Bring Your Own Device—Challenges and Solutions for the Mobile Workplace

Kevin J. Smith and Shira Forman

Technological advances in the workplace often introduce new levels of convenience—and a whole new world of legal concerns. This is true for the growing phenomenon known as "bring your own device." "Bring your own device," or BYOD, refers to the corporate trend in which employers allow, and sometimes encourage, employees to use their personal electronic devices (laptops, smartphones, tablets, etc.) to engage in work tasks. According to a recent survey, 38 percent of companies expect to stop providing electronic devices to their employees by 2016.[1] This means that in the coming years, as employees' personal electronic devices become their work devices, many employers will face the challenge of creating BYOD policies that address complex issues such as data privacy, ownership of information, employee use of social media, and tracking of employee work hours.

This Questions—And Answers column reviews some of the legal and policy issues surrounding the BYOD movement and suggests ways for employers to draft effective, forward-looking BYOD policies.

WHAT ARE SOME OF THE ADVANTAGES AND DISADVANTAGES OF ESTABLISHING A BYOD WORKPLACE?

By permitting employees to carry one device instead of two or more, and by offering employees the ability to select the device that is most comfortable and appealing to them, a BYOD policy has the potential to increase employee satisfaction. In addition,

© 2014 Wiley Periodicals, Inc.
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/ert.21436

the freedom to work on their own devices has the potential to increase employees' productivity. There is also obvious cost-efficiency to having employees purchase their own devices, even if employers underwrite a portion of the purchase.

Among the possible downsides to the BYOD trend is the added security risk associated with allowing employees to easily access company data outside the workplace. This includes concerns about the dissemination of trade secrets, the sharing of sensitive information with friends and family, and the potential for devices containing private information to get lost or stolen. Additionally, employers that permit the use of personal devices for work have to be sure that employees do not develop unrealistic expectations of privacy with respect to the personal information stored in their devices. BYOD policies also present challenges for an employer's information technology department, which must provide support for various types of devices instead of one standard device used by all employees across the company.

DOES ALLOWING EMPLOYEES TO USE THEIR OWN DEVICES FOR WORK RAISE ANY CONCERNS REGARDING COMPLIANCE WITH WAGE-AND-HOUR REGULATIONS?

The Fair Labor Standards Act (FLSA) requires employers to pay all nonexempt employees at least minimum wage for all compensable time worked, and overtime pay at a rate of not less than one-and-a-half times their regular rate of pay for time worked over 40 hours in a workweek.[2] Employers are required to keep records of the hours worked and wages earned by all nonexempt employees.

Any scenario in which employees can perform work-related tasks after official work hours is ripe for wage-and-hour violations. For example, in recording time worked under the FLSA, insignificant or "de minimus" periods of time beyond the scheduled working hours are not required to be documented. When employees use mobile devices to perform tasks like checking e-mail or listening to voice messages after hours, it can be difficult to determine the point at which these tasks go beyond "de minimus" and begin to constitute compensable time.

Recently, a conditional class of nonexempt retail workers sought to certify a FLSA class action against their employer, alleging in part that they were required to review and respond to company e-mails and text messages even when they were not "punched in" to their employer's timekeeping system.[3] The US District Court for the Southern District of New York decertified the class in part because the plaintiffs' claims regarding off-duty communications varied too widely to "conclude that [the defendant] had any uniform

business practices or 'culture' across its 2,000-plus retail stores encouraging off-duty electronic communication."[4] Notwithstanding that ultimate result, the case is a reminder that, as after-hours communication via electronic devices becomes the norm, employers must ensure that employees record and report their time accurately and are compensated appropriately.

In a company using BYOD, there is also the possibility that round-the-clock access to the virtual workplace will tempt employees to work overtime without permission. Employers should make clear in their BYOD policies that employees may not work overtime on their personal devices without prior authorization from a supervisor.

WHAT PRIVACY ISSUES SHOULD EMPLOYERS CONSIDER WHEN IMPLEMENTING A BYOD POLICY?

Courts have generally taken the approach that there is no reasonable expectation of privacy in communications voluntarily sent by an employee over an employer's computer system.[5] However, when an employer accesses communications sent by an employee on his or her own device, there is a stronger argument that such access may constitute an invasion of the employee's privacy.

