Employment Law Report

July 2013

Yours, Mine, or Ours?

Bring-Your-Own-Device Programs Save Money but Raise Legal Questions.

The "Bring Your Own Device" trend – known by its now-popular acronym, BYOD -- is gaining traction as employers look for simple ways to cut costs and improve employee morale. A BYOD policy allows employees to use their personal smart-phones, tablets, or laptops for business purposes rather than requiring them to use company-issued equipment - a practice that may not only help a business to heighten morale but also increase productivity.

Companies want their employees focused on their job duties, not on learning the nuances of a new laptop or smart-phone. Employees, too, want to feel comfortable with and adept at managing the technology that they use—which is more often the case when the device is personal to them.

The practice of BYOD, however, is not without its perils. In order for a BYOD program to work successfully, the company must set forth its expectations and restrictions regarding the practice. A well drafted BYOD policy that is effectively communicated to all participants will often prevent misunderstandings or disputes regarding the use of the devices. While the policy may be part of a larger computer-use policy or employee handbook, it may be better to create a stand-alone BYOD document that is more easily revised as technology and business requirements change. As with employee handbooks, we recommend that each employee participating in the program sign an acknowledgment of his or her understanding and receipt of the policy, together with his or her agreement to abide by its terms.

Employers may find themselves vulnerable if they haven't considered the possible scenarios that can ensue when employees use their own devices for company business.

Because the BYOD trend is so new, little has found its way into legal precedent. This should change as BYOD-related cases begin to appear in court. When that happens, employers may find themselves vulnerable if they haven't considered all of the possible scenarios that can ensue when employees use their own devices for company business. When drafting these policies, employers should consider as many risk-related scenarios as possible and should definitely address the following topics:

Continued on Reverse>>

SHAPIRO SHER GUINOT & SANDLER

About the Firm

In 2012 Shapiro Sher Guinot & Sandler was named the top medium-size law firm in Maryland for Business & Transactions by Super Lawyers, a division of Thomson Reuters. Founded by sports lawyer Ronald M. Shapiro in 1972, the firm represents clients in numerous practice areas, including employment law, litigation, corporate, real estate, tax, and banking.

Shapiro Sher Guinot & Sandler's **Employment Law Group** is co-chaired by **Eric R. Harlan** and **Renée Lane-Kunz**. They are prepared to assist organizations with a wide spectrum of employment law matters, including recruiting and hiring practices, employee handbooks, discrimination matters, executive compensation, wrongful termination claims, and issues involving Title VII of the Civil Rights Act, The Family and Medical Leave Act, and The Americans with Disabilities Act. The Employment Law Group also assists with employment, severance, non-disclosure and non-compete agreements, among other matters.

Renée Lane-Kunz offers ongoing employment counsel to small and mid-sized companies as well as schools and institutions. She works closely with clients to help them anticipate and avoid litigation and regulatory complications. From handbooks to employment agreements, to general HR policies, she is ready to provide employers the tools they need in today's legal environment. As she brings to her practice extensive HR management experience in the hospitality industry, she fully appreciates the concerns of business owners.

Eric R. Harlan is a trial lawyer dedicated to the vigorous representation of clients in litigation. He has achieved favorable results in employment-related matters including claims involving violations of federal and state anti-discrimination laws, actions to enforce non-compete and non-solicitation agreements, wrongful discharge, and wage-and-hour litigation.

Who will be permitted to participate in the BYOD program and what devices will be supported by the company?

In most companies, IT resources are limited, and as the number and type of permitted devices increase, so do the support issues. Further, in a BYOD environment, a company's IT staff may no longer manage each device being used; rather, IT's role will now focus on the management and protection of the content and data found on each personal device. Therefore, you may want to identify those employee groups who would most benefit from such a program (department managers, outside sales executives, etc.) and limit the BYOD option to those individuals. An employer must also remember to evaluate each participating employee's status under the Fair Labor Standards Act ("FLSA"). Permitting a non-exempt employee access to work outside of regular, paid working hours could cause the employer to run afoul of wage and hour requirements under the FLSA. Finally, IT staff will also need to consider how best to educate, monitor, and support each BYOD user. For example, IT may wish to limit they types of devices that will be supported and require additional applications or changes in settings in order to adequately protect the company's proprietary information.

What restrictions will the company impose on the use of each device?

Now that the company will have mobile devices outside of its network, it should consider establishing guidelines for how each device may be used. For example, the company could require each user to enter a password, PIN, or fingerprint scan to access each device, and could further require users to inform IT whenever they change a password or device. Also, consider the potential exposure if an employee's smart-phone, tablet, or laptop, packed with confidential and proprietary company information, is lost or stolen. The company will want to include remote wiping privileges in its BYOD policy to protect against this contingency.

Moreover, if the company is going to require remote access for wiping purposes, another topic that must be addressed is the separation and protection of the employee's personal data. Will the employee release the company from liability associated with the loss of any such personal data? What if the employee shares the device with another person who is not employed by the company? If that user's information is lost, who is liable? A BYOD policy may need to contain provisions that protect the company from claims arising from such a complication. Fair policies will strike a balance between employee privacy and management's need to mitigate the threat of litigation.

How will the personal devices be supported and monitored?

Today a company's livelihood is often dependent on its technology. Businesses spend top dollar to purchase, support, and upgrade their hardware and software in order to remain current with technology trends and to remain competitive in the marketplace. When BYOD is introduced, management will need to decide how to handle the purchase and installation of "new and improved" programs, applications, and/or equipment that it deems necessary to meet business demands. Will employees be expected to pay for these required advancements? To what extent will the company reimburse the employee for such expenses? How will service plans and replacement costs be evaluated and resolved? It would be best to address these issues prior to implementing a BYOD program and to include the decisions in your policy statement.

Other considerations?

We all recognize that a BYOD program can save equipment costs; however, BYOD can expose a business to expenses in other areas of the budget. Consider litigation. While litigation costs generally can be daunting, the costs associated with responding to discovery requests related to electronically-stored information can be extraordinary. Imagine the difference between reviewing one company server and 25 desktops versus one company server, 25 desktops, and 75 other diverse, personal devices, including laptops, tablets, and smart-phones. Simply identifying all of the devices that may contain discoverable information can be a time-consuming, costly task. And let's not forget about the potential claims that may arise from the owners or users of these personal devices if either the equipment or the information contained therein is damaged, compromised, or lost entirely.

Although businesses may not yet be able yet to predict the future of BYOD policies and how they will stand up in court to privacy laws, data-breach, and other concerns, employers will want to do all they can to protect their businesses in the event of claims arising from a BYOD practice. After all, it's a trend that isn't going away soon.

For more information, please contact Renée Lane-Kunz at rlk@shapirosher.com or at 410.385.0202.