BARNES & THORNBURG LLP

Five Things To Consider When Creating A Bring Your Own Device (BYOD) Policy

October 14, 2013 | | Social Media And Technology,Labor And Employment

As employers and employees become more heavily dependent upon immediate communications through the use of smart phones, many companies still have not created or implemented Bring Your Own Device (BYOD) policies. As a result, employers are vulnerable in having their confidential business and trade secret information exposed, or worse, taken. Employers also risk having legal claims, such as harassment or defamation, asserted against them because of the communications employees make using their smart phones.

To minimize these risks, employers may want to consider implementing sound BYOD policies. Below are a few things to take into account when drafting a BYOD policy.

Deciding the Scope

In creating a BYOD policy, employers may first want to determine what smart phones and tablets employees are using. Then, in creating the policy, the company can decide whether the BYOD policy applies only to smart phones or does it include the tablets. Employers will want to clearly communicate which devices it will and will not support as well as the information that will be permitted to be accessed through those devices.

Requiring Passwords

Similar to requiring an employee to log on and use a password with his/her company-issued computer, the BYOD policy might include the same requirement. Because smart phones or tablets can more easily be lost or stolen, strong passwords should be required, not just a simple 4-digit pin. Instead, most experts recommend that the passwords entail an alphanumeric password.

Employees are often resistant to these types of passwords because it does not provide immediate access to information. A strong BYOD policy makes it clear that the need for a more complex password is required in order to protect and preserve the company's confidential business information.

Who Owns What?

Although it seems fairly straightforward, employers may want to communicate in the BYOD policy that the company owns the information stored on its servers that the employees access through their devices. Additionally, the policy might go on to explain that the company can wipe (delete) the information stored on the device in the event it is lost or stolen because that information contains confidential business information owned by the organization. Finally, employers may want to communicate that there is no expectation of privacy in the employee's use of the personal device similar to the use of the company-issued computer.

RELATED PRACTICE AREAS

Internet and Technology
Labor and Employment
Workplace Culture 2.0

However, a word of caution: while the company may own the information stored on the server, employers may want to consider resisting the temptation to access and/or read emails from the employee's personal email account which may have been on the personal device. A recent case in the Northern District of Ohio found that a company violated the Stored Communications Act after a supervisor, without authorization, read more than 40,000 emails sent to the employee's personal email account through the company-issued smart phone. Not only could the violation of the Act carry significant fines and penalties, but also criminal consequences.

Acceptable Use

The BYOD policy will also likely include the employer's acceptable use policy, which would mirror the policy for an employee's use of its company-issued computers. For example, if Company A prohibits access to Facebook or certain objectionable websites via its computers, their BYOD policy would have similar language. Additionally, employers should consider adding language in the BYOD policy requiring employees that they must follow the company's anti-harassment, respectful treatment in the workplace policy.

Parting Ways

When an employee separates from an organization with his/her personal device, the company could be vulnerable and risk losing its confidential business information. A thorough BYOD policy will likely address this by making it mandatory that the employer will wipe (delete) any company-stored information on the personal device at the time of the employee's departure. Because many employees have personal information such as photographs or music or other purchased applications, employers should consider developing a protocol to protect the employee's personal information while still removing the company data.