Employee Use of Dual-Purpose Electronic Devices: Legal Threats for Employers

Protecting Employer Interests When Smartphones, Tablets and Laptops Are Used for Personal and Work Purposes

TUESDAY, SEPTEMBER 13, 2011
1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:

Margaret A. Keane, Partner, Dewey & LeBoeuf, Silicon Valley, Calif.
Philip L. Gordon, Shareholder, Littler Mendelson, Denver

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Managing the Privacy and Security Risks Inherent In Employees’ Use of Personal Smartphones and Tablets for Work

BY PHILIP L. GORDON

The lines snaking from the front door of almost every Apple store are symptomatic of a critical privacy and information security challenge that U.S. employers are now confronting. Employees are willing to spend their disposable income on hand-held devices that are “cooler,” faster, and more sophisticated than company-issued devices, and employees want to use those personal devices for work. While the challenge has been percolating just below the surface for years, the explosive growth of iPads and iPhones has blasted the issue to the forefront for many businesses.

In response, employers are seeking to balance a desire to accommodate employees’ digital preferences against the risks inherent in the use of personal devices for work, such as the potential loss of control over confidential business information and sensitive employee and customer data. As with each major technological shift in the past decade, this one likely will not find its equilibrium for several years. In the meantime, employers seeking to avoid some of the worst-case scenarios—e.g., thwarted workplace investigations, the loss or theft of sensitive data, the misappropriation of trade secrets—should strongly consider a range of measures designed to reduce these risks.

Below are 10 key steps that employers can take before allowing employees to use a personal device for work:

1. Enable Security Measures Selected By the Company: Employees often consider security measures that are standard on company-issued devices to be an inconvenience, and as a result, will not enable those security measures on a personal device. Employers should establish a standard set of security measures that employees must enable before being permitted to use a personal device for work. Such security measures might include, for example, encryption (which would be required for devices on which the personal information of Massachusetts or Nevada residents might be stored), password protection, inactivity timer, and data removal after invalid password entry. Employers also should consider uploading to the personal device enhanced protections against malicious software (to the extent technically feasible), given that personal devices may be used for activities—such as peer-to-peer file shar-
ing, downloading games, and viewing pornography — that increase the risk of infection by malware.

2. Require an Acknowledgement That All Company Policies Apply: As a practical matter, employees likely will feel less constrained to comply with corporate policies when using a personal device for work. Consequently, employers need to remind their workforce members that all company policies apply to their conduct when using a personal device for work. Employers should focus these reminders particularly on their policies for the protection of confidential business information and sensitive employee and customer data as well as on workplace harassment and anti-discrimination policies.

Employers need to remind their workforce members that all company policies apply to their conduct when using a personal device for work.

3. Amend Your Organization’s Electronic Resources Policy to Address Monitoring of Personal Devices: Corporate electronic resources policies commonly speak only in terms of the corporate computer network and company-issued equipment. As a result, a court likely would find that warnings in an electronic resources policy that employees should have no expectation of privacy have no impact on an employee’s privacy expectations with respect to information stored on his or her personal device — even if used for work. Yet, when an employee connects a personal device to the corporate network, that device likely will be subject to the same invasive monitoring practices as company-owned devices, exposing the employer to privacy-based claims. To reduce this risk, the corporate electronic resources policy should be modified to warn employees that the policy applies with equal force to personal devices that are connected to the corporate network.

4. Get Consent to Access the Personal Device for Legitimate Business Purposes: Employers who permit widespread use of personal devices for work almost inevitably will need to access employees’ personal devices during the course of employment. Access may be necessary for a workplace investigation or to implement a litigation hold. Unlike company-issued devices, the employer has no inherent right to access an employee’s personal device, even for a legitimate business purpose. Employers should notify employees up front that their refusal to comply with a reasonable and legitimate request for access to information stored on a personal device that is used for work could result in discipline up to and including termination of employment.

