LJN LAW JOURNAL NEWSLETTERS

THE PRIVACY & DATA PROTECTION LEGAL REPORTER™

Volume 1, Number 4 • May 2006

ALM

What Every U.S. Employer Should Know About Workplace Privacy

Part One of a Two-Part Series

By Lisa J. Sotto and Elisabeth M. McCarthy

The U.S. privacy arena is a minefield for employers. The United States has no omnibus employee privacy law. Instead, employers are faced with a patchwork of privacy laws that they must piece together to avoid legal liability. This article focuses on the key privacy issues employers in the U.S. must confront.

Background Screening

According to a January 2004 survey by the Society for Human Resource Management, 82% of employers investigate the backgrounds of potential employees. Employers conduct background checks on job applicants not only to verify the candidates' credentials, but also to ensure workplace safety and avoid potentially devastating financial and reputational harms associated with negligent hiring, retention, and supervision claims. It is significantly less costly to conduct a thorough background check on a job applicant than to hire an employee with a history of violence, sexual harassment, or embezzlement. Conducting appropriate background checks has reached a new imperative since 9/11. This has been further fueled by the corporate scandals of 2002 involving companies such as Enron and WorldCom.

Employers typically ask consumer reporting agencies to assemble and evaluate information about a job applicant's professional and personal life. Certain jobs, such as those in the banking, childcare, health care, airline, and trucking industries require criminal background checks.

Many sources of information used in background checks are public records, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation, and driving records. The Fair Credit Reporting Act ("FCRA") imposes restrictions on the inclusion of certain public records in background screening reports. For example, for positions with an annual salary of less than $75,000, civil judgments and paid tax liens cannot be reported in a background screening report after 7 years, and bankruptcy filings cannot be reported after 10 years. In addition, records relating to an individual's arrest cannot be included in a background check report after 7 years. A criminal conviction, however, may be reported indefinitely. To the extent that an employer conducts a background check internally, these limitations do not apply. In the event a consumer reporting agency errs and includes in a report provided to the employer information beyond the applicable time limit, an employer would not be precluded from considering such information.

A job applicant or employee background check may also include an employment report from one or all three of the credit reporting agencies (Equifax, Experian, and TransUnion). An employment report contains information regarding an individual's credit payment history and other credit habits, but does not include the individual's credit score or date of birth. Employers often look at an individual's credit history as an indication of financial responsibility.

In addition, employers may seek to obtain education records relating to job applicants or current employees. This type of information may include dates of attendance at educational institutions and degrees earned. Employers seeking information from education records, however, may be restricted in gaining access to certain records without authorization from an adult-age student or parent due to restrictions set forth in the Family Educational Rights and Privacy Act.

Employers can also learn much about job applicants and employees by using an Internet search engine like Google. Employers likely will be able to determine information such as an individual's age, marital status, house value (complete with an aerial photograph), political affiliation, liens, blog entries, and more.

Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act of 2003

The FCRA was enacted in 1972 (and amended in 1996) to promote the accuracy, fairness, and privacy of personal information assembled by consumer reporting agencies. The FCRA allows consumer reporting agencies to furnish an entity with consumer reports only where the recipient has a permissible purpose to use the reports. Permissible purposes include use for employment purposes or use in connection with credit or insurance transactions. The FCRA defines a "consumer report" as "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, which is used or collected in whole or in part for the purpose of serving as a factor in establishing the

continued on page 2

Workplace Privacy

continued from page 1

consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes; or any other permissible purpose authorized under 1681b."

The FCRA does not require that employers conduct background checks, but establishes national standards that employers must follow when screening potential employees or investigating current employees using consumer reports obtained from consumer reporting agencies.

Under the FCRA, an employer must disclose to the job applicant or employee that the employer will be retaining a consumer reporting agency to prepare a consumer report on the individual. This disclosure must be on a stand-alone document and not part of an employment application. The employer must receive the individual's signed consent to the preparation of such a report prior to requesting the report from the consumer reporting agency.

If the employer uses information contained in the consumer report for an "adverse action," such as failure to hire or promote, rescinding an existing job offer, or reassigning or demoting an existing employee, where such actions are based, in whole or in part, on information contained in the report, the employer must notify the subject of the report prior to taking the adverse action. This pre-adverse action notice must include a copy of the report and an explanation of the individual's rights under the FCRA. After the adverse action occurs, the employer must provide the individual with an "adverse action notice." This notice would include the name, address, and phone number of the consumer reporting agency that prepared the report and statements that 1) the employer, and not the agency, made the adverse decision regarding the individual, 2) the individual has the right to a free copy of the report, and 3) the individual has the right to dispute the accuracy or completeness of the information contained in the consumer report.

