PUBLICATION

BYOD – Bring Your Own Device Policies

Authors: Zachary B. Busey
August 23, 2013

Companies, big and small, spend a large amount of resources on IT infrastructure, IT logistics, and IT support. A quality workforce will swiftly crumble if individuals cannot communicate quickly and effectively. This IT burden is a significant and often costly one, to which companies dedicate a vast amount of human and financial resources. In an effort to relieve themselves from this burden and stay competitive in the marketplace, companies have started to develop and implement bring-your-own-device or BYOD polices.

What Are We Talking About?

A BYOD policy is fairly straight forward. Rather than providing to employees electronic devices (e.g., a smart phone, tablet, and laptop), an employee simply uses (i.e., brings to work) his or her personal electronic devices. A BYOD policy eliminates the proverbial "company provided" device. In a BYOD workplace, the company provides the hardware and storage for the information, and the employees provide the devices through which that information is accessed.

Why Have a BYOD Policy?

It is cheaper. A BYOD policy can significantly reduce day-to-day IT costs, as well as upfront costs for emerging companies. For example, think of all that comes with just one smart phone: the phone, a charger, multiple cables and an equal number of adapters, replacement parts (Who has more than one BlackBerry battery?), stands/cases/covers, and the nearly constant managing of firmware and software updates. A BYOD policy can significantly, if not entirely, reduce these hassles and costs.

It gives employees freedom to choose. A BYOD policy allows employees to choose the type of device they want. It is difficult for companies to be flexible in their technology offerings. Most hardware only becomes affordable when bought in relatively significant quantities. And no matter what the option is, no single option will ever please everyone. Just ask the next person you see with an iPhone if he or she would mind switching to BlackBerry, or Android, or Nokia, or anything besides the iPhone. With a BYOD policy, employees are free to choose their own device—relieving the company of that decision. Employees are typically happier when they are the ones calling the shots, and the freedom to choose can be a competitive advantage.

What Concerns are There with BYOD Policies?

BYOD policies are a recent invention, and unfortunately, we do not yet have all the answers. Nor have we seen any publicized disputes or litigation in which a BYOD policy took center stage. But the scenarios that could trigger litigation are not difficult to imagine:

Who owns the phone number? On their personal devices, sales employees make hundreds of calls a day to current and prospective clients. An employee leaves the company, but clients continue to call the former employee's personal number thinking it is that of the company. Can the company obtain the rights to the

former employee's phone number? Did the former employee relinquish the rights to his personal phone number by using it at work?

Does checking e-mail count as overtime? This is already a hot-topic in employment law. 200 police officers recently filed a lawsuit in Chicago claiming that they are owed millions of dollars in unpaid overtime for checking e-mails and taking calls on city-issued BlackBerrys, outside of normal working hours. BYOD policies grant hourly employees tremendous freedom to check e-mails outside of normal working hours, and employers must remain vigilant as such activities can violate wage and hour laws.

Should the company remote wipe a personal device? Employer fires employee for being a three-day, no-call no-show. The employer then remotely wipes the personal device that the employee had been using under the employer's BYOD policy. In doing so, the employer also inadvertently deletes and destroys the employee's personal data. Has the employer opened up itself to liability? Would a written policy, acknowledged in writing by the employee lessen the chance for liability?

E-discovery. The ever-expanding realm of e-discovery would most certainly include personal devices used as part of a BYOD policy. This means that litigation and e-discovery holds would have to be expanded to include those personal devices, and steps would have to be taken to preserve and collect the information stored on the personal devices. The preservation and collection of information on a personal device comes with its own questions and concerns, which we'll save for a later post.

What Should be in a BYOD Policy?

Ultimately, the implementation of a BYOD policy requires an employer to balance its own security/confidentiality interests with the privacy interests of its employees. As with all workplace policies, a written BYOD policy, properly implemented and consistently enforced, is a great starting point. Areas covered within a BYOD policy should include:

- A brief explanation of what the policy is and the freedom of choice the policy affords to employees.
- A financial disclaimer and/or explanation. The policy should make clear that the employer will not purchase for the employee devices or replacement devices. Some employers, however, may choose to reimburse employees for certain items, e.g., $30/month for a data plan or a one-time, $100 reimbursement for the purchase of a smartphone with the ability to perform certain functions.
- A reference to the employer's electronic use policy, and an explanation that the electronic use policy applies equally to electronic device(s) used as part of the BYOD policy.
- A password requirement. All devices used as part of the BYOD policy must be password protected and settings should be set so that a password prompt appears after 1 minute of inactivity, when the device is powered on, or when the device is “woken up”.
- A privacy disclaimer. The BYOD policy should make clear that employees have no right to privacy in the device(s) used as part of the BYOD policy.
- A liability disclaimer. The employer should disclaim (and the employee should agree to waive) any liability or responsibility for damage to, or the loss/corruption of data stored on, a device used as part of the BYOD policy.
- A search/access agreement. The BYOD policy needs to make clear that the employer has the right to physically and remotely access any device used as part of the BYOD policy. The details of how and for what purpose an employer would access an employee's device will be company specific.
- A limitation on access/use. No third-parties should be allowed to use and/or access any device used as part of the BYOD policy. We don't want a young child accidently e-mailing all contacts with something like: “aad;flkjafja;lsllllllsdfjads.”

- A reporting requirement. The BYOD policy should require employees to immediately report to a specifically identified individually if a device is lost or stolen.
- A written acknowledgment/verification. All employees using the BYOD policy need to verify in writing that they received the policy, understand the policy, and agree to be bound by it. The written acknowledgement/verification should also include a description (make, model, color) of the employee's personal device that he or she will use as part of the BYOD policy.

Perhaps above all else, a BYOD policy should identify what actions employers may take under certain circumstances—for example, "If/when a device is reported lost or stolen, Employee authorizes the Company to remotely wipe the device and clear the device's contents at the Employer's discretion." Think of it this way: If an employee knows (i.e., acknowledges in writing) that his or her employer may take a certain action under certain circumstances, the employer is less likely to be held liable for that action. While this certainly is not always this case, it is a great rule of thumb for drafting a BYOD policy.

Lastly, there are a number of applications/software available that create internal "firewalls" on personal devices. These firewalls prevent the combining of company and personal data, and the applications/software provide other security benefits to companies, such as the remote locking and remote wiping of devices. Whether these types of applications/software are appropriate will depend on a company's specific needs and technological capabilities.