THE RECORDER
ESSENTIAL CALIFORNIA LEGAL CONTENT An ALM Web site

Increase in BYOD Is Reason for Concern

By David J. Walton

August 17, 2012

David Walton, Cozen O'Connor partner

When I first started practicing employment law, one of the big issues my clients dealt with was how employees used company-owned computers and Internet services. The Internet was relatively new. Many employees didn't have access to the Internet at home and if they did it was via dial-up (remember that term?). In addition, computers were expensive. When laptops first came out, a lot of employees couldn't afford them for personal use. Many of the early laptop purchases were employers that give them to employees, especially those who traveled. Employees generally loved this, and they frequently used their employers' laptops for personal use. Not surprisingly, these computers and the employer's Internet were sometimes used for improper purposes, creating all types of potential liability for employers. Policies governing the employee use of computers and Internet were in high demand.

Now, with the "consumerization" of the electronics industry, this world has completely pivoted. This development is known as BYOD — bring your own device — to work. Employees, as consumers, have access to the best devices — iPad, iPhones, Android phones, Android tablets, Ultrabooks and all the apps that come with these devices. They want to use these devices for work, especially employees who travel a lot. They don't want to use the clunky laptops their employers still have. They don't want to carry around one phone for personal use and a different one for work. They don't want to use a Blackberry, which most employers purchased. And they want to use tablets, which many employers haven't yet bought.

BYOD gives businesses some advantages over their competitors. BYOD allows some employers, especially smaller and midsize ones, to save money by pushing some technology costs to employees. A recent technology report stated that more than 50 percent of companies with BYOD models required employees to cover all costs, but employees often do not object. They generally would rather pay for their own devices because it provides them with greater choice and flexibility. BYOD is so prevalent that many manufacturers that were developing tablets and smartphones for enterprise use have abandoned these projects. For example, Cisco Systems Inc. recently decided to drop its "Cius" business tablet because employees are bringing more of their own electronics to work in place of the tablets, smartphones and other devices provided by their employers.

Another benefit of BYOD for employers is that personal technology can make employees more productive. The line between work and personal lives is virtually decimated. People are checking their work email constantly over the weekends, at night and on vacations. Employees like having immediate access to their email and work information so they can work where they want, how they want, and however long they want. This added flexibility is being embraced by employees due to the increasingly mobile nature of our workforce. Indeed, one of the reasons Cisco decided to stop development of the Cius tablet is because they found in their own survey that 95 percent of the organizations surveyed allowed employee-owned devices in the workplace.

BYOD Concerns

At the same time, there are some serious concerns with BYOD. The biggest problem is the security of company data. This is especially true with the growth of personal cloud storage. Services such as Dropbox, iCloud, SugarSync and Boxnet allow employees to easily lease space (mostly cost-free) on large servers so they can access their data from anywhere in the world, as long as they have access to the Internet.

These types of services are also important because of the increasing use of tablets. Tablets, especially the iPad, do not have a USB port. There is no way to transfer files between a work computer and a personal tablet via a flash drive. Thus, employees rely on cloud-based services such as Dropbox so they can store files in one place and access them from work and from a tablet. These types of services also allow for collaboration among employees who are working from home and/or in different geographic areas.

But again, the major problem with Dropbox and these other cloud storage services is the security issue. Based on security concerns, some companies have tried to ban personal devices at work altogether. Like prohibiting the use of Facebook and other social media sites, banning the use of personal devices at work will cause a mini-revolt at many employers and will be virtually impossible to consistently enforce.

Technical developments will make it easier to manage BYOD. Many software companies are developing a security programs to help with BYOD. New software is being developed for

encryption, tracking and remote wiping of mobile devices. Some smartphones now have "toggle" features, allowing the user to toggle between personal and business use on the phone.

BYOD Policies

Companies must think proactively by adopting policies that protect their data while giving employees the freedom of choice they crave. These policies should include several points. First, employees should be required to refrain from using company information on personal devices for anything other than their use for the company at issue — i.e., they may not turn this information over to a competitor.

Second, if employees are going to use personal devices for work, they should be required to use passwords for the devices and disclose to their employer the passcode for each device. They should also describe the type of information they want to store on their device and promise to update the company if they purchase a new devices or access more information than initially identified.

Third, some companies are aggressively banning the use of personal cloud storage for company information. In 2010, IBM Corp. adopted a BYOD policy mostly because of the security issues involved. But in doing so, IBM banned the use of many apps such as Dropbox because they were concerned about controlling the spread of company information and trade secrets.

If, however, you don't want to strictly prohibit using these services for company data, the BYOD policy should require employees who use these services for company information to tell the company what sites they are using, provide the account information to IT (user name and passcode), give IT permission to access the site, and to promise to allow IT to check the site before the employee shuts it down (especially after the employee leaves).

Fourth, when an employee leaves the company, IT must have the right to wipe, or at least inspect, any personal computers or devices that were used to store or access the company's confidential information.

Fifth, while BYOD cannot be realistically eliminated from the workplace, companies still should prohibit specific, vital types of data from being copied to or stored on these devices. Companies should also conduct an assessment of their actual trade secrets. If data is clearly a trade secret, the company should customize protections for that type of information to make sure that it does not fall into the wrong hands through an employee's use of a personal device. Treating all trade secrets the same will potentially undermine a company's legal protections.

BYOD is here to stay. In the personal electronics world, the individual consumer is king. They, not employers, are driving the development of the electronics industry. This trend will not reverse. Employers must learn to adapt, think ahead and be vigilant in protecting their information in a BYOD world.

David J. Walton is a partner in Cozen O'Connor's labor and employment group and co-chair of the firm's E-Discovery Task Force. He concentrates his practice on all aspects of employment litigation. He has extensive experience in litigating matters involving restrictive covenants, trade secrets, fiduciary duties and defending employers targeted by discrimination lawsuits.