The FCRA permits an employer to obtain a consumer report that has information about an individual's "character, general reputation, personal characteristics and mode of living" collected as a result of interviews with neighbors, friends, relatives, associates or others as part of an employment background check. Such reports are "investigative consumer reports." When an employer requests an "investigative consumer report," the FCRA requires that the employer provide written notice to the individual that the background report will include interviews, provide the individual with a statement of the nature and scope of the requested report and the individual's right to request additional details and, if requested, provide a written notice informing the subject of the report how to obtain a copy of his or her file. The employer must certify to the consumer reporting agency that the employer has provided the proper notice to the individual.

The FCRA also requires employers to certify to the consumer reporting agency that the employer 1) is requesting the report for a legitimate purpose (*ie*, investigation of a job applicant or existing employee), 2) has provided the employee or job applicant or employee with the requisite notice of the background check, 3) has obtained written permission from the employee or job applicant to request the background report, 4) will provide the applicant or employee with a copy of the report and written notice of the applicant's or employee's rights prior to taking an adverse action based in whole or in part on information contained in the background report, and 5) will use the background report only for employment purposes. The FCRA's notice and consent requirements do not apply to employers that conduct background checks internally rather than retaining a third-party consumer reporting agency to do so.

Employers that fail to comply with the FCRA's requirements may be liable to the individual that is the subject of the consumer report for actual damages, litigation costs, attorneys' fees, and punitive damages. Employers also may face criminal penalties for obtaining a credit report under false pretenses. The FCRA authorizes the Federal Trade Commission ("FTC") to enforce its provisions. The FTC may sue employers for up to $2500 per violation of the FCRA.

A number of states have laws that contain provisions similar to the federal FCRA. Several states, including California and New York, have FCRA analogues that regulate the use of background screening for "employment purposes." Most state analogues provide protections similar to those found in the FCRA. To the extent an employer conducts background investigations in which it requests credit reports, it should 1) determine whether the relevant state has an FCRA analogue, and 2) if it does, comply with its requirements.

In 2003, the Fair and Accurate Credit Transactions Act ("FACTA") amended the FCRA to establish standards for "employee misconduct investigations." An "employee misconduct investigation" is an investigation of an employee which is conducted by a third party that the employer hires if the employer suspects the employee of workplace misconduct or noncompliance with federal, state, or local laws or regulations, pre-existing written policies of the employer, or rules of a self-regulatory organization. FACTA exempts from the definition of "consumer report" communications made by a third party to an employer in connection with an employee misconduct investigation. Consequently, an employer is not required to obtain an employee's consent before hiring a third party to investigate employee misconduct. If the employer decides

continued on page 3

Lisa J. Sotto is a partner in the New York office of Hunton & Williams LLP and heads the firm's Privacy and Information Management Practice. She also serves as Acting Chair of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. **Elisabeth M. McCarthy** is counsel in the New York office of Hunton & Williams LLP and advises clients on privacy and information management issues.

continued from page 2

to take an adverse action against an employee following an employee misconduct investigation, however, the employer must give the employee an "adverse action" notice after such adverse action has occurred.

The employer must provide the employee subject to the adverse action with a summary of the investigation report that resulted in the adverse action. The employer is not required to disclose the sources of information for the report or the identity of any witnesses. The investigation report must be kept confidential and may only be disclosed to the employer or the employer's agent, governmental authorities, and the self-regulatory organization with regulatory authority over the employer or employee. FACTA does not permit an employee who is subject to an adverse action as a result of an investigation to dispute the findings contained in the report.

Disposing of Employee Personal Information

FTC Rule on the Disposal of Consumer Report Information

In November 2004, the FTC issued regulations requiring businesses to properly dispose of consumer report information. The rule, which became effective on June 1, 2005, was designed to help combat identity theft resulting from the improper disposal of information. The Disposal Rule requires companies to take reasonable steps to guard against unauthorized access to or use of consumer report information in connection with its disposal. It applies to any business that maintains or otherwise possesses "consumer information," which is defined as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report ... [or] a compilation of such records." Because employers frequently rely on consumer reports in connection with employment decisions, the Disposal Rule affects them. Information that does not identify individuals, such as aggregate or blind data, is not covered by the rule.

