Bloomberg BNA

Daily Labor Report®

PRIVACY RIGHTS

Employers may appreciate the ease with which they can reach workers—day or night—via personal electronic devices, but that convenience comes with pitfalls. In this BNA Insights article, attorney Sonya Rosenberg describes some of those risks and lays out proactive solutions to address challenges relevant to employers.

BYOD Challenges and Solutions for the Workplace

BY SONYA ROSENBERG

"BYOD," or "Bring Your Own Device," is no longer just a possibility—it's quickly becoming the norm. More and more, employers are allowing their employees to use their personal phones and tablets to connect to work, including to send e-mails, access and modify company documents and/or perform various other tasks. And, as has become typical with rapidly evolving technologies, employer policies and the law have been slow to catch up. The result is that many employers have been allowing BYOD, without taking the necessary measures to address and mitigate for the real challenges, risks and legal exposure it creates in the workplace.

Increased employee accessibility and availability through BYOD certainly is attractive. Managers appreciate being able to reach their subordinates anytime and anywhere, and receive responses more quickly. Employees appreciate having the flexibility to "remote in" to get work done, if they have to take time out of their regular work day for any reason. But these benefits come with risks, and these are the top five we tend to see from our clients:

Sonya Rosenberg, a partner in the Labor & Employment practice at Neal, Geber & Eisenberg LLP, focuses on the various employee-related legal issues that arise in the employment relationship. Additionally, she represents employers in litigation, including the defense of numerous administrative charges, lawsuits and appellate proceedings at the state and federal levels.

1. Security Threats. With increased remote accessibility to work systems and files, BYOD makes it easier than ever for employees to misuse and jeopardize employers' confidential, sensitive information and trade secrets. Or, if the device is lost or stolen, the employer's data and sensitive information could end up in the hands of hackers or sophisticated criminal operations that, as we have seen in a number of recent cases in the news, can severely compromise if not threaten the very existence of a company.

2. Productivity-Related Concerns. As work and life responsibilities and activities merge on an employee's phone, some employers face a real productivity challenge. For example, if able to check Instagram, post on Facebook, watch a favorite show or text a friend—and, also, update that finicky, tedious Excel spreadsheet for work—many will choose "fun" over work. Employers have to be thoughtful about the parameters they set, and the related checks they may decide to put in place, to help ensure their employees do not take advantage of BYOD to compromise productivity.

3. Wage and Hour/FLSA Issues. The Fair Labor Standards Act and parallel state laws generally require that employers ensure accurate tracking of the time worked and pay employees who are not exempt from overtime 1.5 times their hourly rate for any hours worked more than 40 in a regular workweek. If an employee who is not exempt from overtime works regular eight-hour workdays, but later at night checks and responds to work e-mail, for example, applicable law would dictate that the employer track and pay for that after-hours BYOD time and, likely, at an overtime rate.

4. Discrimination and Harassment. With communications becoming more remote and impersonal through ever-increasing use of technology, including e-mail,

various messaging applications, social media platforms and texting, BYOD creates increased risks for potential discrimination and harassment scenarios within an employer's workforce. Specifically, managers and employees can use their devices to make harassing, discriminatory, disparaging and otherwise inappropriate comments to co-workers. Some of these problems may remain unknown for a long time—exacerbating the company's exposure ultimately—if employees use newer data-erasing and security apps like Snapchat, Confide, Dstrux, Wickr and TextSecure, to mask their actions. In most instances, however, work and personal communications sent via an individual's cell phone may be recovered later, to create a comprehensive, discoverable record.

5. Ownership, Control and Reimbursement. Employers that allow BYOD must think through a host of practical considerations, including those surrounding ownership, control and reimbursement. For example, the employee brings and uses his or her own phone in a BYOD scenario, but the employer installs its own software to provide access to the company's network, and may require an appropriate level of monitoring and security precautions, including the capability for remote wiping in case the phone is lost or stolen. Depending on the kind of software used, employers should attempt to wall off access to employees' personal, private information on their phones, including password-protected social media and personal e-mail accounts, so as to avoid claims under federal and state privacy protections. With respect to reimbursement, as employees incur additional charges through their cell phone providers for the extra minutes, data use and travel-related fees incurred for work-related purposes, employers should develop a working plan for providing timely reimbursement.

While BYOD creates certain practical and legal challenges, its increasing popularity requires employers to implement smart, working strategies and solutions to maximize BYOD's many benefits, while minimizing the related risks and pitfalls. To that end, employers that already allow BYOD, and those considering doing so, should formally define and implement a tailored BYOD program and policy consistent with their individual needs and relevant areas of risk. Such programs and policies should likely include the following five basic components:

1. Approvals and Security. Employees who wish to use personal devices (as opposed to previously common, employer-provided devices) for work purposes should be required to comply with their employers' related expectations and rules. First, employees should receive express approval of management prior to participating in a BYOD program. Second, employees must agree to provide their phone to the employer for the installation of appropriate, company-approved software, including, for example, mobile device management software, and appropriate and remote monitoring and wiping capabilities, to ensure the employer's information is not subject to a security threat if the phone is lost or stolen, and that such information will be returned to the employer when the individual's employment ends. Employees should be required to notify management immediately in the event their devices are misplaced, lost or stolen.

2. No Expectation of Privacy. Similar to an employer's systems use and monitoring policy, a BYOD policy should notify employees that, to the extent permitted by applicable law, they should not expect privacy in the personal devices they use for work. Employers should reserve the right to monitor and preserve any communications that use the company's networks in any way, and to review, retain or release personal and company-related data on personal devices—including, for example, for investigation and litigation-related purposes.

3. Work and Personal Time. State expressly that while at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Personal use of the devices should be kept to a minimum, so as not to interfere with productivity.

4. Compliance With Policies. The company's policies pertaining to harassment, discrimination, retaliation, trade secrets and other confidential or sensitive information should apply with full force to the employees' use of personal devices for work-related activities.

5. Safety. Include an express requirement that employees follow applicable laws and regulations with respect to safe use of personal devices for work-related purposes, including, particularly, while driving.

In addition to these typical components, a BYOD policy should define the reimbursement structure, and—as any good, working policy—include a disciplinary component, allowing the employer to terminate an individual's use of BYOD and/or to take disciplinary action, up to and including termination, in the event of misuse.

Although the general considerations outlined here are likely to apply to most workplaces, employers should be wary of going with a one-size-fits-all approach to BYOD, and instead seek sound legal counsel to implement tailored, proactive solutions for their workplace, to address relevant practical and legal challenges, while embracing the technological advancement and the real business opportunities they create.

  DLR ISSN 0418-2693