012)). In *Cotton,* there was no contention that the employer provided the cell phones to the employees, that they used the cell phones for any work-related purpose, or that the employer otherwise had any legal right to obtain employee text messages on demand. Accordingly, the court denied the plaintiff's motion to compel, since "it appear[ed] to the court that Costco does not likely have within its possession, custody, or control text messages sent or received by these individuals on their personal cell phones." *Id.* at *6.

In *Ewald v. Royal Norwegian Embassy*, 2013 WL 6094600, at *10 (D. Minn. Nov. 20, 2013), the court held that the plaintiff was entitled to discovery of text and voice messages on cell phones provided by the employer to the plaintiff and another individual. However, the court denied the motion to compel production of personal mobile devices belonging to witnesses because the plaintiff failed to demonstrate her entitlement to such devices. Courts may be more likely to compel the production of work-related documents stored on employees' personal devices where those devices are used for work-related purposes pursuant to a BYOD policy.

C. Employee Privacy Issues. Employee privacy issues can arise in a number of ways when employers implement BYOD policies. In addition to the risk of employers accessing personal information stored on personal devices used in a BYOD program or monitoring employees' electronic communications, GPS technology on personal devices such as cell phones can create concerns of employer tracking.

1. Fourth Amendment Issues. As noted above, private employers are not subject to the requirements of the Fourth Amendment, which protects citizens from unreasonable searches and seizures by the government. The Supreme Court's decision in *City of Ontario v. Quon*, 560 U.S. 746 (2010), discussed in § III(A)(2)(a) above, provides guidance to private employers regarding searches of employee text messages on employer-provided devices, emphasizing the importance of clear and well-communicated electronic usage policies. However, the Court specifically did not rule on whether the employees had a privacy interest in the text messages, noting that it must "proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer." *Id.* at 759.

More recently, the U.S. Supreme Court addressed the issue of criminal defendants' privacy interest in data stored on their personal cell phones. *See Riley v. California,* 134 S. Ct. 2473 (2014). Subsequently, a federal court referenced *Riley* in addressing employee privacy issues raised by discovery requests to review a defendant's cell phone in a civil case. In *Bakhit v. Safety Marking, Inc.,* 2014 WL 2916490, at *2-3 (D. Conn. June 26, 2014), the court denied the plaintiffs' request to inspect and image the mobile devices of individual defendants in a discrimination lawsuit. In denying the request, the court held that it was "overly broad and too intrusive for this stage of discovery," noting that the plaintiffs failed to demonstrate they were unable to obtain similar information through other discovery methods. *Id.* at *2. The court also held that the discovery request raised privacy concerns, especially for two of the individual defendants not shown to be connected to the alleged cell phone misconduct. In addressing the individual defendants' privacy interest in the data stored on their cell phones, the court quoted *Riley*:

> As Chief Justice Roberts, writing for the Court noted, the modern cell phone's immense storage capacity, "has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second a cell phone's capacity allows even just one type of information to convey far more than previously possible." *Id.* at 18.The Supreme Court further recognized that, "[a]lthough the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different." *Id.* at 19. In this regard, the Supreme Court points to an internet search and browsing history that may reveal an individual's private interests and concerns, such as "symptoms of disease, coupled with frequent visits to WebMD." *Id.* Indeed, this is precisely the information that may be implicated by plaintiffs' search of the individual defendants' cell phones and with what the Court takes issue.

Bakhit, 2014 WL 2916490 at *3. Although *Riley* is a criminal case, if other courts extend its analysis of the privacy of cell phone data to the civil context, it could have an impact on BYOD policies.

D. Monitoring Employees. As discussed in § III above, employees may file lawsuits against employers under the federal Wiretap Act, the SCA, or state law based on the employer's actions in monitoring an employee's electronic communications or activities or tracking an employee's location. While employees frequently are found to have no reasonable expectation of privacy in employer-owned equipment or vehicles, the analysis may be different when BYOD policies are involved. Employees may be viewed as having a greater expectation of privacy with regard to communication and activity conducted on personally-owned device. Additionally, dual-use devices, even when issued by the employer, may provide access to an employee's personal accounts or information, which may create another avenue of potential liability for employers. Furthermore, employers must take additional precautions to ensure location tracking services on personal devices are not used to monitor employees during non-working hours.