The Disposal Rule requires covered entities to properly dispose of consumer report information "by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." "Disposal" includes:

- discarding or abandoning consumer information; and
- selling, donating, or transferring any medium, including computer equipment, on which consumer information is stored.

The rule does not define what is "reasonable," instead allowing for a flexible standard that permits covered entities to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. The rule includes specific examples of measures the FTC believes satisfy the rule's disposal standard. These examples, which are intended as guidance and not as safe harbors or exclusive methods for compliance, include:

- implementing policies and procedures that require 1) the burning, pulverizing or shredding of papers containing consumer information, and 2) the destruction or erasure of electronic media containing consumer information, so the information cannot practicably be read or reconstructed;
- after conducting due diligence of the disposal company (which due diligence could include conducting an independent audit of the company's operations, obtaining references, or requiring that the disposal company be certified), entering into a contract with the disposal company to dispose of consumer information in a manner consistent with the disposal rule;
- for disposal companies, implementing policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with the first example set forth above; and
- for entities subject to the Gramm-Leach-Bliley Act's Safeguards Rule, incorporating the proper disposal of consumer information as required by the disposal rule into the information security program required by the Safeguards Rule.

State Records Disposition Laws

Several states also have laws that address the disposition of records containing personal information. Employers should determine whether the state in which they conduct business has enacted such a law and, if so, be sure to comply with its requirements.

Social Security Number Laws

Social Security Numbers ("SSNs") were initially issued by the federal government for the purpose of administering Social Security programs. Over time, however, many businesses have taken to using SSNs as unique identifiers for individuals. As a result, SSNs have become a widely used device for managing employee files, medical records, health insurance records, credit and bank accounts, and educational records. In addition, SSNs are frequently printed on licenses and identification cards.

Limiting the widespread use of SSNs has become a major focus of state legislators seeking to curb identity theft. In an attempt to limit access to SSNs by unauthorized individuals, many states have enacted laws that limit their use or require that SSNs be redacted. At the end of 2005, at least 25 states had enacted laws restricting the use of SSNs.

At least 13 states prohibit printing an individual's SSN on any card required for the individual to receive products or services provided by the person or entity issuing the card. Eight states prohibit printing SSNs on materials that are mailed to individuals unless otherwise required by federal or state law. A couple of states have chosen to allow redacted SSNs to be used in certain circumstances. A recent law enacted in California requires employers, by Jan. 1, 2008, to use no more than four digits of an employee's SSN on checks or vouchers. As of Jan. 1, 2006, health insurance carriers in Washington state are prohibited from displaying on identification cards more than any four-digit portion of the subject person's SSN. Delaware prohibits health insurers from using SSNs

continued on page 4

Workplace Privacy

continued from page 3

entirely as identification numbers on health insurance cards.

To date this year, at least 38 states have introduced additional legislation restricting the use of SSNs. More states likely will follow with similar legislation. Employers should understand how their organization uses its employee SSNs and remain vigilant about the impact of evolving legal requirements.

Next month's installment will discuss the Health Insurance Portability and Accountability Act of 1996, information security; and monitoring employee telephone, e-mail, and Internet use.

—❖—

HUNTON& WILLIAMS

Hunton & Williams LLP • www.hunton.com

Atlanta • Bangkok • Beijing • Brussels • Charlotte • Dallas • Houston • Knoxville • London • McLean • Miami • New York • Norfolk • Raleigh • Richmond • Singapore • Washington

ALM
LAW JOURNAL NEWSLETTERS

THE PRIVACY & DATA PROTECTION LEGAL REPORTER™

Volume 1, Number 5 • June 2006

What Every U.S. Employer Should Know About Workplace Privacy

Part Two of a Two-Part Series

By Lisa J. Sotto and Elisabeth M. McCarthy

Last month's article discussed background screening and Social Security number laws. This month's installment covers the Health Insurance Portability and Accountability Act of 1996; information security; and monitoring employee telephone, e-mail, and Internet use.

