December 2012

Weil

Employer Update

Privacy Challenges in Drafting BYOD Policies

By Jeffrey S. Klein, Nicholas J. Pappas and Kendra Okposo

Employers realized long ago the benefits derived from providing their employees with smartphones, tablets or other handheld devices. Those benefits include gains in employee productivity and morale, resulting from employees having the flexibility to work from the road or during non-business hours. For many years, employers frequently chose to issue BlackBerry smartphones to their workforces for these reasons. Employers also issued BlackBerry smartphones to their workforces because the BlackBerry allowed employers to retain a high level of control over data access and security.[1] However, since 2009, sales of BlackBerry smartphones have declined dramatically,[2] and more recently BlackBerry usage among businesses has substantially decreased while usage of iPhones and Android-based smartphones is on the rise.[3]

Consistent with these changes in the market for smartphones, employees are increasingly asking their employers that they be excused from using employer-issued mobile devices. Instead, employees overwhelmingly appear to be asking to connect to company email and data networks using their own smartphones. A survey of 3,000 workers reported by McKinsey last summer indicates that 80 percent of smartphones used for work are employee-owned.[4] Employees who choose to use their personal devices for work not only avoid the inconvenience of juggling multiple mobile devices, but also have the benefit of choosing the device that best suits their personal preferences. The trend of employees using their own personal devices to access their employer's email and other data networks has been dubbed "Bring Your Own Device" or "BYOD."

Though BYOD is already a fact of life in numerous workplaces, many employers have not yet modified their policies to address privacy issues arising from employees using their personal mobile devices for business purposes. When employer-issued BlackBerry devices are issued to employees, employers could exercise complete control over the devices, as well as provide security protocols governing when the employer can access the device and erase sensitive data from the device. However, when the employee owns the device, employers must consider whether and how to secure sensitive employer data on mobile devices the employer does not control. How does an employer gain access to an employee's personal device while steering clear of the employee's private information that may also be contained on the device? To what extent is the employer's sensitive data subject to being compromised if the device is lost or stolen? Does the employer have a need to wipe all data from the device to protect the employer's sensitive data, including the employee's photos, contacts and personal

In This Issue

email? These questions raise concerns regarding employer compliance with state and federal privacy laws regarding access to and monitoring of electronic data and communications.

In this article, we examine state and federal privacy laws relevant to BYOD and provide recommendations for employers in crafting policies to address BYOD.

The trend of employees using their own personal devices to access their employer's email and other data networks has been dubbed "Bring Your Own Device" or "BYOD."

Background

Various state and federal laws prohibit unauthorized access to electronic communications and invasion of privacy. Federal law prohibits intentional unauthorized access to employees' personal electronic devices. The Electronic Communications Privacy Act of 1986 (ECPA) was enacted to amend existing wiretap laws to regulate emerging forms of electronic communications. The Stored Communications Act (SCA) contained in Title II of the ECPA, provides that "whoever intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage . . . shall be punished as provided. . . ." 18 U.S.C. § 2701(a)(1). The statute includes a civil action as well as criminal punishment. 18 U.S.C. § 2701(b). However, the SCA permits access to a stored communication when consent is provided by the user. 18 U.S.C. § 2701(c)(2).

New York Penal Law likewise prohibits eavesdropping, defined as "unlawfully engag[ing] in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing electronic communication." New York Penal Law § 250.05 (McKinney 2000). The statute defines "intercepting or accessing electronic communication" as intentionally "acquiring, receiving, collecting, overhearing or recording of an electronic communication without consent from the sender or intended receiver. . . ." New York Penal Law § 250.00(6) (McKinney 2000). Eavesdropping is a Class E felony and may carry a punishment of up to four years in prison.

New York does not recognize a common law right of privacy.[5] However, many other states have adopted a cause of action for intrusion upon seclusion from the Second Restatement of Torts. This cause of action provides civil liability for intentional physical intrusion upon the solitude or seclusion of another. Restatement (Second) of Torts § 652B. The physical intrusion need not be into a person's space or senses. *Id*. It may be an investigation or examination of a person's personal concerns or effects, including electronic devices. *Id*.

