BCLP. Client Intelligent

**RetailLawBCLP**

# RETAILERS SHOULD BE AWARE OF DATA PRIVACY CONCERNS WITH BRING YOUR OWN DEVICE POLICIES

Sep 01, 2017

Many retailers permit their employees to use personal mobile devices, such as smartphones and tablets, to access company-specific information, such as email, under a Bring Your Own Device ("BYOD") policy. BYOD policies can be popular for employees that want to use hand-picked devices and for retailers that want to avoid the cost of providing, and maintaining, company-owned devices. Nonetheless, the use of company data on non-company devices implicates both security and privacy considerations.

A reported 40 percent of companies offer BYOD to all employees, according to a survey by Crowd Research Partners. Security concerns, data leakage, and malware were all listed as top concerns of retailers in allowing BYOD.

Consider the following when deciding upon a BYOD policy:

**Is the scope of your control over employees' mobile devices consistent with your company's interest?** Retailers should consider why they have an interest in knowing about their employees' mobile devices; that interest should be the basis from which a BYOD policy should emerge. If the company simply wants to allow an employee to access work email on a mobile device, then the policies and restrictions should proceed with that focus.

**To what extent and for what purpose does your company monitor employees' use of mobile devices?** Many servers create logs showing when an employee's device accessed the organization server using certain authentication credentials. As security measures such logs are often appropriate. To the extent that a retailer wants to monitor more substantive actions by an employee on a mobile device, such monitoring should be in line with an appropriate purpose.

**What procedures are in place to restrict the transfer of data from the network by way of the mobile device?** Organizations often protect against the risk that organization data will be "floating" on multiple devices by limiting the types of data accessible to mobile devices (*e.g.*, email) and restricting, to the extent possible, how that data can be used on the mobile device (*e.g.*, policies on copying and requiring certain security settings). For example, some organizations use sandboxed applications for accessing work-related email. Such apps open email in a program that is separate

and apart from the native email system that is built-into the device and control aspects of the user's experience. For example, they may restrict the user from locally saving any emails, or attachments, to the user's device.

**For security purposes, does the organization require a minimum version of the operating system and/or software before an employee can use a mobile device?** Minimum versions ensure that certain security protections and bug fixes are present on the device.

**Can data on a mobile device be remotely wiped?** By whom? A best practice for devices that contain confidential or sensitive organization information is to ensure that the data can be remotely deleted from the device by the retailer if, for example, the device is stolen or the employee is terminated. To the extent that the employee only accesses work-related data when accessing a sandboxed application, it may be relatively easy to restrict the device from accessing such data remotely. To the extent that an employee was permitted to locally store work-related data (*e.g.,* cache work emails locally, or download attachments), a retailer should consider whether it has the right, and technical means, to remotely wipe the entire device.

**What procedure is in place for an employee to report a missing mobile device?** Accidents happen to everyone, but their aftermath can determine whether they become catastrophes. Employees should report a missing device to someone – perhaps the IT department or help desk – so that the retailer's device removal policy can be followed.

**What steps does the company take to proliferate its mobile device policies?** Retailers often rely on their IT staff, self-help materials, and employee certifications to ensure employee awareness and enforcement of the retailer's policies.

**Do the security measures in place match the sensitivity of the data accessed through the mobile device?** For some employees that receive non-sensitive information minimal restrictions may be appropriate. For employees that receive sensitive or confidential information higher restrictions may be appropriate.

**Is BYOD required of the employee?** Although BYOD programs are widely lauded for increased productivity and "off-the-clock" accessibility, this benefit can expose retailers to potential wage-and-hour issues if the BYOD user is a nonexempt employee.

**Does the employee have a means of tracking and recording his time?** If a nonexempt employee is permitted to use a mobile device for work related purposes after working hours, is there a policy that mandates that the employee must report the time that he or she worked? Is there an effective and efficient means for the employee to report such time?

## MEET THE TEAM


### Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435


---