HIPAA

Through the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Congress called on the U.S. Department of Health and Human Services ("HHS") to promulgate regulations that would help ensure the privacy and security of health information. The Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") and the Security Standards (the "Security Rule") promulgated pursuant to HIPAA apply to "covered entities" and limit the ability of such entities to use or disclose protected health information ("PHI"). The Privacy Rule defines a "covered entity" as a health plan, health care clearinghouse, or health care provider who transmits health information in electronic form in connection with certain specified transactions. While the Privacy Rule and the Security Rule do not directly apply to employers, the requirements of these rules do apply to ERISA-covered "group health plans" that are sponsored by many employers.

The Privacy Rule prohibits covered entities from disclosing PHI except where disclosure is 1) to the individual who is the subject of the PHI, 2) for treatment, payment, or health care operations as defined in the Privacy Rule, 3) authorized by the individual, or 4) specifically permitted without authorization by the individual. The Privacy Rule requires covered entities to adopt written policies and procedures regarding the use and disclosure of PHI that are designed to comply with the Privacy Rule.

The Security Rule imposes obligations on covered entities to ensure the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits. Pursuant to the Security Rule, a covered entity is required to conduct a risk assessment of the potential risks and vulnerabilities to the confidentiality of electronic PHI held by the covered entity and to implement a risk management program to reduce the identified risks and vulnerabilities to a reasonable and appropriate level. Covered entities must have in place certain specified administrative, physical, and technical safeguards to protect the electronic PHI they maintain. Covered entities are required to adopt written policies and procedures regarding how these administrative, physical, and technical safeguards will be implemented.

The fundamental purpose of the Privacy Rule and the Security Rule is to preserve and safeguard PHI. Because plan sponsors often perform functions that are integral to the functions of group health plans and thus require access to an individual's health information held by the group health plan, the Privacy Rule restricts the flow of information from the group health plan to the employer plan sponsor. Under the Privacy Rule, a group health plan may disclose PHI to its plan sponsor only for limited purposes and only after the plan sponsor has complied with the Rule's prescribed requirements for disclosure. The principal purpose of this regulatory barrier between a "group health plan" and an employer plan sponsor is to prevent employers from using their employees' PHI to make employment-related decisions. It is worth noting, however, that the Privacy Rule exempts from the definition of PHI, employment records held by a covered entity in its role as employer. Pursuant to this exemption, to the extent that an employer in its capacity other than as plan sponsor collects and maintains health information regarding its employees, HIPAA would not apply.

To determine the impact of the Privacy Rule, an organization must examine 1) the type of health information the plan sponsor receives; 2) the purposes for which the plan sponsor receives information; and 3) the extent, if any, to which the plan sponsor performs administrative functions on behalf of the group health plan.

continued on page 2

Lisa J. Sotto is a partner in the New York office of Hunton & Williams LLP and heads the firm's Privacy and Information Management Practice. She also serves as Acting Chair of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. **Elisabeth M. McCarthy** is counsel in the New York office of Hunton & Williams LLP and advises clients on privacy and information management issues.

Workplace Privacy

continued from page 1

The Privacy Rule defines a plan sponsor's responsibilities based on whether the plan sponsor receives "protected health information" or "summary health information." A plan sponsor that receives summary health information — that is, information that is a subset of PHI that summarizes claims history, expense, or experience and is stripped of certain personal identifiers — is minimally impacted by the Privacy Rule. A plan sponsor that needs only summary health information to effectively manage its health benefits program may receive the information if it agrees to limit its use of the information to 1) obtaining premium bids for providing health insurance coverage to the group health plan, or 2) modifying, amending, or terminating the group health plan.

On the other hand, a plan sponsor that receives PHI is subject to increased operational and administrative burdens. Plan sponsors typically may receive PHI either from the group health plan itself or from another entity (such as an insurer) that administers the company's health benefits program. Before a plan sponsor may receive PHI, the group health plan or the insurer acting on behalf of the plan must get assurance in the form of a "certification" that the plan sponsor has complied with the new regulatory requirements.

A plan sponsor must certify to the group health plan that it has amended the plan documents to incorporate various provisions. Unless disclosing PHI for enrollment purposes, the plan documents need to be amended before the sponsor may receive PHI. The plan sponsor must agree to:

- not use or further disclose PHI except as permitted or required by the plan documents or as required by law;
- ensure that any subcontractors or agents to whom the plan sponsor provides PHI agree to the same restrictions;
- not use or disclose PHI for employment-related actions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- report to the group health plan any use or disclosure that is inconsistent with those provided for in the plan documents;
- allow individuals to inspect and copy PHI about themselves;
- allow individuals to amend PHI about themselves;
- provide individuals with an accounting of disclosures of their PHI;
- make the plan sponsor's practices available to the Department of Health and Human Services ("HHS") for determining compliance;
- return and destroy all PHI when no longer needed, if feasible; and
- ensure that firewalls for records and employees have been established between the group health plan and the plan sponsor.