The Computer Fraud and Abuse Act (CFAA), a federal law that prohibits the unauthorized access of computer data, has been the basis of many lawsuits by employers who claim that their employees or former employees unlawfully obtained confidential company data or trade secrets. In the BYOD context, employees could claim that employers who access "private" information on employees' personal devices have run afoul of the CFAA.[6] In crafting BYOD policies, employers should make clear to employees that the employer reserves the right to monitor all employee communications that are sent over the employer's network.

DOES EMPLOYEES' USE OF THEIR OWN DEVICES AT WORK RAISE CONCERNS REGARDING COMPLIANCE WITH EQUAL EMPLOYMENT OPPORTUNITY (EEO) POLICIES?

In a recent sexual harassment lawsuit in Puerto Rico federal district court, female employees alleged that they were subjected to a hostile work environment that included, among other things, their male manager showing them photographs of naked people on his cell phone. Numerous other recent discrimination and harassment lawsuits have included claims by employees that they were sent explicit text messages by colleagues or superiors when using their personal electronic devices.

These cases illustrate the extent to which e-mail, text messages, and social media have become conduits for the distribution of inappropriate and harassing content in the workplace. As the BYOD trend grants employees increased access to their personal e-mail accounts and other external content, and blurs lines between work and private life, employers must be vigilant about updating and enforcing their antidiscrimination and antiharassment policies. Employees should be reminded that they are prohibited from using their personal devices to send or display content in violation of the company's EEO policies.

IF A FORMER EMPLOYEE RETAINS TRADE SECRETS OR CONFIDENTIAL CLIENT INFORMATION ON A PERSONAL DEVICE, CAN THE EMPLOYER DEMAND THAT THE EMPLOYEE TURN OVER THE DEVICE?

Long before the BYOD movement, employers have had to deal with the problem of employees taking trade secrets, client lists, and other valuable information with them when they transition to new employment. The BYOD trend brings new dimensions to this area of concern, as demonstrated by a recent New York state appellate court decision.[7] The case involved an investment firm that sued its former analyst, alleging that when the analyst left the firm, he breached his employment contract by misappropriating the firm's confidential information, including client contact lists, and used them to solicit former clients on behalf of his new employer.

During discovery in the case, it was revealed that while the analyst worked for the firm, he had used his personal iPhone to call clients. The firm served a document request including a demand for the defendant's iPhone call logs from the time he left the firm. Over the defendant's objection, the court issued an order requiring him to produce his iPhone to the plaintiff. The appeals court reversed the order, holding that requiring production of the entire iPhone was too invasive. The court directed that the iPhone be reviewed *in camera* to ensure that only relevant, nonprivileged information would be disclosed. It reasoned, "[O]rdering production of defendant's iPhone, which has built-in applications and Internet access, is tantamount to ordering the production of his computer. The iPhone would disclose irrelevant information that might include privileged communications or confidential information."

The court's decision highlights the difficulty involved in balancing employee privacy rights with the need to protect company data, as well as the importance of including in every BYOD policy requirements with respect to the retrieval of company data upon an employee's separation from employment.

HOW DOES BYOD AFFECT THE DISCOVERY PROCESS WHEN AN EMPLOYER IS INVOLVED IN LITIGATION?

Discovery requests in litigation generally demand that a litigant produce all responsive data that is within its control. When an employee's personal device contains data that is responsive to discovery requests, employers are faced with questions about whether they are required—and permitted—to search their employees' devices for responsive data.

Courts are generally reluctant to require the production of personal data on employees' personal devices unless there is a compelling need to do so. For example, in a recent New York federal district court case, an employer anticipated being sued by a female employee for discrimination.[8] In investigating the employee's complaints, the employer learned that a male employee who was present for the challenged conduct had communicated with the complainant via his personal cell phone. The male employee refused to turn over his cell phone to the employer or to have its data backed up, so the employer asked the court to order him to turn it over, for fear that he would erase its contents. The court refused, finding that generalized concern that an employee might destroy evidence was not a compelling enough reason to require the phone to be turned over before the litigation even commenced.

