PUBLICATION

The Perils of BYOD Policies

January 13, 2016

Over the holidays, many employees are out of the office on family vacations or otherwise using their time off. Many employers rely on employees' use of their own personal electronic devices to keep up with what is going on in the office while they are away. While employers enjoy having employees at the ready, checking in with work while away from the office could spell legal trouble to employers. The perceived efficiency and cost savings created by such easy access to work can pale in comparison to the legal ramifications and costs that allowing unregulated access to work information on remote devices can have.

Bring your own device (BYOD) policies are becoming very popular. More and more employers are allowing their employees to use their own devices (smart phones, tablets, laptops etc.) to connect to work and to perform such tasks as checking emails, modifying company documents or engaging in off-site conferencing. While worker engagement and availability seem ideal, employers need to make sure they take the appropriate measures to mitigate the legal risks such devices pose in the workplace.

For instance, the Fair Labor Standards Act (FLSA) requires employers to keep track of the hours their non-exempt staff work and to pay overtime for hours worked over 40 in a regular workweek. A non-exempt employee who works a normal 9-5 shift, 40 hours a week, but then logs on remotely at home after hours to check email, is entitled to overtime. Moreover, the employer is required to keep accurate records of all hours, including those from home or while traveling, that employees work. In light of the proposed changes to the white collar exemptions, in the near future more employees will be considered non-exempt for FLSA purposes. Thus, employers may have to be even more vigilant in monitoring who is logging on and when, or be faced with the increased probability of FLSA liability.

Allowing employees to bring their own devices to work could also pose a security risk to an employer. Allowing remote access to an employer's email system, company documents, etc., makes the risk of an employee misusing confidential or proprietary information greater. Additionally, employers need to have plans and security in place should an employee's device be lost or stolen. For employers that allow employees to have remote access to information that is sensitive, such as social security numbers or protected health information, a lost or stolen device can have enormous legal and reporting ramifications.

Employers that allow employees to use their own devices must make sure that employees know that, when using such a device, they are required to follow all employment-related expectations and rules. Prior to being allowed remote access to work email, an employee should be granted permission from the employer so that the employer is aware of the possibility an employee could be working remotely. For non-exempt employees, the employer should require the employee to promptly report all time spent working remotely so that the employee can be paid accordingly. Employers should establish policies for non-exempt personnel regarding approval for work away from the office and expectations on how much time, if any, should be spent on activities such as nightly catching up on emails.

To mitigate the risk associated with a lost or stolen device, employers should require employees who have remote access to provide their devices for installation of company-approved security software that, for instance, allows remote wiping of data should the device be stolen or misplaced. Employers should require

employees to notify them immediately if any of their devices are lost or stolen so that appropriate safeguards and reporting can be quickly initiated.

As with most areas of the law, technology is outpacing the legislature's ability to regulate. Employers should be vigilant and attentive regarding how technology is used in the workplace and should seek legal counsel in drafting workplace policies that reflect the true nature of the work environment, especially regarding remote access.