5. Prohibit Use of Personal Accounts to Conduct Company Business: Employers need to understand that permission to use a personal device for work does not mean permission to use a personal account, such as text messaging through the employee’s cell service provider or exchanging e-mail through a personal web-based account. Because the federal Stored Communications Act generally prohibits electronic communications services from disclosing stored communications without the consent of the sender or recipient, an employer could lose access to important business communications and information sent by an employee through a personal third-party service provider. If an outright prohibition is impractical, employees should be warned that the employer may, for legitimate business reasons, ask them to authorize disclosure by their service provider of stored communications and that a failure to comply with that request could result in discipline up through and including termination of employment.

6. Prepare Ahead of Time for a Potential Security Incident: A lost or stolen personal device containing personal information, such as employees’ or customers’ Social Security numbers or credit card numbers, could trigger security breach notification obligations. Requiring that employees activate encryption on a personal device, when available, should eliminate the need for security breach notification because of the “encryption safe harbor” in all security breach notification laws. If encrypting an employee’s personal device is not feasible, the employer should require that the employee allow the employer to install software on the personal device that will wipe the device clean upon the employer’s transmission of a “kill command.” Sending a kill command will not necessarily permit an employer to avoid statutory notification obligations because a sophisticated thief might be able to access personal information on the device before the kill command is activated. However, promptly wiping the device clean should go a long way towards reducing the risk of harm to potentially affected individuals. Employers also should require immediate reporting to their security incident response team of any loss or theft of a personal device used for work. Relatedly, employers should ensure that employees using a personal device for work have the contact information needed to report the loss or theft.

Sending a kill command to an employee’s personal device without the employee’s prior consent runs the risk of violating federal and state law.

7. Limit The Storage of Sensitive Information on Personal Devices: While encryption may prevent unauthorized users from accessing sensitive information on an employee’s personal device, it will not stop family members and friends who know the employee’s password or with whom the employee shares a personal device. Employers can reduce the risk of this type of unauthorized access by, for example, permitting employees to use a personal device only for purposes of accessing corporate e-mail and by requiring that employees perform other business functions involving sensitive information only with a company-issued device. Employers also could consider requiring that employees permit installation of software that creates an “encrypted container” that can store sensitive business information and which has a password that is different from the password used to access the device.

8. Get Consent Before Sending a Kill Command: Although no U.S. court has yet addressed this specific issue, sending a kill command to an employee’s personal device without the employee’s prior consent runs the risk of violating the federal Computer Fraud and Abuse Act and state computer trespass laws. These laws gen-
erally prohibit unauthorized destruction of information stored on someone else’s computer. To avoid potential criminal and civil liability under these statutes, employers should obtain prior written consent to send a kill command to any personal device that is reported lost or stolen.

9. Get a Release Before Sending a Kill Command: Kill commands typically will wipe not only sensitive corporate information but also the employee’s personal collection of music, videos, photographs, books, and more. That collection often will be backed up. If it is not, however, the employer could be facing a significant bill to replace the employee’s electronic library. To avoid such claims, employers should obtain a release from employees for any damage to personal files deleted by a kill command.

10. Think About How Your Organization Will Retrieve Business Information When Employment Ends: Having a cache of confidential business information on a personal device provides one of the easiest vehicles for misappropriating trade secrets. Upon termination of employment, the employee can misappropriate simply by keeping his or her personal device. To reduce this risk, employers should consider incorporating the review of information stored on an employee’s personal device used for work into the standard exit interview process. For hostile partings, sending a kill command may be the only feasible way to prevent misappropriation of trade secrets. However, without the consent and release noted above, those actions could strengthen the hand of a hostile former employee in pending or threatened litigation with the employer.

How can employers implement these steps as a practical matter, particularly the ones likely to be less palatable for employees? Employers can unilaterally implement some of these steps by modifying existing policies or purchasing new technology. The suggestions that require the employee’s prior written consent can be embodied in a “personal device agreement.” As an incentive for employees to enter the agreement and as consideration for the employee’s consent, an employer can offer to reimburse a portion of employees’ monthly cost associated with the personal device or a portion of the purchase price. For employees who are not willing to cede any control over their personal device, employers must consider whether the degree of control that can be gained through unilateral policy changes and technological controls reduces the risks of the employee’s use of a personal device for work to a tolerable level.