Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Employers Must Obtain Employee Consent For BYOD Programs

Law360, New York (May 24, 2013, 11:12 AM ET) -- As employers continue to roll out "bring your own device" programs, they should carefully consider how to handle the privacy and data security law implications of their conduct.

Thirty-eight percent of chief information officers told Gartner that their organizations will stop providing company-issued laptops, smartphones and tablets to workers by 2016, according to a report released this month. Instead, these employers will require workers to participate in BYOD programs and use their personal devices to access work email and apps. BYOD offers employees increased flexibility to use devices of their choice, and it helps employers reduce information technology costs.

But BYOD also presents novel privacy and data security challenges. To protect sensitive information, many employers must access their employees' personal devices and remotely wipe devices that are lost or stolen. In many cases, such conduct can violate federal and state computer hacking laws, unless the employer has obtained clear and unambiguous consent from the employee.

Obtaining employee consent can be a tricky balancing act. The employee notifications must be comprehensive enough to comply with federal and state anti-hacking laws. But when employers broadly reserve the right to access or monitor personal devices, they may discourage some employees from participating in BYOD programs.

In this article, we assess the legal risks for companies that access their employees' personal mobile devices, and we suggest guidelines for developing BYOD policies that comply with federal and state laws.

The largest legal risk to employers comes from the federal Computer Fraud and Abuse Act and similar state laws. The CFAA imposes criminal and civil penalties on individuals and companies that "intentionally access a computer without authorization or exceed authorization" to obtain "information from any protected computer." The statute also prohibits individuals and companies from "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."

Not all courts have made determinations as to whether smartphones are "protected computers" that are covered by the CFAA, so, particularly for organizations that have a presence in multiple jurisdictions, a prudent and cautious approach is to assume that the statute may cover smartphones. If so, employers cannot access information on their employees' smartphones or remotely wipe data from the devices unless they have obtained appropriate authorization from employees. This authorization typically must come in the form of consent that the employee provides when signing up for the BYOD program.

Many employers, understandably, are concerned that a request for consent could discourage employees from participating in BYOD programs. After all, employees do not want to provide their employers with the ability to monitor their personal smartphone use. At the same time, however, employers must ensure that they have sufficient authorization to securely offer BYOD access. The following are some guidelines that we suggest employers consider when developing their BYOD policies:

1) Require employees to provide affirmative consent.

Some employers may want to merely add a BYOD policy to the employee handbook, rather than require each employee to agree to that policy. This may not constitute sufficient authorization under the CFAA and similar state laws. The employee should provide explicit and affirmative consent to the BYOD policy, either by signing a form or clicking "I agree" to an electronic policy. (Courts have not stated whether CFAA consent must be written, electronic, or verbal, but federal law states that an electronic signature has the same legal effect as a written one.).

2) Maintain records of that consent.

Employers should permanently retain either the signed written consent or the records of each electronic consent and be able to produce them if needed.

3) Determine when you may need to view personal content.

Employees understandably want assurances that their personal content will not be accessed or monitored. Unfortunately, that is not always possible from a technical or human resources perspective. For example, if an employee's work email account is not functioning properly, the employer's IT department may not be able to provide technical support without viewing some personal content. Moreover, some employers may want the ability to inspect a BYOD device upon an employee's departure from the company to ensure that the device does not contain any sensitive or proprietary data. Employers should consult with their IT and HR departments to determine when they might need to access personal content, and the consent should incorporate those scenarios.

4) Consider whether remote wiping could damage personal content.

Employers likely want to delete all of their data from an employee's personal device if the device is stolen or if the employee leaves the organization. On some devices, remotely wiping the employer's data also may affect, damage or delete personal content. The CFAA not only prohibits unauthorized access; it also prohibits unauthorized damage of files on protected computers. Thus, the consent form should anticipate the possibility that some data may be damaged.

5) Use clear and direct language.

Some employers may be tempted to draft BYOD consent language with vague language. This approach can be fraught. First, employees usually will spot hidden loopholes. And more importantly, if the policy is vague, a court is more likely to find that it did not constitute sufficient consent to access the device.

For example, consider an employer that has determined that it may be necessary to view personal content only in a few specific situations. Instead of stating, "We aim to avoid viewing the content on your device," the policy should be more specific. Instead, it could state, "We reserve the right to access the personal content on your device use in the following situations: (1) to assist in an internal investigation, (2) if your device has been stolen, (3) if required by a court order or other valid legal process, (4) if your device requires technical support."

6) When in doubt, choose broader language.

The CFAA not only prohibits unauthorized access to computers; it also prohibits companies and individuals from exceeding authorized access. Thus, if you believe that there is a reasonable chance that you will need to access or remotely wipe a device for a particular reason, you should include that scenario in the BYOD consent.

BYOD presents tremendous opportunities to increase productivity and satisfy growing employee demand to access both work and personal email on one device. But it also presents a number of technical, security, and legal challenges that employers must address. To address these challenges, an employer's legal, information technology and human resources departments should collaborate and determine the nature and scope of the consent that they will need to obtain from employees.

--By Yaron Dori and Jeff Kosseff, Covington & Burling LLP

Yaron Dori is a partner and Jeff Kosseff is an associate in Covington & Burling's privacy and data security practice in Washington, D.C.