GONZALEZ SAGGIO HARLAN

THE GSH 60 SECOND MEMO®

SPONSORED BY THE GSH EMPLOYMENT GROUP

July 10, 2013

Warren E. Buliox, Esq.

Questions on this topic? CLICK HERE

Attack of the Smartphone: The Rise of Legal Issues Surrounding "Bring Your Own Device" Programs

By Warren E. Buliox

While we may not be at the point where, like in the cult classic "Terminator" movies, machines with artificial intelligence have staged a dramatic and downright epic *coup d'etat*, we are at the point *in the employment space* where the integration of, and our reliance on, mobile computing devices has created an onslaught of issues which, if not managed correctly, can lead to significant legal risks for employers.

Let's start at the beginning. With the advent of smartphones, tablets, and other mobile devices like laptops and netbooks, the work space has evolved to become increasingly fluid and less confined to the four walls of an office building. The ability to work from home or from anywhere and be just as (if not more) productive is an attractive proposition for employers and employees alike. To use personal computing devices, rather than corporate-issued ones, can be an even more attractive proposition, as employees get to use a single device of choice for both work and their personal lives, and employers get to shed the cost of providing employees with these devices. Given this dynamic, many employers have implemented bring-your-own-device ("BYOD") programs. These programs typically manage the use of confidential and propriety information and address potential security issues with unsecured data on lost devices, all of which help to curb some of the inherent risks associated with the use of personal devices for work.

Some risks, however, are occasionally missed, as the assimilation of personal devices into the workplace creates a host of employment-specific legal issues, some of which are more obvious than others. These issues range from privacy concerns to labor issues to wage and hour issues. Below, we look at each of the more pressing issues in turn.

Invasion of Privacy Considerations: It almost goes without saying that employees have little to no expectation of privacy when it comes to electronic communications over company-provided equipment, such as computers and mobile phones. This allows employers to monitor emails and other communications without running afoul of state and federal privacy laws, providing of course there are policies in place governing the same. However, when the equipment used is the personal property of the employee, an expectation of privacy may attach, as any review of communications on the device may inadvertently result in the inspection and copying of personal and private content, some of which may be protected by the federal Computer Fraud and Abuse Act and similar state laws. To avoid this, any BYOD program should, at the very least, require employees to sign off on an authorization allowing for the retrieval and review of communications on the device. This is effective because consent is generally a defense to invasion of privacy claims.

Discrimination and Harassment: Discrimination, and particularly harassment, can occur outside the workplace just as easily as within. The introduction of smartphones and similar devices into the equation, however, may increase the odds. According to a poll reported in the *Huffington Post*, nearly 1 in 5 adults engage in some level of "sexting" -- sending sexually explicit or suggestive text messages or emails. If this occurs between employees, whether during working hours or not, it can serve as the basis for harassment claims. The text messages or emails are also discoverable and can serve as direct "smoking gun" evidence of harassment. Any BYOD program should explicitly prohibit inappropriate texting of any form as well as other activity that could be construed as illegal harassment, such as the sharing of racially insensitive pictures and videos.

Wage and Hour Issues: The "always-on-the-clock," ready-to-serve nature of BYOD environments can create significant issues for employers under the Fair Labor Standards Act ("FLSA"). The FLSA, as well as similar state laws, require employers to pay non-exempt employees at least minimum wage for all compensable time worked, and to further pay these employees overtime pay for hours worked in excess of 40 hours a week. As compensable time generally includes time performing work for an employer, time spent on smartphones, tablets, and laptops responding to emails and completing projects may constitute compensable time for FLSA purposes which, if not paid, can lead to liability. To minimize this risk, employers should incorporate into BYOD programs (or timekeeping policies) measures

to accurately capture time spent outside the office or normal business hours performing tasks on mobile devices. This can be as simple as a requirement that all employees record and report all time worked.

Another potential wage and hour issue concerns minimum wages requirements. Fees and expenses are often times attached to mobile devices. To the extent an employer requires the use of personal mobile devices, an employer can open itself to liability under the FLSA if the fees and expenses associated with the same operate to effectively reduce an employee's wages below that of the minimum wage. To lessen the likelihood of this happening, employers can provide reimbursements for various fees and expenses, or simply identify these additional fees and expenses and pay employees at a rate that ensures they do not fall below minimum wage.

Employee Negligence: Under the legal theory known as *respondeat superior* (which is Latin for "let the superior answer"), employers can be held liable for the negligent acts of their employees. This assumes, though, that the employee was acting within the scope of his/her employment at the time of the negligent act. With mobile devices, the workday arguably never ends, and an employee who gets into a car accident while attending to a work-related email will surely expose his/her employer to liability. Any BYOD program should specifically address this and restrict the use for mobile devices for work-related matters while driving or operating heavy machinery (as would be the case in construction and factory settings).

Labor Issues: For security and other reasons, some BYOD programs limit the information and/or types of communication that can be exchanged on personal mobile devices brought into the workplace. Employers should be especially careful here, as the National Labor Relations Act ("NLRA") affords employees in both unionized and non-unionized settings the right to engage in "concerted activities for the purpose of collective bargaining or other mutual aid or protection." Accordingly, and as the National Labor Relations Board has held, overly broad policies or practices that curtail an employee's ability to discuss and/or share information about work-related issues violate the NLRA. Without a clear statement of what types of information/communications are restricted (e.g., trade secrets, security protocols, etc.) and a statement that the restrictions in place will not be used to interfere with, restrain, or coerce activity engaged in for the mutual aid or protection of employees, a BYOD program can easily fall into this category and expose an employer to unanticipated litigation and possible liability.

The goal for employers is to tread lightly and watch your BYOD policies. The issues discussed herein are just a sampling of some of the issues and risks inherent in BYOD environments. If your work

environment is such that a BYOD program makes sense, carefully assess and account for the unique legal issues and risks associated with BYOD policies prior to moving forward.


Forward this issue

Arizona | California | Connecticut |Florida | Georgia | Illinois | Indiana | Iowa
Massachusetts | New Jersey | New York | Ohio | Tennessee | Washington, D.C. | Wisconsin

www.gshllp.com