This article recently appeared in *Privacy & Security Law Report*, April 2006.

Re-Thinking Privacy: 10 Reasons Why Your Business Should Be More Concerned About Workplace Privacy

by Philip L. Gordon

"The Customer Is King"—a mantra that drives most sales and marketing departments appears to be driving the privacy agendas at many organizations, relegating workplace privacy to an afterthought, if that. While no empirical study has compared the resources dedicated to safeguarding the privacy of customers versus those dedicated to employee privacy issues, anecdotal evidence strongly suggests that workplace privacy has fallen into the crevice between the Chief Privacy Officer's branch of the organizational chart and the branch headed by the Director of Human Resources. Professional journals in the area of privacy overflow with articles addressing consumer privacy issues, with only a sprinkling of coverage concerning workplace privacy. Conferences aimed at privacy professionals provide presentations on every conceivable angle of consumer privacy while paying only fleeting attention, if any, to workplace privacy.

While the emphasis on customer privacy is understandable and its importance cannot be denied, the lack of attention given to workplace privacy issues is surprising. For a long list of reasons, those issues pose equal, if not greater, risks and potential rewards. This article discusses 10 of the most important reasons.

1. Don't Expect Your Employees to Care About Customer Privacy if You Don't Care About Their Privacy.

Organizations seeking to establish brand loyalty and enduring customer relationships by building customer trust need to impress on employees their roles as data stewards because employees pose the most significant risk to confidential business and consumer information. According to the Ponemon Institute, a leading privacy research organization, insiders are responsible for 70 percent of all data thefts. The Centers for Medicare and Medicaid Services, which is responsible for enforcing information security regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), identifies the employees of health care organizations as the number one threat to protected health information (PHI). Reducing the risks to customer privacy and data security posed by an organization's own workforce requires education in an area that often runs counter to the self-interest of employees who may see avenues to increase their compensation through "creative" uses of customer information.

Training sessions that emphasize an organization's concern for customer privacy are likely to ring hollow for employees whose own privacy interests are not respected. Why, for example, should employees take seriously an employer's request that they safeguard customer credit and debit card account numbers when their employer's own carelessness allowed a hacker to obtain access to employee Social Security numbers? Similarly, employees hardly can be expected to safeguard the PHI of patients or insureds when the employees' own medical conditions routinely becomes the subject of office gossip. Conversely, employees who believe that their employer respects their privacy interests are far more likely to embrace their role in safeguarding customer information against misuse and abuse.

2. Stored Employee Information Creates Data Protection Obligations

Fundamental principles of data protection reflect the common sense notion that less data means fewer risks of privacy violations

and security breaches. These principles call upon organizations to collect only the minimum information necessary to achieve lawful objectives and to retain that information only for as long as is necessary to achieve those objectives. As the quantity and sensitivity of stored information increases, so do the exposure and the responsibilities of the organization that stores the information. Viewed from this perspective, employee information creates significant responsibilities—potentially greater than those resulting from collections of customer information—because employers typically possess substantial stores of sensitive information about their employees.

Virtually all employers maintain, at a minimum, a database containing their employees' first and last name, home address and telephone number, rate of compensation, date of birth, direct deposit information, and Social Security number. This information typically is just the tip of the iceberg. In the wake of 9/11, employers are increasingly scrutinizing job applicants before hiring and employees before promotion. According to a 2004 study conducted by the Society of Human Resources Management, the percentage of employers conducting criminal background checks jumped from 51 percent to 82 percent between 1996 and 2003, and the percentage of employers conducting credit checks almost doubled. By combining the information obtained through these searches with the educational and occupational histories provided by job applicants, most employers maintain a near-complete picture of their employees' past.

Many employers supplement this historical information with substantial detail about their employees' daily lives. While most background checks do not include medical information, employers acquire a fairly detailed picture of their employees' physical and psychological condition by administering employee benefit plans, engaging in the reasonable accommodation process mandated by the Americans with Disabilities Act, reviewing requests for medical leave under the Family and Medical Leave Act, and receiving routine notices of health-related absences. As computer storage capacity has become increasingly inexpensive and an increasing number of employees spend their days at a computer keyboard, employers are retaining vast stores of employee e-mail and expanding logs of daily Internet use. Employers also monitor their employees' daily activities through the use of "time clocks" (now often sophisticated devices using biometric technology), video surveillance, and regular performance appraisals.

