Bloomberg Law Reports® Labor & Employment

Safeguarding Your Employees' Personal Data: How to Protect Employees, Your Company's Reputation, and the Bottom Line

Contributed by Allegra Lawrence-Hardy & Jessica Sawyer Wang, Sutherland Asbill & Brennan LLP

Every time a company laptop is lost or a password is inadvertently disclosed, the door is opened for a serious data breach. Employees are at risk of identity theft or other crimes, and employers could be liable for failure to protect their employees' compromised personal identifying information, or "PII." To protect their employees and themselves, employers must ensure that their PII policies cover the familiar basics, such as employees' social security numbers and financial information—but that's not necessarily all. The recent enactment of expansive data security laws means that, in a growing number of states, employers must also provide protections for additional types of employee PII, such as home addresses, cellular telephone numbers, and email addresses. As a result of these new laws, employers are increasingly at risk of lawsuits based on misuse of employee PII. What's more, some states call for administrative investigations and stiff civil penalties when a breach occurs. And no employer wants to be embarrassed by the sensational news stories that so often follow a security breach. Establishing comprehensive PII policies will protect not only the employee data, but also the company's reputation and ultimately its bottom line.

Under most data security laws, PII is any information that can be used alone, or with other sources, to uniquely identify a single person. Because modern technology has made it easier to amass large quantities of PII, and because technology is so easily portable, PII is extremely vulnerable to breaches. In response to this growing threat, legislatures have enacted a variety of laws to limit the accessibility to and distribution of PII. At least thirty states have passed laws protecting social security numbers, and all fifty states have laws criminalizing the use of PII for identity theft. Almost all states require notification when a breach occurs. Increasingly, however, state legislatures are determining that these protections are insufficient, and they are imposing new and expanded duties on employers to safeguard the PII of their employees.

For example, in 2009, New York enacted a statute protecting employee PII, which is expansively defined to include an employee's social security number, home address, telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, and driver's license number.[1] The law dictates that employers may not "[c]ommunicate an employee's personal identifying information to the general public."[2] Employers can be fined for any knowing violation of the law. Connecticut is another state that has tasked employers with the safeguarding of employee data.[3] That state's law mandates that employers destroy, erase, or make unreadable PII contained in computer files or documents prior to disposal.[4] The law defines PII as "information capable of being associated with a particular individual through one or more identifiers."[5]

Other states also are moving towards providing more privacy protections. Even if their laws are not aimed at protecting employees, *per se*, they nevertheless will impact employers. In California, for example, businesses that license or own the PII of a California resident must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[6] The California law defines PII as including a person's full name in combination with some other identifying information, such as a driver's license number, a financial access code, or medical information.[7] This broad definition includes PII that employers often maintain.

Nevada and Massachusetts have passed the most demanding of the recent laws protecting PII. The Nevada law, which went into effect January 1, 2010, requires encryption of all PII that is transferred "beyond the logical or physical controls" of a company or its data storage provider on any data storage device.[8] A "data storage device" is "any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself."[9] This includes, for example, CDs or DVDs containing PII. Massachusetts mandates the use of encryption "to the extent technically feasible."[10] It also calls for development of a comprehensive written security program and other specific measures.[11] The Massachusetts regulation became effective March 1, 2010.

In light of this trend towards stronger protections for PII, and particularly employee PII, it is wise for employers in *every* state to implement safeguarding policies and procedures. Employers should identify sensitive information and may want to conduct periodic risk assessments identifying threats and vulnerabilities. The system should be tailored to the

company's needs, depending on the probability and seriousness of potential risks, the company's size and capabilities, the sensitivity of the information to be protected, and the costs of the security measures. The protective measures in place should be consistently monitored and updated to react to new threats—and new laws.

As a practical reality, employers need the cooperation of employees to keep PII safe. Employers should educate their employees on the importance of maintaining data security. Employers should consider developing, and having employees sign, a policy statement explaining that employees should not publicly disclose PII about any other employee and should not remove any PII, whether in print form or on a digital storage device, from the physical workplace. Providing a detailed incident response plan with instructions on whom to notify in the event of a breach will enable employees to respond appropriately. Such policies and procedures should be included in employee handbooks.

Employers should also be judicious in collecting data from employees—only that which is necessary should be collected. Employers should consider providing an "opt out" provision allowing employees to decline to have their contact information published in any type of employee directory. When publishing an employee directory, employers should consider providing the information online in a format that cannot be printed and removed from the office setting. Employers should also obtain the written consent of an employee before using his or her PII for commercial gain, such as in a news article about the company. PII should be destroyed once an employee is no longer associated with the company or once the information is no longer needed by the company.

Creating and implementing these kinds of policies and procedures will help companies avoid costly and embarrassing data breaches. Employers that develop comprehensive data security policies can avoid serious problems down the road. By minimizing the risk associated with a data breach, such policies will help protect employee data, the company's reputation, and its bottom line.

Allegra J. Lawrence-Hardy, a member of Sutherland Asbill & Brennan LLP's Litigation Practice Group and co-leader of the Business and Commercial Litigation team, has extensive experience handling complex multi-party, class action, multi-jurisdictional commercial and labor and employment matters. She has successfully defended primarily Fortune 100 companies throughout the United States and abroad in numerous trials, arbitrations and other forms of alternative dispute resolution.

Jessica S. Wang is an associate in Sutherland's Litigation Practice Group focusing on commercial litigation, education law, and labor and employment law.

The authors thank Katherine Smallwood for her assistance with this article.

---

[1] *See* N.Y. Lab. Law § 203-d.

[2] *Id.*

[3] *See* Conn. Gen. Stat § 42-471.

[4] *See id.*

[5] *Id.*

[6] Cal. Civ. Code § 1798.81.5.

[7] *See id.*

[8] *See* Nev. Rev. Stat. § 603A.

[9] *Id.*

[10] 201 Mass. Code Regs. 17.04.

[11] *See id.*