BROOKS PIERCE

BYOD: Five Things To Consider When Creating

Digital Media and Data Privacy Law Blog

By Elizabeth Spainhour on 04.01.2015
Posted in Privacy Policies

"BYOD" or "bring your own device" (also known as the "consumerization of IT") is a fact of life in today's workplace. BYOD refers to the practice of using personally owned devices—like smartphones, tablets, and laptops—for work purposes and allowing these devices to connect to company networks and applications. According to a Gartner study released in late 2014, 40% of U.S. employees working for large companies use personally owned devices for work purposes. Of those who reported using personally owned devices, only 25% were required by their employers to do so. And of the 75% who chose to use their personally owned devices for work, half did so without their employers' knowledge.

If that last statistic doesn't alarm you a little, it should.

BYOD can be great for productivity, but it also creates risk for companies. Why? Because personally owned devices are not managed or controlled by company IT, and security of the device is in the hands of the employee. In other words, these devices can be a source of company data loss or data leakage. For example, if an unencrypted personal laptop with company data on it gets lost or stolen, you may have a data breach on your hands.

So how do you address these concerns? Start with a written, employee-acknowledged BYOD policy.

Here are five things to consider as you develop your policy:

1. Start by building an interdisciplinary team to create the policy. The team should include IT, human resources, legal, compliance, and employees who use their personally owned devices. BYOD is not just an IT issue but also a legal and business issue. Different perspectives will help lead to a policy that fits your organization's needs and is capable of being followed.

2. Develop the goals of the policy. Security should be a goal but productivity is also important. Cost savings may also be an objective. These, and other goals, may be in tension at times. In the end, you want to develop a policy that strikes the right balance for your company. Consider a BYOD policy that ensures the only way enterprise data flows into or out from a device is through enterprise systems (e.g., avoid emailing business information to employee personal email accounts).

3. Determine which employees are covered and how they are covered. There may be different policies for different types of employees based on job type or function. For example, the policy for exempt employees may be different than the one for non-exempt employees. Consider whether all employees need to be able to use tablets (for example) to access corporate data for work purposes. Be sure to consult with counsel about employment laws and regulations that may apply in this area.

4. Decide which devices/uses are permitted and how the policy applies to each. For example, the BYOD team should conduct "app reviews" to decide what apps are okay for business use and what apps are not allowed. Particular types of smartphones, tablets, or laptops may not meet the company's security requirements and, if not, should not be permitted. Also, the policy for smartphones may be different than the policy for laptops because they are different devices used in different ways and may pose different security risks.

5. Build in training so that each employee knows the policy and how it applies to him or her. In the end, security is about people just as much as it is about technology.

This isn't an exhaustive list of considerations, but it will help get you started crafting a BYOD policy tailored to your company. It's important that you do so, if you haven't already.