CARLTON FIELDS

Risky Business: "Bring-Your-Own-Device" and Your Company

September 23, 2013

Smartphones and tablets are everywhere. Largely prompted by Apple, Samsung, and Google's consumer-centric marketing strategies, people are spending more and more money on the latest and fastest mobile devices, upgrading them almost constantly, and integrating them into every part of their lives. A large part of that integration is work-related. Employees use their own devices to manage work calendars, view and respond to e-mail, take notes at meetings, and almost anything else they would ordinarily do at their in-office workstation. Allowing employees to bring their own devices to work is no longer a trend; it has become a business necessity. As a result, an increased number of personally owned devices are making their way onto company networks, and it is undeniable that the bring-your-own-device (BYOD) phenomenon is here to stay. BYOD presents companies with a myriad of new risks and challenges and lawyers need to understand the issues involved in order to provide quality advice to clients as it relates to information management. The most important thing every corporate attorney and outside counsel advising clients on information governance and BYOD needs to understand is this: the biggest risk with BYOD is data loss. An effective BYOD program and policy should emphasize security and contain clear instructions on what behaviors and activities are permitted on personally owned devices that have access to corporate information systems. However, most companies do not have the information architecture, hardware infrastructure, or resources to protect and secure all the data flowing through networks filled with different operating systems, applications, and devices – many of which, by the way, are widely dispersed and access internal corporate data via unsecure Internet connections. In order to fill this gap, companies are turning to Mobile Device Management (MDM) service providers to equip themselves with software tools and security solutions to protect the devices and data on their networks. Installing MDM software can help mitigate a lot of the technical risk associated with allowing employees to access company data on their own devices. For example, it is common for MDM solutions to allow a company to encrypt data on mobile devices, remotely lock and wipe devices, know the location of the device in real time, enforce a PIN policy, access personal data and contacts, and track user activity. While these capabilities address many of the security risks associated with BYOD, they also create problems related to employee rights and privacy. Monitoring privately-owned devices creates a significant policy dilemma for companies and it raises a lot of legal questions for attorneys. If your client monitors too much, it can be seen as invading employee

privacy, and in some parts of the world, may even be breaking the law. If it does not monitor and control enough, it places the company's data at a huge risk. Balancing these two seemingly opposing interests is the single greatest challenge to successfully implementing a BYOD program, and it is the role of legal counsel and in-house lawyers to make sure this implementation is done within the law, transparently, and without exposing the company to unnecessary legal risk. So, as an attorney, when a company you represent or work for informs you that it is interested in investing in technical solutions such as MDM to address security risk factors associated with BYOD, you should be prepared to respond that along with a technical solution, and in fact, ahead of it, it will be necessary to create a comprehensive BYOD policy that is transparent, easy to understand, and sufficiently detailed to help protect the company from unwanted regulatory scrutiny and litigation and to avoid the privacy pitfalls that can arise with the rollout of a BYOD program. As briefly described above, MDM software gives companies a lot of power to control and manipulate the devices their employees use to access corporate data. Before they deploy any type of MDM, counsel should advise their clients to create a training program to educate employees about the scope and capabilities of the software. Every single person employed by your client should consent to MDM software installation before installation and should understand exactly what information is collected, how the MDM software is used, which capabilities are enabled, what happens during an incident, and what the employees' expectations are upon termination of employment. Security incident procedures must also be spelled out in your client's BYOD policy. For example, the BYOD policy must clearly explain what will happen if an employee reports a missing smartphone. Will the device be auto-locked? Will the company attempt to locate it using geo-location? Will the device be wiped completely? Will the employee's access rights be restricted? To avoid confusion and provide a framework for incident response, all these procedures should be spelled out in writing in the BYOD policy and provided ahead of time so employees do not encounter any unexpected results or surprises. Lawyers will have to work hand-in-hand with the CIO and the IT department to ensure that the BYOD policy accurately reflects and considers all of the capabilities of the MDM solution being deployed. There are also several notices that must be incorporated into an effective BYOD policy. For example, employees must be made aware of all "passive" or "background" security measures in effect on their devices. If your client is going to track user activity on its employees' devices, they must be told exactly what is being tracked and how that information is being used and stored by your client. If the client is tracking the location of the device via MDM software or other means, the BYOD policy must also describe how location data is used and who has access to it and why. The best and most transparent way to increase monitoring of activity on privately-owned devices is to provide notice and ask for permission. When drafting a BYOD policy, it is "smart lawyering" to explain each process in detail and ask for specific consent. Consent is a key component to any successful BYOD policy and BYOD program because it empowers your client to govern and monitor the activity of its employees' privately-owned devices without appearing to be secretive or deceptive. Here is a good rule of thumb: advise your clients never to install anything on any employee's personally-owned device without obtaining consent first. If a new feature is added that changes the way monitoring occurs, revise the BYOD policy and have employees acknowledge that they understand the changes.