No business comes close to obtaining and retaining as wide a range of information about its customers as it does about its own employees. Financial institutions, for example, may have credit histories and even full background checks about their customers, but they possess only very limited information, if any, about their customers' health, job performance, and daily e-mail and Internet usage. Health care providers may possess more detailed health information about their patients than employers do about their employees, but are unlikely to possess background checks or information about rates of compensation or job performance.

3. State Data Protection Laws Apply to Personnel Information

A recent spate of state-enacted data protection legislation has forced many businesses to focus more attention on consumer privacy and information security. While these newly enacted laws may have been intended to protect customer information, many also have significant implications for businesses in their capacity as employers.

- Eighteen states—including California, Illinois, Michigan, New Jersey, and Texas—have enacted statutes that impose restrictions on publicly displaying Social Security numbers, printing Social Security numbers on cards used to obtain goods or services, transmitting unencrypted Social Security numbers over the Internet, and/or mailing Social Security numbers. Each of these provisions has an impact on all employers who, by law, must obtain their employees' Social Security numbers. For example, SSNs no longer can be printed on identification badges or on insurance benefit cards; employee benefits Web sites must provide secure transmission before requiring entry of an SSN for identification purposes; and employer mailings that contain an SSN should be subject to legal review before being sent.
- Six states—Arkansas, California, Nevada, North Carolina, Rhode Island, and Texas—now require entities which own computerized "personal information"—defined to include, among other things, first and last name plus Social Security number—to provide reasonable safeguards for that information. Some of these statutes also require that data owners obtain written assurances from those with whom they share personal information under contract to implement reasonable and appropriate safeguards for the information. The first prong of these statutes applies directly to all employers in those states who collect and store employee SSNs in computerized form. The second prong applies to the increasing number of employers that rely on business process outsourcers—such as third-party benefits administrators, payroll administrators, and COBRA administrators—who need employee SSNs to perform their services.
- Twenty-three states—including California, Florida, Illinois, New Jersey, New York, Ohio, Pennsylvania, and Texas—now require that any entity which owns "personal information" (as defined above) to provide notice to those whose unencrypted "personal information" has been acquired by an unauthorized person. Again, because most employers today retain employee SSNs in computerized form, these statutes have a direct impact on most employers.

4. Workplace Privacy Laws Extend Far Beyond State-Enacted Data Protection Statutes

The newly enacted state data protection statutes comprise just a portion of the state, federal, and international privacy legislation and regulation that has an impact on employers. In fact, employers are subject to a host of additional laws related to workplace privacy. Complying with this expanding web of rules—only a portion of which can even be mentioned here—often will be a substantial challenge for any organization.

HIPAA imposes strict privacy and data security obligations on most employers who choose to self-insure their group health, vision, or dental plans, or who sponsor health care reimbursement flexible spending accounts or employee assistance programs. Background checks, credit checks, and criminal history checks cannot be obtained and used for employment decisions without following the detailed procedures in the Fair Credit Reporting Act (FCRA), and the Federal Trade Commission's (FTC) "Disposal Rule"

establishes standards for the proper destruction of such reports. The ADA minimizes the circumstances in which employers may inquire about a job applicant's or employee's health condition and strictly limits the use and disclosure of the medical information obtained in response to such inquiries. The European Union (EU) Data Protection Directive restricts the "export" of personal data from the EU to the United States.

A variety of state laws create additional privacy protections for employees. Employers who conduct drug or alcohol testing must do so in accordance with applicable state law, which often limits an employer's right to test if the test will infringe upon state protected privacy rights. Many states have enacted statutes restricting the use of genetic information in employment decisions and limiting the circumstances in which employers can take adverse employment action based upon an employee's lawful off-duty conduct, such as the consumption of tobacco products or "blogging." California law creates privacy protections for employee health information that supplement protections established by HIPAA and the ADA. Delaware and Connecticut require notice to employees of electronic monitoring.