In addition, the plan documents must identify, either by name or function, any employee of the plan sponsor who receives PHI for payment, health care operations, or other matters related to the group health plan. The plan documents also must restrict access to and use of PHI to specific, identified employees for the purpose of completing the administrative functions the plan sponsor performs for the group health plan. Finally, the plan documents must provide an effective mechanism for resolving issues of improper use of or access to PHI. The health insurance issuer or other group health plan may disclose PHI to the plan sponsor only after it receives the plan sponsor's certification indicating that the plan documents were amended.

Disclosure of PHI in violation of HIPAA can result in steep civil and criminal penalties (up to $250,000 in fines and 10 years of imprisonment). Consequently, employers who act as plan sponsors must carefully assess their compliance with HIPAA's Privacy Rule and Security Rule.

HIPAA establishes a basic level of protection for health information. State laws relating to the privacy of health information are not pre-empted by HIPAA if they offer more stringent protections. Employers should consider relevant state laws on a case-by-case basis as specific issues arise.

Information Security

Security Breach Notification Laws

The recent increase in identity theft crimes (discussed earlier) resulted in the enactment of numerous state security breach notification laws. These laws generally do not distinguish between consumers and employees. Consequently, employers would be required to comply with these laws in the event that unauthorized individuals acquire certain employee personal information. A security breach occurs when an unauthorized person acquires or accesses personal information maintained by a company. It is not a breach when an employee or company agent acquires or accesses the data for company purposes as long as the data is not used or disclosed in an unauthorized manner.

Although these laws differ somewhat, generally an entity that maintains "personal information" about individuals needs to notify those individuals of certain security breaches involving computerized data. Specifically, entities are required to notify those whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. "Personal information" typically means unencrypted data consisting of a person's first name or first initial and last name, in combination with a Social Security number; a driver's license or ID card number; or an account, credit card, or debit card number along with a password or access code. Entities subject to these laws must notify individuals immediately following discovery of a breach if an unauthorized person may have acquired unencrypted electronic personal information.

To date, 29 states have enacted security breach notification laws. Most of these state laws differ at least to some extent. Employers are well advised to determine whether the state in which they operate has a security breach notification law and

continued on page 3

Workplace Privacy

continued from page 2

to comply with such state's specific requirements in the event of a security breach.

Safeguarding Personal Information

Considering the tremendous cost to businesses that suffer security breaches, employers are well advised to develop and implement a plan to safeguard the personal information that they maintain. Such a plan should be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it maintains. While there are a handful of basic elements listed below that every safeguards plan should address, businesses have the flexibility to implement policies, procedures, and technologies that are appropriate to their unique circumstances.

1) Designate one or more employees to coordinate a safeguards program.

Whether an organization tasks a single employee with coordinating safeguards or spreads the responsibility among a team of employees, someone in the organization needs to be accountable for information security. In deciding who it should be, employers should recognize that information security is fundamentally a management issue, not a technology issue. While information technology can play a significant role in protecting data, effective information security requires a broader focus and should include physical security, employee training and management, and business processes.

In addition, an appropriate safeguards program will almost certainly require the coordination of legal, human resources, information technology, audit, and business functions. The person or team that coordinates the program should have the ability to communicate and work effectively with all of these different groups.

2) Identify and assess the risks to individuals' personal information in each relevant area of the company's operations and evaluate the effectiveness of current safeguards for controlling these risks.

To conduct a risk assessment, an employer will need to identify the information that is being protected and the related risks to that information. In particular, an employer should focus on protecting individuals' personal information in addition to the company's business information and operations. To begin, an employer should identify the personal information that it actually collects, how the employer uses it, where it is stored, to whom it is disclosed, who has access to it for what purposes, and how it will ultimately be disposed. The employer should map these data flows and classify data by sensitivity so security measures can be prioritized.