If (not really if, but when) it is discovered that your client has been engaged in any clandestine activity or secret monitoring of an employee's privately-owned device, it will almost certainly lead to conflict, disapproval, and possibly litigation. For example, in a case that went all the way to the U.S. Supreme Court, a California police officer sued his police department after he discovered that they had collected and reviewed personal text messages he sent from an employer-issued device. The Court, in *City of Ontario, California v. Quon*, ruled that the Fourth Amendment rights of a government employee had not been violated when the contents of his personal text messages – which were sent from a government-issued device – were reviewed in the course of an investigation. However, the Court expressed restraint in saying that its decision was deliberately narrow because "a broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted." Further, the Court stipulated for purposes of its discussion that Quon had a reasonable expectation of privacy in the text messages sent on the government-issued device. The implications of this reasoning for purposes of BYOD are significant because it is fair to assume that if a reasonable expectation of privacy exists on a government-issued device, then at least the same or an increased expectation of privacy will exist for a device the employee personally owns. In addition to the Supreme Court chiming in on digital privacy in the workplace, several state legislatures have passed laws requiring employers to notify employees when monitoring their electronic communications. *See* Del.Code Ann., Tit. 19, § 705 (2005); Conn. Gen.Stat. Ann. § 31-48d. The threat of "spillage" or information leaking out of the confines of the company's protected network is another significant challenge with BYOD. In order to prevent spillage, IT departments want to have the option and capability to wipe devices or destroy data at any time. Lawyers must caution clients against such broad control of and access to personally-owned devices because wiping or destroying data on any device with or without the consent of the owner is a very risky proposition. For example, if wiping a device deletes the owner's media library containing thousands of dollars worth of movies and music, is your client then responsible for the loss of property? What if a device is reported lost, gets wiped, and then is found the next day in a safe location? Is your client responsible for helping recover all of the wiped personal information? As employees become more aware of their own risks associated with BYOD, it will become more difficult for companies to implement security solutions that grant them widespread control over their devices. Companies will be forced to make uncomfortable compromises and lawyers will have to play a lead role in helping them decide what their risk tolerance is for both the loss of corporate data and the possibility of violating their employees' privacy. One countermeasure that can be employed to reduce the risks associated with device control and device-wide wipes is "sandboxing." Sandboxing is a form of software virtualization (via MDM software) that allows programs to run in an isolated virtual environment on a device. MDM software can then manage the sandboxed portion of the device only and encrypt and wipe data inside the sandbox as necessary. For sandboxing to be effective, the data in the sandbox must stay in the sandbox, but unfortunately, that is not always the case. Two close cousins of BYOD – BYOA (bring your own app) and BYOC (bring your own cloud) – are making it increasingly difficult for companies to employ sandboxing methods to safeguard data. BYOA includes all of the "wild" apps on your client's

employees' devices. These apps are impossible to control and it would be extremely difficult – both legally and logistically – to know, let alone regulate, what apps employees should and should not install on their devices. BYOC presents an even more complex problem. In many instances, people use cloud services on mobile devices without even knowing it. For example, many smartphones back up data to the cloud automatically and tons of apps operate in their own proprietary clouds or interface with multiple clouds at once. With this level of cross-pollination taking place, it is impossible to prevent at least some data from leaking onto a third-party cloud. And when your client's corporate data is stored on or travels through a third-party cloud, you must consider it compromised. An often-overlooked challenge with BYOD is legal discovery. If your client is engaged in litigation or involved in some other type of legal proceeding, an employee's device may become discoverable. This presents significant legal problems. People store all sorts of private information on their mobile devices, ranging from healthcare information, financial data, search results, and contact lists to family photos, social media profiles, and personal passwords. Some of this information, such as healthcare information, is legally protected, but may nonetheless be made public during the discovery process. Something as seemingly innocuous as a missed call may reveal private information if it is discovered that the call came, for example, from a psychiatrist's office. As you can see, the privacy concerns surrounding incidental or non-relevant disclosures as a result of discovery that involves BYOD are considerable. On the other hand, if it is the employee who is in litigation and he or she turns over a device for discovery, sensitive company information may be compromised in the process. Worse yet, if your client were to attempt to wipe a device subject to discovery, the punitive legal consequences may be significant. It is important for counsel to emphasize the dangers of BYOD in the discovery process to clients because it is very likely to be overlooked if not considered at the outset. BYOD presents some surprising but inevitable challenges as well. For instance, no matter how hard they try, companies will never be able to ensure that only pre-approved and authorized persons have access to their employees' devices. For example, if an employee takes his or her iPhone into an Apple store for repair, he or she has to give the device password to the technician, and in many cases has to leave the phone in the store overnight or ship it to a remote location. If your client handles financial data or healthcare data as part of its business, just leaving an iPhone at the Apple store may be considered a data breach and trigger reporting requirements. As explained above, the use of third-party apps is also problematic. For instance, many people use tools such as Siri or other personal assistant apps to send e-mails, make calendar appointments, etc. Apple stores (in the cloud) everything you tell Siri for two years. Therefore, without intending to, employees may be sharing sensitive information with unauthorized parties simply by using the common features on their phone or tablet. Implementing a BYOD program is a choice, but failing to do so may result in decreased employee satisfaction, lower performance, increased costs, and loss of competitiveness. Many of the risks associated with BYOD can be mitigated or avoided by implementing MDM solutions and encryption solutions. But as you have just read, these solutions themselves create a series of new challenges. It is up to counsel to help their clients navigate the legal hurdles involved in implementing a BYOD program and to help them develop a BYOD policy and BYOD program that combines technology solutions with clear and

comprehensive policies and procedures to help safeguard sensitive data, remain respectful of employee rights and privacy, and defend against litigation. Because the rules of the game are not clear, and because technology continues to evolve at breakneck speed, litigation is inevitable in this field and BYOD will be at the forefront of the controversy. By investing in new technology and implementing comprehensive and commonsense policies that are understandable and transparent, you can help your clients mitigate some of the exposure that has become necessary to remain competitive in the marketplace. *Originally published by the ABA's Business Law Today (September 2013).*

Related Practices

Business Transactions
Cybersecurity and Privacy
Labor & Employment