In short, the number and breadth of laws and regulations that address employee privacy far exceeds those addressing customer information.

5. Employee and Customer Information Are Equally Vulnerable to Security Breaches.

According to the Privacy Rights Clearinghouse, more than 125 publicly reported data breaches between February 2005 and February 2006 exposed the personal information of more than 50 million individuals. The causes of these data breaches included stolen hard drives and servers, lost laptops and back-up tapes, attacks by hackers and the shenanigans of unscrupulous or disgruntled employees. These vulnerabilities exposed *both* customer and employee information.

A sampling of publicly reported data breaches illustrates the point. Time Warner's storage vendor lost a back-up tape containing information about 600,000 current and former employees. Boeing Corp. announced that the theft of a computer exposed the personal information of 161,000 employees. MCI Communications reported that a lost laptop contained the personal information of 16,500 employees. At Honeywell International, a disgruntled former employee posted the personal information of 19,000 current and former employees on a Web site.

Fourteen security breaches examined by the PGP Corp. in November 2005 cost $14 million on average—$5 million in out-of-pocket losses, $1.5 million in lost productivity, and $7.5 million in damaged business reputation. While the study focused on data breaches involving customer information, security breaches involving employee information could easily cost an organization *more*, particularly in lost productivity, because affected employees can be expected to engage in remedial measures during working hours.

6. New Technologies in the Workplace Raise New And Complex Privacy Issues.

An increasing number of new technologies are entering the workplace, raising a whole new genre of workplace privacy issues. Employees are shirking under the watchful eye of Radio Frequency Identification (RFID)-enabled security badges and (GPS) global positioning system-enabled cell phones that are capable of tracking and storing employee movements inside, and away from, the workplace. "Blogging," whether sanctioned by the employer or used by the employee after work "to blow off steam" or engage in union organizing, has become a prickly issue for many employers who do not want to overreach, but are concerned by the blogs' provocative content. Camera phones expose employees to intrusive photography by voyeuristic co-workers whose conduct can expose the employer to liability. Each of these technologies calls upon the employer to consider developing new policies and procedures that appropriately balance the employer's business interests and employees' privacy interests.

7. Employee Privacy Breaches Create a Significant Risk of Litigation

While the risk of consumer-based privacy litigation stems almost exclusively from data breaches, employee-based privacy litigation can stem from a wide range of sources in addition to unauthorized cquisition of employee data. Indeed, employees routinely sue their employers for alleged privacy misconduct, including, for example, improprieties in connection with drug or alcohol testing, the misuse or abuse of employee health information, violations of the FCRA's requirements governing the use of background checks, improper searches of areas that the employee claims to be private, and reviewing e-mail stored in an employee's Web-based e-mail account.

To be sure, government agencies, such as the FTC and state attorneys general, typically assert privacybased claims only on behalf of consumers, not employees. Even so, the number of employee-based lawsuits alleging privacy violations against employers dwarfs the number of government-initiated privacy actions filed on behalf of consumers.

8. Privacy-Based Litigation Involving Employees Can Expose an Organization to Large, Adverse Jury Verdicts.

Litigation stemming from data breaches poses similar risks regardless of whether employee or consumer information is involved, and the damages awarded to any individual plaintiff most likely will be relatively small. By contrast, other types of workplace privacy violations pose a significant risk of large damage awards because they frequently involve deeply humiliating circumstances and/or loss of employment.

Several recent jury verdicts illustrate this point. A Florida jury awarded two female employees $1 million in damages each against a financial services company where a co-worker planted a hidden camera under the plaintiffs' desks and then posted the photographs on a pornographic Web site. The Arkansas Supreme Court upheld a $1.65 million jury verdict against Wal-Mart based upon the search of an employee's home for allegedly stolen property. An employee who claimed that his former employer improperly opened his personal mail won a jury verdict exceeding one-half million dollars. And, a Hooter's waitress recovered $275,000 based upon her allegation that male co-workers observed her through a peep hole into the women's restroom.