Next, an employer should consider all the ways that personal information can be compromised. While an employer should obviously consider intrusions by computer hackers, employers should also think about ways that employees, service providers, business partners, or vendors could compromise the security of personal information either intentionally or through carelessness. Employers should take into account risks beyond those associated with information technology and consider business processes as well. It is advisable to have the risk assessment process be conducted by a team that includes both technical and business personnel because of their different perspectives on the likelihood and impact of threats.

Once the risks are identified, a gap analysis is necessary to evaluate where current safeguards are inadequate to address the identified risks. Employers should consider the likelihood that a given risk will occur and the severity of the consequences should it happen. Employers should also consider the effectiveness of the various available security measures and their cost, relative to the harm caused by a compromise.

Employers should recognize the full range of potential costs in the event of a security breach: the cost of investigating a security breach; mitigating and remediating damage to systems, and securing the systems after the breach; lost sales or productivity caused by the unavailability of systems or data; notifying affected individuals and government agencies, as appropriate; responding to regulator inquiries and enforcement actions; legal fees and costs for the defense of private lawsuits; lost customers; reputational damage; and a possible drop in stock price. The harm caused by a compromise should be defined more broadly than just the resulting financial costs.

3) Design and implement a safeguards program, and regularly monitor and test it.

In designing a safeguards program, employers should consider all areas of operations, such as employee management and training; information systems; and managing system failures, which encompasses prevention, detection and response to attacks, intrusions, and other system failures.

The goal is to create security policies and procedures that are more than mere paper and will actually be followed in day-to-day business operations. Employers should monitor and test each of the elements of their program to reveal whether it is being followed consistently and whether it is operating effectively to manage the risks to personal information that it was designed to address.

4) Select appropriate service providers and contract with them to implement safeguards.

When service providers or other third parties have access to data or information systems, steps should be taken to determine whether they can be trusted not to compromise information security and to ensure that they are contractually required to meet specified safeguards standards.

When conducting due diligence on third-party service providers, employers should review an independent audit of the third party's operations; obtain information about the third party from several references or other reliable sources; require that the third party be certified by a recognized trade association or similar authority; review and evaluate the service provider's information security policies and procedures; and take other appropriate measures to

continued on page 4

Workplace Privacy

continued from page 3

determine the competency and integrity of the party.

Contracts with third parties should specifically address safeguards obligations; a general confidentiality provision is not sufficient. Employers should also require third parties to notify them of significant security incidents (so the employer can determine whether it has any legal obligations to provide notice to individuals of a possible data compromise) and to cooperate in responding to security incidents and investigating data breaches. In addition, an employer may want to ask for the right to audit a third party's safeguards program for compliance with legal and contractual requirements.

5) Evaluate and adjust the safeguards program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring.

Security is an ongoing process, not a static condition. Employers need to evaluate and adjust their safeguards program at regular intervals and respond to results obtained through testing and monitoring the program. A safeguards program also will require changes to keep up with technology, business practice, and personnel. Employers should remain vigilant about new or emerging threats to information security and changes in the legal and regulatory environment.

Monitoring Employee Telephone, E-mail, and Internet Use

Employers have a legitimate interest in knowing how their employees spend their time at work. Inappropriate e-mail can trigger workplace lawsuits and sexual harassment claims. Cyberslacking and excessive personal telephone calls at work waste employee time, costing employers millions of dollars in lost productivity. Technological advances make it increasingly easy for employers to monitor employees and limit negative behavior. Employers should make certain, however, that they understand their legal rights and obligations before conducting such monitoring.

Telephone Monitoring

The Federal Omnibus Crime, Control and Safe Streets Act of 1968

The Federal Omnibus Crime, Control and Safe Streets Act of 1968 (the "Federal Wiretapping Law") governs the access, use, disclosure, interception, and privacy protections associated with wire communications. The Federal Wiretapping Law prohibits the intentional interception of wire communications such as telephone calls. "Intercept" means the acquisition of the contents of any wire communication through the use of any electronic, mechanical, or other device. There are exceptions under the Federal Wiretapping Law for telephone calls intercepted by wire communications service providers in the ordinary course of business and where there is express or implied consent by one of the parties to the communication. Employers generally are considered to be service providers because the employer typically provides the telephone service being used. Whether or not one of these exceptions applies is determined on a case-by-case basis. For example, the Eighth Circuit in *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992), and the 11th Circuit in *Watkins v. L.M., Berry & Co.*, 704 F.2d 577 (11th Cir. 1983), ruled that implied consent does not exist where an employee is only informed that telephone conversations might be monitored. Implied consent requires a higher standard of awareness that monitoring will take place. The court in *Watkins* also held that personal phone calls may not be intercepted in the ordinary course of business, except to guard against unauthorized activity or to determine that such communications are personal. An employer must discontinue recording or monitoring of any personal communication once it is known that the call is personal. In *Deal v. Spears*, the court held that excessive monitoring without a legitimate business purpose is not permitted.

