Bloomberg BNA

BNA's
Corporate Counsel Weekly™

Reproduced with permission from Corporate Counsel Weekly Newsletter, 30 CCW 11, 03/18/2015.
Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Internal Investigations and Data Security in a Bring-Your-Own-Device Company

HOLLY H. WEISS AND
MICHAEL L. YAEGER

As cell phones have become smartphones, employees have gained 24/7 access to a tremendous amount of company information. And as the Bring-Your-Own-Device (''BYOD'') trend has spread, so has the risk that companies will lose control of that information.

In a BYOD company, employees own the mobile devices that they use for work. Company information is therefore being transmitted to and from, and stored on, devices that the company does not own. Further, because many employees choose to avoid the ''two-pocket'' problem by having only one smartphone or laptop, they engage in both business and personal activities on the same device.

Left unaddressed, these two facts—employee ownership and dual use—could severely hamper companies' ability to protect their data and conduct internal investigations. Companies should therefore draft their information security policies with special attention to the ways that BYOD practices create security risks and affect investigations.

The Backdrop

Imagine that an employee is suspected of misconduct—anything ranging from theft of trade secrets to sexual harassment. Or assume that a company is concerned that a hacker has gained access to and infected an employee's device.

A company in these situations will want to examine the employee's devices for evidence.

To that end, the company will also want to copy (or ''image'') the devices. Forensic examinations of computers can take weeks, and it is usually not obvious where all relevant evidence might be found, especially when the investigation just begins. Nor is it obvious what personal information on a device will be irrelevant to an investigation.

When a company owns the devices on which employees work, it can be confident in its legal rights to take these normal investigative steps. In general, a company can secure, study or erase data stored on devices or systems that it owns if it puts employees on notice of its powers and intentions.[1]

But an employer has far less control over an employee's own device.[2] Authority over a computer comes from ownership, and without authorization, access can constitute trespass.

Holly H. Weiss (holly.weiss@srz.com), a partner in the Employment & Employee Benefits Group at Schulte Roth & Zabel LLP, focuses her practice on the representation of employers in all aspects of employment law and employee relations. She advises employers on employment law compliance, best practices, human resources matters, hiring and termination, and litigation avoidance, litigates employment disputes, drafts and negotiates employment agreements, separation agreements and other employment-related agreements, provides training, and conducts investigations.

Michael L. Yaeger (michael.yaeger@srz.com), a special counsel in the Litigation Group of Schulte Roth & Zabel LLP, focuses on white-collar criminal defense and investigations, securities enforcement, internal investigations, accounting fraud, cybercrime and data security matters, as well as related civil litigation. While serving as an Assistant U.S. Attorney in the Eastern District of New York, he was the co-coordinator for Computer Hacking and Intellectual Property crimes.

[1] *See, e.g., United States v. Simons*, 206 F.3d 392 (4th Cir. 2000); *Muick v. Genayre Elec.s*, 280 F.3d 741 (7th Cir. 2002); *United States v. King*, 509 F.3d 1338 (11th Cir. 2007); *In re Info. Mgmt. Servs., Inc. Derivative Litig.*, 81 A.3d 278, 294 (Del. Ch. 2013).

[2] *Cf. Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (finding that employee had a reasonable expectation of privacy, even though he had not only accessed those accounts on employer-owned equipment but had also saved his password and login there, enabling one-click account entry by anyone who could turn on the computer); *State v. Granville*, 423 S.W.3d 399, 402 (Tex. Crim. App. 2014), *reh'g denied* (April 2, 2014) (high school student did not lose his legitimate expectation of privacy in his cell phone simply because it was being stored in the jail property room after he had been arrested for a Class C misdemeanor); *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, 637-38 (Tex. App. 1984) (finding expectation of privacy when employee provided own lock to secure employer-owned locker).

COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0886-0475

This latter principle is enforced on both the federal and state levels through criminal and civil law. The Stored Communications Act makes it a federal crime to ''intentionally access without authorization a facility through which an electronic communication service''—such as email or chat—is provided.[3]

The Computer Fraud and Abuse Act (CFAA) makes it a federal crime to intentionally gain unauthorized access to, or exceed authorized access to, a ''protected'' computer.[4] (As a practical matter, almost any computer is a protected computer under the statute because protected computers include those merely ''affecting interstate or foreign commerce.''[5]) The CFAA also provides for private rights of action when the unauthorized access or exceeded access causes more than $5,000 in damages.[6] All 50 states have similar laws, which function as computer trespass statutes.[7]

In short, a BYOD company will have no authority to obtain or search an employee's phone if it has not previously obtained the employee's consent to do so. Moreover, employees are far less likely to grant such consent when they know they are under investigation or after their employment has been terminated. In this area, rapid response will not substitute for careful planning.

[3] 18 U.S.C. § 2701 (a)(1).

[4] 18 U.S.C. § 1030 (e)(2).

[5] ''The phrase 'affecting interstate commerce' is a term of art that signals congressional intent to cover as far as the Commerce Clause will allow.'' Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1570 (2010).

[6] 18 U.S.C. § 1030(g).

[7] *See* Computer Crime Statutes, Nat'l Conference of State Legislatures, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (last visited Feb. 23, 2015).

Elements of a BYOD Policy

Companies' needs are different, and policies should be tailored with those needs in mind, but in our experience, including the following items make sense for most companies:

Restrictions. A comprehensive BYOD policy should include provisions regarding password protection, encryption of company data that is stored on the device, locking or wiping after a certain number of unsuccessful access attempts, restrictions on the source of apps (e.g., only Apple or Google), no friends or family access, and no storage of corporate data on remote servers through consumer-grade ''cloud'' storage services. If a company chooses to use cloud storage, it should carefully select an enterprise-grade provider that provides better security, as well as the ability to monitor and wipe what an employee has stored. Companies should also require immediate reporting of lost or stolen devices.

Monitoring. Companies should alert their employees that they have no expectation of privacy in company data on the device or in personal data transmitted over the company's systems (e.g., company e-mail). Companies should obtain consent to monitor data that is stored, sent from or received on the device; companies should obtain consent to remotely wipe corporate information if the device is lost or stolen and upon termination of employment; and companies should obtain prior consent from employees to image all of the data on their device in the event of an actual or reasonably suspected security breach, or in response to a subpoena, court order, discovery request, audit or suspected misconduct.

Coordination with Other HR Policies. Companies should ensure that BYOD policies do not conflict with other HR policies and specify that any other policies such as equal employment opportunity, anti-harassment, confidentiality and compliance policies apply to work performed on the device.

Provisions Contemplating Termination of Employment. Security issues are most acute upon termination of employment. Remote-wiping capabilities are especially important in this circumstance. As noted above, companies should therefore obtain prior permission to wipe a device of company information. To this end, companies should also obtain consent to install mobile management software that gives them remote wiping capability.

Using a corporate cloud service and setting up a corporate ''sandbox'' for employees to use helps to preserve the integrity of company information, but will not capture all company data if some continues to be stored on the device itself. Companies should therefore require employees to consent to an inspection of the device during and upon termination of employment.

Compliance with Recordkeeping Obligations. Whether a company has a recordkeeping obligation depends on the content of the communication rather than the platform used to communicate. For example, if text messages include communications that relate to recommendations or advice by a registered investment adviser, they are subject to the recordkeeping obligations under Rule 204-2 of the Investment Advisers Act.[8] Companies should make sure that they have access to and maintain all information that is subject to recordkeeping obligations. In addition, policies should allow for retrieval of employee-owned devices for compliance-related inquiries.

Conclusion

When a company does not own a device, it must take special steps to exercise control of that device. Companies should therefore review their existing policies and procedures to determine if any updates are necessary to account for the ways that BYOD practices create security risks and affect investigations.

[8] The Office of Compliance Inspections and Examinations, *Investment Adviser Use of Social Media*, National Examination Risk Alert, Jan. 4, 2012 at 2; see 17 C.F.R. § 275.204-2.

COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC.
CCW ISSN 0886-0475