9. Employers That Monitor Employee E-Mail Are Exposed to New Risks.

Given the generally accepted wisdom that employers who tell their employees that they have "no reasonable expectation of privacy" in their e-mail can monitor employee e-mail with impunity, it is not surprising that most employers engage in some form of e-mail monitoring. The American Management Association reported in 2005 that 60 percent of 840 companies surveyed were regularly monitoring employee e-mail.

An August 2005 decision by the United States Court of Appeals for the First Circuit, which received only passing attention in employment and privacy circles, suggests that at least some of the many employers who engage in e-mail monitoring are exposed to potential liability under the Federal Wiretap Act. In that case, *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc), the appeals court held that a software program which copies electronic mail while fleetingly stored incident to transmission and delivers the copy to a person other than the intended recipient effectuates an "interception" within the meaning of the Act. At least some purveyors of e-mail monitoring software suggest that their product is fundamentally indistinguishable from the software at issue in *Councilman* by advertising the software's "real-time" interception capabilities. Thus, employers who have implemented such monitoring software may be intercepting e-mail in violation of the Federal Wiretap Act.

To be sure, such interceptions would be lawful under the Act if the monitored employees consented to the interceptions. However, case law construing the Act strongly suggests that telling employees they have no reasonable expectation of privacy in their e-mail, without more, does *not* amount to consent to real-time monitoring for purposes of the Act. Given that the Federal Wiretap Act provides for minimum statutory damages of $10,000 per violation, the potential liability is significant.

Putting aside the exposure arising from monitoring e-mail in real time, a December 2005 decision by the New Jersey Superior Court, Appellate Division raises a different risk of liability from any form of e-mail or Internet monitoring. In *Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. Sup. Ct. App. Div. 2005), the court held that an employer had a duty to stop an employee's child-porn activities conducted using the employer's electronic resources and to notify law enforcement authorities, because the company's review of computer logs and the "Web sites visited" function on the employee's desktop revealed that the employee was accessing adult pornography. In other words, employers who fail to respond appropriately to an employee's unlawful conduct using the employer's Internet access, or even to lawful (albeit inappropriate) conduct that suggests criminal activity, could be held liable in negligence to the employeecriminal's victims.

10. Organizations Are Under Increasing Pressure to Disclose Employee Information to Government Agencies.

Given the vast stores of data that employers accumulate about their employees, it should be no surprise that government agencies investigating potential terrorist activities have trained their attention on records held by employers. According to a November 2005 report in the *Washington Post*, the FBI now issues annually to U.S. business 30,000 "National Security Letters" (NSLs), demanding communications and financial records, and an unknown number of "FISA [Foreign Intelligence Surveillance Act] subpoenas," which demand production of "any tangible things (including books, records, papers, documents and other items)."

These demands became so intrusive and burdensome that a coalition of business/employer advocacy groups—which included the U.S. Chamber of Commerce, the National Association of Manufacturers, the Financial Services Roundtable, and the American Corporate Counsel Association—lobbied for and obtained amendments to the USA PATRIOT Act that impose limits on the FBI's use of NSLs and FISA subpoenas. Re-flecting the increasing sensitivity of corporate America to workplace privacy issues, these groups, in a November 2005 letter to Senator Arlen Specter (R-Pa.), chairman of the Senate Judiciary Committee, cited "potential violations of the privacy and civil liberties of employees" as one justification for their position. The groups also emphasized that responding to NSLs and FISA subpoenas puts them at risk of "loss of reputation or litigation—here or abroad—for violating the privacy rights of others."

Conclusion

Workplace privacy issues raise a host of challenges for employers. A corporate culture that complies fully with workplace privacy laws and takes employee privacy concerns into account can reduce an organization's exposure to privacy violations and security breaches involving both employees and customers. To that end, employers should consider taking steps, such as conducting a workplace privacy legal compliance audit; appointing a senior-level employee with overall responsibility for workplace privacy issues; creating or updating policies, practices, and procedures to address rapidly evolving legal standards and workplace technologies; properly managing sensitive employee information; and developing a strategy for responding to government, and other third-party, requests for employee information that will reduce the risk of litigation.

Reproduced with permission from
Privacy & Security Law Report,
Vol. 5, No. 15, pp. 524-527
(April 10, 2006).