State Wiretapping Laws

Most states have passed anti-wiretapping laws that regulate the interception and recording of telephone calls. Most states require at least one person who is a party to the conversation to consent to recording the conversation. Some states, however, require the consent of all parties involved.

Employers wishing to monitor telephone conversations of employees should be aware of, and abide by, the applicable state law prior to engaging in such activity.

E-mail Monitoring

Federal Electronic Communications Privacy Act of 1986 and the Stored Communications Act

Although primarily drafted to apply to law enforcement authorities, the federal Electronic Communications Privacy Act of 1986 ("ECPA") governs the access, use, disclosure, interception, and privacy protections associated with electronic communications. The ECPA prohibits the intentional interception of electronic communications, including e-mail in transit, but not such communications in storage (*ie*, in an e-mail "In Box"). There is an exception, however, for e-mail intercepted in the ordinary course of business and another exception where there is express or implied consent by at least one party to the communication. The ECPA as initially drafted did not apply to electronic communications in storage. The ECPA eventually was amended by the Stored Communications Act, which governs access to electronic communication in storage. This Act prohibits the intentional unauthorized access to e-mail in storage. Service providers, however, are exempt when accessing stored electronic information. Employers generally are considered to be service providers because the employer typically provides the electronic communications service being used. Therefore, the federal statutes permit employers to monitor employee e-mail.

State E-mail Monitoring Laws

Connecticut and Delaware are the only states that specifically regulate the monitoring of employee e-mail by employers. Both states have enacted statutes that require employers to provide advance notice of any

continued on page 5

Workplace Privacy

continued from page 4

electronic monitoring in the workplace and prohibit monitoring without such notice to employees. There is no case law in either Connecticut or Delaware interpreting or applying the relevant statutes.

Connecticut. Section 31-48d of the Connecticut General Statutes governs an employer's ability to electronically monitor its employees. This law requires employers to conspicuously post a notice concerning the types of electronic monitoring in which the employer may engage. "Electronic monitoring" is broadly defined as "the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems."

There is a limited exception for the investigation of illegal activities. Pursuant to the exception, an employer may conduct monitoring without giving prior written notice when 1) an employer has reasonable grounds to believe an employee is engaged in conduct that violates a law, violates legal rights of the employer or other employees, or creates a hostile workplace environment, and 2) electronic monitoring may produce evidence of such misconduct. Violation of the statute may result in monetary penalties.

Delaware. Delaware law requires employers who monitor employees' Internet access, telephone calls, or electronic mail to provide notice to the employees at hiring or before beginning monitoring. Employers may provide notice either by posting it electronically so an employee sees it at least once each day or by providing a one-time notice in writing, in an electronic record or in another electronic form and having it acknowledged by the employee either in writing or electronically. Unlike the Connecticut law, the Delaware law does not exempt employers from giving notice to employees when the monitoring of e-mail communications is for purposes of investigating an illegal activity. Similar to Connecticut, violation of the statute may result in monetary penalties.

State Wiretapping Laws

Many states have passed anti-wiretapping laws, similar to the ECPA, which regulate the interception of electronic communications. Most states require the consent of at least one person who is a party to the communications. Some states, however, require the consent of all parties involved.

National Labor Relations Board

Workplaces with unionized labor may be subject to additional restrictions on e-mail monitoring. The National Labor Relations Board ("NLRB") Office of General Counsel published an Advice Decision in 1998 stating that business-only e-mail policies (restricting use of e-mail to business purposes only) were unlawful in situations where computers and computer networks are part of employee "work-areas." The NLRB indicated that such policies would deter protected communication among union members. The NLRB found the prohibition of all personal e-mail to be "overbroad and facially unlawful" in situations where the computers are considered an employee's work area because it banned protected oral solicitation by union members. NLRB rules treat union-related oral solicitation and the distribution of written materials differently. An employer may not prohibit all oral solicitation in the work area, but may limit this communication to non-work hours. In finding that the computer systems were part of employee work areas, communications in the work area could not be completely prohibited or limited to business uses without effectively banning oral solicitation in that work area.