In addition, a few states have enacted statutes specifically requiring employers to give notice when monitoring employees' activities on electronic devices. For example, a Delaware statute provides that employers shall not monitor telephone, email, or internet usage unless the employee is given notice every day that these resources are accessed, or the employee acknowledges the relevant policy. 19 Del. C. § 705 (2008). A Connecticut statute requires that employers who engage in electronic monitoring give written notice informing employees that monitoring will occur and post "in a conspicuous place which is readily available for viewing" the types of monitoring which may occur. Conn. Gen. Stat. § 31-48d (2008). New York, Massachusetts and Pennsylvania all have similar legislation pending.[6]

Sitton

Sitton v. Print Direction, Inc., 718 S.E.2d 532 (Ga. Ct. App. 2011) provides one recent example of an employee challenging an employer's access to the employee's personal laptop computer on privacy grounds. Though the *Sitton* case involved an employee-owned laptop computer, the legal issues

addressed by the court certainly may have applicability to employee-owned mobile devices.

In *Sitton*, the plaintiff filed suit against his employer Print Direction Inc., (PDI) after his employment was terminated for conducting a competing business during his employment by PDI. PDI provided employees with a laptop for work related tasks; however Sitton chose to use his own computer to connect to PDI's network and conduct his work. PDI also provided employees with an employee manual which prohibited employees from taking outside jobs with competitors of PDI. During his time at PDI, Sitton brokered more than $150,000 in print jobs for a competing print brokerage business that his wife had started and for which Sitton served as a manager. *Sitton*, 718 S.E.2d at 535. Upon hearing of Sitton's competing business, the president and CEO of PDI, Stanton, entered Sitton's office where Sitton's personal laptop was located. The CEO moved the computer's mouse to find Sitton's emails on the screen, and printed certain emails relating to outside printing companies. The emails were located in a separate email account from Sitton's PDI-issued account, and confirmed Sitton's violations. *Id.* Sitton filed suit alleging computer trespass and invasion of privacy under state law, and invasion of privacy based on unreasonable intrusion upon seclusion under the common law. The trial court entered judgment against Sitton and awarded damages to PDI. Sitton appealed, and the Court of Appeals affirmed the lower court's decision.

Sitton sued under the Georgia Computer Systems Protection Act (OCGA), which provides civil liability and a civil remedy for criminal offenses. Under the OCGA, computer theft, invasion and trespass require that the action be taken "with knowledge," that the use of the computer or examination of another's data was "without authority," and that the actions were taken with the requisite intent to take, obtain or convert personal property, delete data, obstruct or interfere with data or examine any personal data. *Id.* at 535–36.

The court reasoned that Stanton had proper authority to inspect Sitton's personal computer pursuant to the computer usage policy located in PDI's employee manual. The policy was not limited to PDI-owned equipment; it allowed PDI to inspect contents of electronic devices in the course of an investigation triggered by indications of unacceptable behavior. *Id.*

Sitton also sued PDI for common law invasion of privacy, alleging unreasonable intrusion upon his seclusion and solitude and unreasonable intrusion into his private affairs. In order to prove unreasonable intrusion, a plaintiff must show a "physical intrusion." A plaintiff can show "physical intrusion" by demonstrating that the employer-defendant monitored the plaintiff's activities or conducted surveillance. *Id.* at 537. The court concluded that no such intrusion took place because, even if reviewing Sitton's emails was considered "surveillance," it was reasonable in light of the situation. Stanton acted specifically in response to an investigation of improper employee behavior. *Id.*

Practice Pointers

Employers who choose to implement BYOD programs should carefully craft a BYOD acceptable use policy (the "BYOD Policy") which takes into account privacy concerns under federal and state privacy laws. Ideally, a BYOD Policy should be separate from any existing policy governing use of company-issued devices. The policy should detail security measures the company will take to protect its data, occasions for monitoring and accessing an employee's device, and proper procedures that the employee agrees to take in conjunction with the company if the device is lost or stolen. Most importantly, the BYOD Policy must provide employee consent to employer access and monitoring of the device. While consent to access and monitor an employee's device may be stated expressly in the BYOD Policy, for avoidance of doubt employers may also choose to obtain written acknowledgment from employees stating they have received and understand the Policy.

