"Bring Your Own Device" Programs Create a Nest Of Policy Issues

Publication
5.27.13

There is a new trend in the workplace: the bring your own device (BYOD) program. An employer permits employees to use their own laptops, tablets, smartphones, etc. to connect to company servers and access company information. For an employer, a BYOD program may reduce expenses, as it obviates the need to purchase and maintain some expensive company-issued devices. It also can increase productivity, as employees will gain access to company information, including emails, from virtually anywhere at anytime.

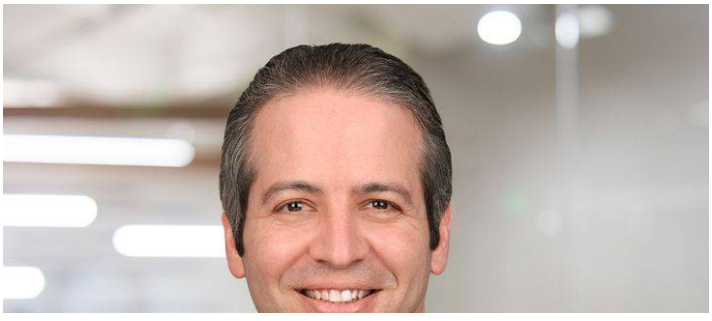
But it also brings potential legal challenges for employers, in such areas as privacy, wage-and-hour issues and trade secrets, and the need to address some critical policy issues.

A company should first clearly identify which if any employees should be granted access to company servers, based on an employee's job duties and responsibilities. A well written BYOD policy informs employees of their responsibility to keep their device secure at all times; notes that all workplace policies extend to use of the device for business purposes; notes that the employee does not have an expectation of privacy for any company information created, transmitted, downloaded, received, reviewed or stored in a company's network; and explains company procedure if the device is stolen or lost, or if the employee is terminated.

Consider implementing a remote data removal, or "remote-wipe," option. This enables the employer to remotely delete its stored information on the device in case the device is lost, or upon the employee's termination.

This article appeared in the April/May 2013 issue of *Today's General Counsel*.

Related People



Todd B. Scherwin
Regional Managing Partner
213.330.4450
Email