Internet Monitoring

Employers have a legitimate interest in monitoring the Internet use of employees. Employers should be aware, however, that if they monitor employee Internet use, the information the employer learns or is on notice of as a result of such monitoring may impose a legal obligation on the employer. In *Doe v. XYC Corp.*, 877 A.2d 1156 (2005), the New Jersey Appellate Court held that an employer that is on notice that one of its employees is using a workplace computer to access child pornography has a duty to investigate the employee, to report the employee's activities to the proper authorities, and to take effective internal action to stop the continuation of such activities.

Common Law Privacy

In circumstances where an employee may not be able to prove a violation of federal or state statutory law, the employer may still be liable for common law invasion of privacy. In the United States, there are four privacy torts: 1) intrusion upon seclusion, 2) false light, 3) appropriation of likeness, and 4) public disclosure of embarrassing private facts. The availability of these tort claims depends on the relevant state law and the specific facts alleged. For example, a constitutional right of privacy exists in California and nine other states. Georgia has a common law right of privacy. New York has neither a constitutional nor a common law right of privacy. Of the four privacy torts, intrusion upon seclusion is probably the most relevant to employers.

The Restatement (Second) of Torts §625B defines the tort of intrusion upon seclusion as the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be "highly offensive to a reasonable person." To determine whether an intrusion would be offensive to a reasonable person, courts have examined the degree of intrusion, the context, the conduct and circumstances surrounding the intrusion, and the intruder's motives and objectives. The key factor, however, is the expectation of the individual whose privacy allegedly was invaded. An individual would have to show that he had a "reasonable expectation of privacy."

The intrusion upon seclusion tort is relevant in the context of information privacy because employees have used it to make arguments against employer monitoring. It is a difficult claim, however, for employees to

continued on page 6

Workplace Privacy

continued from page 5

successfully assert. The U.S. Supreme Court recognized in *O'Connor v. Ortega*, 480 U.S. 709 (1987), that employers have a legitimate interest in monitoring the workspace of their employees. The only cases in which employees have successfully asserted an intrusion upon seclusion claim involve those in which the employer's surveillance activities were considered "outrageous." For example, in *Hawaii v. Bonnell*, 856 P.2d 1265 (Haw. 1993), an employer set up a video camera in an employee break room used only for non-work purposes. The court held that employees have a subjective expectation of privacy to be free from covert video surveillance in the break room and that their subjective expectation was objectively reasonable because the break room was not a public place or subject to public view or hearing. Several court decisions, such as *Smyth v. Pillsbury Co*., 914 F.Supp. 97 (E.D. Pa. 1996), and *Bohach v. City of Reno*, 932 F.Supp. 1232 (D. Nev. 1996), have allowed employers to monitor employees' use of company e-mail and the Internet, finding that employees do not have a reasonable expectation of privacy with respect to an e-mail message communicated over an employer's computer system.

Employers should take care that telephone conversations of a personal nature are not monitored once it is apparent that the conversation is not related to the legitimate business purpose that prompted the monitoring. If employers want to monitor or record conversations of sales or service representatives with customers, employee telephones used for such purpose should be marked appropriately and a recorded notice should be given at the beginning of the telephone call notifying the customer that the call is being monitored or tape recorded.

Employers should apply the following guidelines when monitoring employees:

- Monitor only if there is a compelling reason;
- Clearly inform employees on the full scope of monitoring in an employee handbook or e-mail to all employees;
- Use the least intrusive measures available;
- Retain information obtained as a result of monitoring for only the time needed;
- Treat all employees uniformly and apply policies consistently; and
- Determine whether monitoring imposes an obligation to take action.

Conclusion

Although there is no omnibus U.S. employee privacy law, employers face myriad privacy requirements with respect to the management of employee personal information. These requirements apply prior to the commencement of the employment relationship, throughout the employment period, and after the relationship has ended. Employers should use caution in collecting, using, and disclosing employee personal information and should aim to comply with all the legal mandates that impact the use of such information. Employers are well advised to develop and implement comprehensive written information security programs to safeguard employee personal information from misuse or unauthorized acquisition. Employers should also develop and implement written policies and procedures with respect to monitoring the behavior of their employees. Although U.S. legal requirements affecting workplace privacy are complex, employers should respect and protect the privacy rights of their employees.

—❖—