The BYOD Policy should identify the devices to which it applies. For example, the policy may state that it applies to all "Smartphones including iPhones, Androids, BlackBerry smartphones, Windows phones, and tablets including iPads and

Androids that the employee wishes to use to access employer email or other employer data."

These policy provisions will assist the employer in managing and securing each device. Employers should further specify which operating systems, models or versions of each device are permitted consistent with compatibility with software used by the company. The larger variety of operating systems employees use, the more difficult control and monitoring will be for the employer.

The BYOD Policy should provide that the employee must present any mobile devices to the employer's IT department prior to connecting to the company network, and that the employee consents to the employer installing proper security protocol and necessary office software. The BYOD Policy should also specifically address device security. For example, in order to prevent unauthorized access, the BYOD Policy should specify that devices must be password protected, using a company provided password application. These password applications may require longer, more complex passwords than generally available on smartphones. The BYOD Policy should also provide that if the device is lost or stolen, the employee must notify the company within 24 hours.

Through a carefully crafted BYOD Policy, employers may be able to eliminate any expectation of privacy on employee-owned smartphones used for business purposes. However, employers may decide instead to acknowledge a zone of privacy for employee's personal usage. In such cases, the BYOD Policy may state that employees have a reasonable expectation of privacy on their personal devices, but that the employer nevertheless has the right to monitor or access the device for specified reasons. For example, the employer may access the device "to protect against security risks, investigate employee misconduct, upon need for preservation or notice of discovery, and upon employee breach of contract or termination." The BYOD Policy also should provide that the employer may access the device to remotely wipe data if the device is lost or stolen or if the IT department detects a breach in policy, a virus or any other security threat. The BYOD Policy should state that employers may be required to wipe the entire device if personal and company data are intermingled or the employer detects a security threat and therefore should encourage employees to backup all photos, contacts and personal information on the device. To the extent feasible or desirable, the policy may provide that the employer may endeavor to avoid erasing the employee's non-work related information on the device.

Most importantly, the BYOD Policy must provide employee consent to employer access and monitoring of the device.

The BYOD Policy also should address the nature of the employer data that the employee will be permitted to access using the employee's personal device. For example, the BYOD Policy may state that employees will not download sensitive or privileged data onto their personal devices unless the data is downloaded into a company-provided folder or email box. The policy should specify the extent to which the employer's IT department will be available to support the employee's use of the personal device. The policy also should state that the company will not be responsible for lost or damaged personal data as a result of company services, applications or downloaded information. This policy provision not only allows an employer to secure data but also allows employers efficiently to locate sensitive or relevant data on an employee's personal device when necessary. A release regarding IT support would be a prudent measure for employers, because third party software and data will often slow speed and decrease space on a personal device.

Published in the New York Law Journal*, Dec. 3, 2012 edition. Reprinted with permission.*

1 Lisa Ellis, *BYOD: From company-issued to employee owned devices*, McKinsey & Company (June 2012), *available at* http://www.mckinsey.com/Search.aspx?q=byod.

2 *BlackBerry's Spectacular Decline*, Royal Pingdom (Sept. 25, 2012), http://royal.pingdom.com/2012/09/25/blackberry-spectacular-decline/ (last visited Nov. 26, 2012).

3 *See* Trevor Mogg, *iPhone overtakes BlackBerry to become top phone for business users*, Digital Trends (Nov. 16, 2011), http://www.digitaltrends.com/mobile/iphone-overtakes-blackberry-to-become-top-phone-for-business-users/ (last visited Nov. 26, 2012); *see also* Alan Cohen, *Am Law Tech Survey 2012: Both Sides Now*, Corporate Counsel (Nov. 5, 2012), http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1352632492788&Am_Law_Tech_Survey_2012_Both_Sides_Now&slreturn=20121026154245 (last visited Nov. 26, 2012); *see also The BlackBerry as Black Sheep*, NY Times (Oct. 15, 2012), *available at* http://www.nytimes.com/2012/10/16/technology/blackberry-becomes-a-source-of-shame-for-users.html?_r=0.

4 *See* Ellis, *supra* note 1.

5 *See Stephano v. News Group Publications, Inc.*, 474 N.E.2d 580, 584 (N.Y. 1984).