1. Federal Wiretap Act. In *Sunbelt Rentals, Inc. v. Victor*, 2014 WL 4274313, at *2 (N.D. Cal. Aug. 28, 2014), the plaintiff claimed his former employer violated the federal Wiretap Act and the SCA as well as various state laws by reviewing his text messages on the iPhone the employer issued to him while he was still employer. The text messages were available on the iPhone, which he returned to the employer when he left to work for a competitor, because he failed to unlink the phone from his personal Apple account and subsequently linked his new phone, provided by the new employer, to the same personal account. Because the old phone number was linked to the account, the text messages sent and received from the new phone were available on his old phone, now in his former employer's possession. The plaintiff claimed that his former employer violated the federal Wiretap Act and the SCA by reviewing the electronic communications, including text messages that were available on his old devices.

The court dismissed the federal Wiretap Act claim (with leave to amend) because the plaintiff failed to show Sunbelt intentionally intercepted his text messages. The court held, "the text messages appeared on his Sunbelt iPhone as a result of Victor's act of syncing his new iPhone to his Apple account without first un-linking his Sunbelt iPhone. … Sunbelt did not intentionally capture or redirect Victor's text messages to the Sunbelt iPhone—the transmission of those messages was entirely Victor's doing." *Id.* At *2. Further, the court held that the plaintiff failed to show Sunbelt intercepted any communications, noting that the pleadings suggested they were read after they were sent and received on the Sunbelt iPhone, which is insufficient to establish interception under the Wiretap Act. *Id.* at *3. Noting the "almost instantaneous transmission of text messages," the court found it doubtful the plaintiff would be able to state a claim of interception under the Wiretap Act, but nevertheless dismissed the claim with leave to amend. *Id.* The court dismissed the plaintiff's SCA claims because he did not allege that Sunbelt accessed his text messages through his cellular provider or Apple's network, and accessing them on his old phone did not violate the SCA. *Id.*

2. The SCA. In *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 752 (N.D. Ohio 2013), the plaintiff sued her former employer and supervisor under the SCA, Title III, and state law, claiming her former supervisor used her company-issued Blackberry, which she returned when she left employment, to read 48,000 e-mails in her personal g-mail account. The plaintiff claimed she inadvertently failed to delete her personal g-mail account from her Blackberry when she returned it and, instead of deleting the account, the supervisor used it to access and read her personal e-mails. The court held that the plaintiff stated a claim under the SCA, rejecting the defendants' arguments that the act only applies to "computer hackers," not someone who reads another's e-mail without his or her knowledge. *Id.* 754. The court also rejected the former supervisor's claim that he was authorized to access the e-mails because they were on a company-issued device, which he had authority to access. The defendants argued that the company-owned Blackberry was a facility as used in the SCA, which prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided." *Id.* at 755. The court rejected this argument, holding, "the "electronic communications service" resided in the g-mail server, not on the blackberry, and the g-mail server, not the blackberry, was the "facility." *Id.* at 756. *See also Garcia v. City of Laredo, Tex.,* 702 F.3d 788, 793 (5th Cir. 2012) (An individual's personal cell phone does not provide an electronic communication service just because the device enables use of electronic communication services).

The court also held that the plaintiff did not impliedly consent to the supervisor's reading of her private e-mail by failing to ensure the g-mail account was deleted from the Blackberry before she returned it. "Negligence is, however, not the same as approval, much less authorization. There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone be stopping by." *Id.* at 757. The court also held, however that the plaintiff could only state a claim under the SCA with regard to e-mails that the supervisor accessed that she had not opened. The SCA defines electronic storage as: (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." The court noted that several courts have found that only e-mail awaiting opening by the intended recipient falls within the SCA's definition of "electronic storage." The court held that e-mails the plaintiff had opened but not deleted were not in backup status or electronic storage as those terms are used by the SCA. Accordingly, the plaintiff could not recover for the supervisor's access of those e-mails, only for the e-mails he accessed before the plaintiff opened them.

E. Employment Law Issues.

1. Wage and Hour Issues. While employers may view BYOD policies as boosting productivity, permitting non-exempt employees to use mobile devices (whether personal or company-provided) for work can create "off-the clock" issues if employees claim they were not paid for time spent working outside their normal work hours. To help avoid such issues, employers should define working hours and limit the availability of non-exempt workers during off-hours. Employers may want to consider implementing procedures to track time outside of the office if necessary and develop polices to enable employees to easily track and record time spent working on mobile devices. Additionally, employers should train both managers and employees and make clear that time spent on personal devices responding to e-mails or text messages and answering telephone calls is working time and must be compensated.

2. Distracted Driving. Employers may face liability for an employee who harms someone because of his or her negligent use of a phone while driving, even if the employee owns the device. To help avoid such liability, employer policies should prohibit texting while driving.

