As featured in Seattle Business

The BYOD Question

Sound advice on 'Bring Your Own Device' to work.

The "Bring Your Own Device" to work movement, or BYOD, has drastically changed today's workplace. In a recent study, Cisco Systems found that 95 percent of the 600 companies surveyed permitted the use of personal devices at work. BYOD has some huge benefits for employers. A Dell study found that companies with BYOD programs experienced a 74 percent productivity increase. Intel, for example, moved to BYOD in 2008. It found that instituting BYOD saved employees an average of 57 minutes each day, yielding an annual company-wide productivity gain of five million hours. But BYOD raises some new risks for employers, requiring implementation of a BYOD policy.

1. Employee Privacy Claims. Employees typically do not have a reasonable expectation of privacy when using the employer's computer systems. However, employees have an expectation of privacy when using their own dual device on their employer's computer system. Employees are protected from the unauthorized access of their dual devices, regardless of whether they happen to be connected to their employer's network. The Computer Fraud and Abuse Act and the Stored Communications Act create criminal and/or tort liability when an individual or entity gains unauthorized access to a computer. So, employers want to avoid engaging in unauthorized access to an employee's personal email account or an employee's cloud-based storage provider.

> With company-issued devices, the company can more easily expect compliance with its acceptable use policy. With BYOD, however, the company can lose some control over the appropriate use of the device.

2. Significant Security Issues. What happens when your employee loses his or her phone? One recent study confirmed that employees who are "consistently warned of the dangers to their data … are not keeping security top of mind." Your BYOD policy should require minimum security measures and a process for establishing those controls. Companies may consider using the "remote wipe" switch, which theoretically deletes all information on the device, including personal and employer data. An employer's decision to "wipe" an employee's personal device *without* the employee's authorization (as part of your BYOD policy) could create liability under the statutes listed earlier.

3. Acceptable Use. With company-issued devices, the company can more easily expect compliance with its acceptable use policy. With BYOD, however, the company can lose some control over the appropriate use of the device.

4. Employee Wage/Hour Claims. BYOD will inspire wage and hour litigation. Employees may use their dual use devices after hours. If the company has any way of knowing that the work was performed after hours, the employee is entitled to compensation. Does the company have to reimburse the employee for the cost of the device, phone or data plan? The Fair Labor Standards Act prohibits employers from requiring employees to pay these types of expenses, if doing so would reduce the employee's earnings below the minimum wage or overtime pay rate. So you need to calculate whether the employee's wages fall below the minimum wage and account for overtime pay.

5. When the Employee Leaves the Company. Your BYOD policy must address who will discontinue access to company data, and who owns the phone number.

If you would like to see a model BYOD policy, email reillym@lanepowell.com.

D. MICHAEL REILLY is a Shareholder at Lane Powell and Director of the firm's Labor and Employment and Employee Benefits Practice Group. He is the founder and a contributor to the firm's Boom: The ERISA Law Blog. Reach him at reillym@lanepowell.com or 206.223.7051.