6 *See* H.R. 1862, 2009, Gen. Assem. (Mass. 2009) (Massachusetts bill calling for written general and specific notice to all employees potentially effected by employer monitoring); S. 363. 2009, Gen. Assem. (Pa. 2009), § 2(b) (Pennsylvania bill providing that any employer who engages in electronic monitoring without having provided the employee with notice is liable to the employee for relief); A. 3871, 2009-2010, Reg. Sess. (N.Y. 2009) (New York bill requires employers to provide written notice of monitoring to employees upon hiring, and once each year, informing employees of the types of monitoring which may occur).

Holiday Party Checklist

By Jeffrey Klein and Nicholas Pappas

A Checklist to help employers avoid legal risks presented by employer-sponsored holiday parties.

The festive atmosphere combined with the consumption of alcohol at a holiday office party make it a potential venue for inappropriate behavior and may lead to employee or third party claims based on injuries suffered during or after the event. In planning their holiday parties, employers should take steps to:

- Prevent sexual harassment;
- Avoid harms related to intoxication;
- Minimize the risk of workers' compensation liability;
- Prevent wage and hour violations.

Prevent Sexual Harassment

Employers have an obligation to prevent and respond to claims of sexual harassment. Sexual harassment is defined by the Equal Employment Opportunities Commission (EEOC) as unwelcome sexual advances, requests for sexual favors and other sexual conduct when submission to or rejection of the conduct:

- Affects an individual's employment;
- Unreasonably interferes with an individual's work performance;
- Creates an intimidating, hostile or offensive work environment.

For more information, see the EEOC website (http://www.eeoc.gov/facts/fs-sex.html).

Complaints of sexual harassment arising out of employer-sponsored holiday parties occur with predictable regularity. To reduce legal risks arising from such complaints, employers may wish to:

- *Ensure that human resources policies address employer-sponsored social functions.* Employers may wish to amend their harassment policies to specifically address employer-sponsored social events. In particular, employers may wish to provide specific examples of conduct at holiday parties that is unacceptable. For instance, the policy may remind employees that risqué or adult-themed gifts should not be exchanged with co-workers.
- *Keep holiday customs appropriate to the workplace.* In planning a company-sponsored holiday party, employers should avoid including customs that have the potential to could create romantic or sexually charged situations, such as hanging mistletoe.
- *Consider allowing guests to attend.* Although the addition

of guests raises the cost of a holiday event, employees may be more reserved and less likely to engage in offensive behavior when accompanied by their significant others or surrounded by unfamiliar faces.

Avoid Harms Related to Alcohol Consumption

Holiday parties often are associated with the excessive consumption of alcohol. Intoxicated employees leaving company-sponsored functions may be involved in automobile accidents or other harmful events for which employers may be held accountable under some states' laws, depending on the facts and circumstances. While an employer's potential liability for injuries caused by employees who consume alcohol at company functions varies from state to state, possible theories of liability include:

- common law theories of negligence;
- respondeat superior, which holds employers responsible for the acts of employees undertaken in the course of their employment; and
- social host or Dram Shop liability, which holds the provider of alcoholic beverages to visibly intoxicated individuals liable for injuries those individuals may cause while intoxicated.

Social host and Dram Shop laws vary from state to state. Although some states provide clear statutory grounds on which employers may be liable under those laws, other states:

- limit Dram Shop liability to commercial vendors of alcohol; or
- limit Dram Shop and social host liability to those who provide alcohol to minors.

If, despite the risks, employers choose to sponsor holiday parties at which alcohol is served, employers should take steps to reduce the risk of accidents resulting from the irresponsible consumption of alcohol. For example, employers may wish to:

- *Hold the event at a restaurant or other off-site location.* Employers may wish to hold holiday events at restaurants or other establishments with a liquor license and where alcohol is served by professional bartenders who know how to respond when guests may be consuming alcohol to excess.
- *Hire a professional bartender or caterer for on-site events.* If the event is being held on the employer's premises, the employer should consider hiring a professional bartender or caterer to serve any alcoholic beverages. The employer may wish to confirm that the caterer carries liability insurance. The employer also may wish to instruct bartenders or wait staff not to serve drinks to anyone who is visibly intoxicated. Employees should not be permitted to stand in as bartenders or otherwise serve drinks to coworkers.
- *Limit the amount of alcohol that will be served*. Employers may endeavor to control alcohol consumption by providing a limited number of drink tickets or limiting the time during which alcohol will be served. Other options include scheduling the party for earlier in the day, when it is more socially acceptable not to drink and employees may be less likely to drink to excess, and providing entertainment to shift the focus of the event away from alcohol to something else. In any event, employers should make a variety of non-alcoholic beverages and food available as an alternative to alcoholic beverages.
- *Provide alternative transportation.* Employers should consider implementing a transportation system for employees leaving employer-sponsored events at which alcohol is served.
- *Encourage employees to look out for co-workers who may be intoxicated.* All employees should be encouraged to notify management if another employee appears overly intoxicated. Employers may consider having certain employees designated as "spotters" to look out for colleagues who may have had

too much to drink, although employers should be careful not to designate employees for this role who may be non-exempt from the Fair Labor Standards Act (FLSA) to avoid claims that they were required to work off the clock and therefore are entitled to additional compensation. (See below, Prevent Wage and Hour Violations.)

- *Determine whether the company is insured.* Employers particularly concerned about liability risks and willing to invest in prevention may purchase insurance covering Dram Shop or liquor law liability in states that recognize those causes of action. Review existing coverage before purchasing a new policy because a company's comprehensive general liability may provide sufficient coverage.

Minimize the Risk of Workers' Compensation Liability

Workers' compensation insurance is mandated coverage that provides payment to employees who experience a job-related injury or illness. Although the law varies from state to state, workers' compensation benefits may be available to employees who are injured during, or because of, an employer-sponsored event, depending on the facts and circumstances. Holiday parties tend to lower inhibitions, increase alcohol consumption and raise the risk of injury. To reduce the potential risk of workers' compensation liability associated with such functions, employers should disassociate the event from employees' jobs by:

- letting employees know that there is no business purpose for the event and attendance is not mandatory; and
- hosting events off employer premises.
- inform employees that attendance at the party is purely voluntary;
- hold the party outside normal business hours;
- refrain from making speeches about business matters or distributing bonuses or performance awards at the party; and
- avoid asking employees who may be non-exempt from the FLSA to perform any specific functions at the party for the benefit of the employer to avoid claims that such employees were required to work off the clock.

Employer Update is published by the Employment Litigation Practice Group and the Executive Compensation and Employee Benefits Practice Group of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

Editors

Lawrence J. Baer	lawrence.baer@weil.com	+ 1 212 310 8334
Allan Dinkoff	allan.dinkoff@weil.com	+ 1 212 310 6771

Practice Group Contacts

Jeffrey S. Klein
Practice Group Leader
New York
+1 212 310 8790
jeffrey.klein@weil.com

Boston
Thomas C. Frongillo
+1 617 772 8335
thomas.frongillo@weil.com

Dallas
Yvette Ostolaza
+1 214 746 7805
yvette.ostolaza@weil.com

Michelle Hartmann
+1 214 746 7847
michelle.hartmann@weil.com

Frankfurt
Stephan Grauke
+49 69 21659 651
stephan.grauke@weil.com

Houston
Melanie Gray
+1 713 546 5045
melanie.gray@weil.com

London
Joanne Etherton
+44 20 7903 1307
joanne.etherton@weil.com

Ivor Gwilliams
+44 20 7903 1423
ivor.gwilliams@weil.com

Miami
Edward Soto
+1 305 577 3177
edward.soto@weil.com

New York
Lawrence J. Baer
+1 212 310 8334
lawrence.baer@weil.com

Allan Dinkoff
+1 212 310 6771
allan.dinkoff@weil.com

Gary D. Friedman
+1 212 310 8963
gary.friedman@weil.com

Michael K. Kam
+1 212 310 8240
michael.kam@weil.com

Steven M. Margolis
+1 212 310 8124
steven.margolis@weil.com

Michael Nissan
+1 212 310 8169
michael.nissan@weil.com

Nicholas J. Pappas
+1 212 310 8669
nicholas.pappas@weil.com

Shanghai
Helen Jiang
+86 21 3217 9511
helen.jiang@weil.com

Washington, DC
Michael Lyle
+1 202 682 7157
michael.lyle@weil.com