3. Reimbursement of Employee Expenses. Employer policies should clarify whether the employer or the employee is responsible for expenses related to mobile devices used for work, including the cost of the device, data plans, etc. A California Court of Appeal has held that if employees are required to use their personal cell phones as a part of their job duties, their employer must pay a reasonable percentage of their cell phone bill, regardless of the type of plan they are on or whether they are the ones paying the bill. *See Cochran v. Schwan's Home Service,* 228 Cal.App.4th 1137 (Cal. App. 2014). In *Cochran,* the court held that employees are only required to show that they were required to use their personal cell phone for work-related calls to be entitled to reimbursement under California Labor Code § 2802. In reaching this conclusion, the appeal court held that it does not matter whether the phone bill is paid by a third person or not paid at all. Section 2802 requires an employer to reimburse employees for expenditures or losses incurred in the discharge of their duties or in the obedience of the employer's directions. The court held that this statute requires the employer to reimburse the employee for mandatory work related calls made on a personal device regardless of whether the charges were paid by a third person or whether the employee subscribed to a flat rate plan so that the calls did not create an extra expense on the employee's cell phone bill. According to the court, "[o]therwise, the employer would receive a windfall because it would be passing its operating expenses onto the employee." Consequently, to establish liability under Section 2802, employees only have to show that they were required to use their personal cell phone for work-related calls to be entitled to reimbursement. Other state laws may also require employers to compensate employees for work related expenses, which could include expenses related to personally owned electronic devices used pursuant to BYOD policies. Additionally, the FLSA prohibits requiring non-exempt employees to pay for business expenses of the employer of doing so would cause the employee's pay to fall below the required minimum wage or if it would deprive the employee of appropriate overtime compensation.

4. Theft of Trade Secrets and/or Proprietary/Confidential Information. Another issue presented by permitting employees to BYOD to work is the risk of theft of trade secrets or proprietary information. Employer policies should expressly prohibit the acquisition of confidential data through personal devices such as wearable technology and should prohibit storage of highly sensitive data on personal devices. Policies should also clearly identify information considered confidential or proprietary, including price lists, customer lists, financial information, etc. Any information considered confidential or proprietary should be clearly labeled as such and the distribution should be limited. Consider prohibiting the use of wearable technology and/or personal electronic devices in departments that handle information that is a trade secret or proprietary/confidential. Employers may also want to consider requiring employees to enter into confidentiality agreements and/or restrictive covenants to further protect confidential or proprietary information. The enforceability of such agreements is determined by state law, so employers should consult the laws of the states in which they have facilities to ensure confidentiality agreements comply with applicable laws. For example, restrictive covenants are generally unenforceable under California law. For a more detailed discussion of trade secrets and confidentiality agreements, please see the *Employee Contracts and Noncompete Agreements* SourceBook chapter.

F. BYOD Policy Suggestions.

1. Reassess current policies on relevant issues such as information security, acceptable use of technology, confidentiality and privacy, employment, and harassment and ensure that BYOD policies are consistent with other policies. Cross-reference the policies where appropriate.

2. Determine which employees will be permitted to use personal devices for work and which data will be accessible by personal devices. Employees handling confidential information such as those in research and development or employees handling employee medical information such as those in human resources may not be appropriate candidates for a BYOD policy.

3. Clearly delineate users' rights and obligations, differentiating between business and personal use.

4. Employees should acknowledge and agree in writing that they do not have any rights in company data, and that the employer has the right to access the data on their personal devices, monitor the use of those devices, and retain possession of those devices as needed.

5. Require employees to acknowledge and agree that all of the data on their devices will be erased when the employee stops working for the company. Additionally, if remote wiping technology will be used, explain the circumstances in which such technology may be used, such as where the device is lost or stolen, and the potential consequences. Have employees acknowledge they understand these risks and consent to the use of such technology.

6. Address which parties are responsible for costs related to the use of personal devices, including costs related to lost or stolen devices, taking into consideration the relevant federal and state laws.

7. Consider prohibiting employees from sharing devices with family members, friends, etc.

8. Require security features on personal devices, including passwords, encryption of data, etc. Prohibit transmission of company data over non-secure WiFi networks.

9. Ensure compliance with relevant state and federal data security laws.

10. Set forth how policy violations are handled.

11. Consider implementing geofencing technology that restricts access to devices or applications while inside the company's perimeter, as well as makes it impossible for devices outside the perimeter to access the network.