In a recent class action alleging in part that employees were denied federally required meal periods, an employer asked the court to compel the opt-in plaintiffs to produce all evidence of social media activity during the plaintiffs' working hours on the theory that time spent by a plaintiff on social media posts would be excluded from the compensable time of that opt-in plaintiff. The court denied the request as overly broad and reasoned that "whether or not an opt-in Plaintiff made a Facebook post during work may have no bearing on whether or not the opt-in plaintiff received a bona fide meal period."[9]

Not all decisions, however, are protective of the data on employees' personal devices. The Securities and Exchange Commission recently censured and fined a broker dealer for failing to preserve and produce requested data, including the personal e-mail and personal computer of an independent contractor for the company who had used his personal e-mail to send work-related communications.[10]

WHAT SHOULD EMPLOYERS INCLUDE IN THEIR BYOD POLICIES?

Although every employer should have a written BYOD policy that is tailored to the specific circumstances of its workplace, all employers should consider including the following:

 DOI 10.1002/ert

- ❏ Guidelines regarding which brands and/or models of devices are acceptable for use under the policy;
- ❏ Information regarding who will pay for the device (employer or employee); who will pay for a replacement if the device is damaged, lost, or stolen; and who will pay for the service plan on the device;
- ❏ Information regarding what happens to an employee's device on his or her separation from the company;
- ❏ A requirement that all employees have their devices configured by the employer's information technology department, which can ensure that devices contain the proper security software and applications;
- ❏ A requirement that all employees secure their devices with passwords and that the passwords be changed periodically (e.g., every 90 days); and
- ❏ A requirement that personal devices be set to lock after a certain period of inactivity.

In addition, the policy should inform employees that they:

- ❏ Are required to consent to searches of their devices' content during internal and external investigations and to provide access to the devices should their content be subpoenaed or requested during the discovery phase of a litigation;
- ❏ Are prohibited from storing any company data on cloud-based sharing sites or services, which have been shown to be vulnerable to hacking;
- ❏ Are required to consent to the complete wiping of their devices if the devices are reported lost or stolen;
- ❏ Are required to regularly back up all personal data that is stored on their devices and that the employer is not responsible for the loss of their personal data should their devices require wiping;
- ❏ Should not have an expectation of privacy in the content stored on their devices except to the extent provided by law, and that the employer has the right to monitor any communications that utilize its networks; and
- ❏ Are prohibited from sending work communications over their personal e-mail accounts.

NOTES

1. Wills, D. A. (2013, April 11). Bring your own device: The facts and the future. Gartner Research. Retrieved from http://www.gartner.com/DisplayDocument?id=2422315&ref=clientFriendlyUrl.
2. The Fair Labor Standards Act of 1938, as amended, 29 U.S.C. § 201, et seq.
3. Zivali, et al. v. AT&T Mobility, LLC, 784 F.Supp.2d 456 (S.D.N.Y. 2011).
4. Ibid., at 466.

5. See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); Garrity v. John Hancock Mutual Life Co., 2002 WL 974676 (D.Mass. May 7, 2002).
6. Green, M. Z. (2012). Against employer dumpster-diving for email. South Carolina Law Review, 64, 323, 348.
7. AllianceBernstein L.P. v. Atha, 2012 NY Slip Op 07766, 100 A.D.3d 499 (1st Dep't Dec. 26, 2012).
8. In re Petition of John W. Danforth Grp., Inc., 13-MC-33S, 2013 WL 3324017 (W.D.N.Y. July 1, 2013).
9. Jewell et al. v. Aaron's, Inc., 1;12-CV-0563-AT, 2013 WL 3770837, *4 (N.D. Geo. Jul. 19, 2013).
10. In the Matter of vFinance Investments, Inc., SEC Admin. Proc. File No. 3-12918 (2010).

Kevin J. Smith *is special counsel at Sheppard, Mullin, Richter & Hampton LLP in the firm's Labor and Employment group. He has extensive experience in employment litigation, including trials and appeals in federal and state courts, and conducting arbitrations and administrative hearings. His employment law practice also includes counseling Fortune 500 companies in all types of employment and labor law matters. He may be contacted at kjsmith@sheppardmullin .com.* ***Shira Forman*** *is a labor and employment associate in the New York office of Sheppard Mullin Richter & Hampton LLP. Her practice is devoted to representing employers in employment-related matters, and she regularly counsels employers on compliance with federal and state labor and employment issues. She can be contacted at sforman@ sheppardmullin.com.*