Bloomberg BNA

Corporate Law & Accountability Report™

LITIGATION

The Business (and Litigation) Case for 'Bring-Your-Own-Device' Policies

BY KAREN LEE LUST

According to an early 2015 report, *74 percent of companies* are currently using or plan to use BYOD, or ''Bring Your Own Device'' programs, which allow their employees to use their own mobile devices for business purposes. BYOD devices include employee-owned smartphones, tablets and laptops, each with potentially different operating systems, technologies and applications to create and store data—and each with their own set of information governance and e-discovery challenges. Despite the popularity of BYOD, a summer 2014 survey found that *only 39 percent of companies* have a formal BYOD policy in place. Ironically, BYOD is one of the *highest-risk areas* with regard to potential data losses. Companies that implement BYOD programs should recognize that their employees are handling potentially sensitive or proprietary company information, outside the secure environments set up by information technology within a traditional office. Moreover, any data transmitted or stored on personal devices, just like on company devices, can potentially become discoverable in future litigation.

Karen Lee Lust is an associate in Reed Smith's Litigation and Records/E-Discovery groups. Her information governance practice involves counseling clients about records management, litigation readiness, e-discovery and data privacy matters, including prevention of or responses to a data privacy breach.

Mobile devices have the advantage of enabling employees to work from anywhere. This necessarily means that a company's business records and trade secrets may travel anywhere with them. Not only might employees lose their smartphones or laptops while traveling, through theft or simple forgetfulness, but their devices could be hacked or infected with malware that can compromise company information. Terminated or otherwise departing employees may not be motivated to return or delete company proprietary information stored on their personal devices—which can be an especially thorny problem when the ex-employee goes to work for a competitor. Employees might also feel proprietary towards all data stored on their smartphones, regardless of whether such items relate to company business or not. Where employees don't understand their preservation obligations under the law, this could lead to deletion of discoverable information (whether intentional or inadvertent), and adverse legal consequences including possible spoliation sanctions.

How Can Companies Mitigate BYOD Risks?

Companies with a BYOD program should consider adopting a secure Mobile Device Management (or ''MDM'') system to protect company data for smartphones. MDM software, such as Good or Airwatch, can enable ''sandboxing'' so that company programs are run in a segregated and isolated virtual environment on the device, separated from the employees' personal applications and data. The MDM might encompass options for encryption of data, remote locking of the device, wiping/reformatting of the device, and even geotracking it. It is a wise practice for companies to adopt written BYOD policies that employees are required to agree to if they want to participate in the BYOD program.

The policy should clearly and concisely set forth the parameters of the program in easy-to-understand language. The policies should require participating employees to allow installation of the MDM system and/or

 ISSN 2330-6300

other security software on any personal devices they wish to use in transacting company business. Employees should also be notified that if they mix personal communications or data with company communications or data, their personal information may be subject to review for discovery or investigations, and the personal information may be wiped if their device is ever lost or stolen. It is a fine line for companies to walk—to monitor, control and protect company data, all while trying to respect employees' privacy and not subject employees' personal devices to unnecessarily intrusive or draconian measures. While there is not yet much case law on these issues, a number of ''best practices'' can be gleaned from the few relevant cases that have touched on BYOD issues.

What Should a BYOD Policy Cover?

A good BYOD policy should provide employees with information about why and how company data is to be protected in the BYOD environment. Furthermore, training regarding the BYOD program and policy is also helpful. A BYOD policy should state, among other things:

- By using BYOD, the employee consents to and agrees to abide by the policy's terms;
- The type of MDM software to be used, and what kinds of capabilities are being deployed on the employee device, including tracking and password protection (especially where a number of incorrect password attempt triggers a lock, delete or wipe function);
- What communication functions on the BYOD smartphone are acceptable for business use. For example, some MDM solutions may not cover text messaging;
- That the company has the discretion to take disciplinary action where it has reason to believe that an employee has violated the policy, including by: creating business records via text outside of the MDM solution, or inappropriately storing confidential information and/or other sensitive company data outside of the secure environment on a personal device;
- What happens in response to an incident of loss, hacking or theft, and how and when it must be reported to the company;
- Technological requirements and security updates that are required for BYOD devices, especially laptops;
- What happens if the employment relationship is terminated by either party; and
- Secure handling of the device (so that only authorized persons have access or are given passcodes).

The policy should make clear that company records and data may be discoverable or owned/accessed by the company as required by legal or business needs. Without this provision, employees may claim a reasonable expectation of privacy in the data created or sent even on employer-issued devices. It is important to recognize that some states have also enacted legislation mandating that employers inform their employees regarding any monitoring of their electronic communications. *See, e.g.*, Conn. Gen. Stat. § 31-48d (2008) (stating that employers must ''give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur.'')

In *Rajaee v. Design Tech Homes, et al.*, Civ. Action No. H-13-2517, 2014 BL 318273 (S.D. Texas, Nov. 11, 2014), upon a sales representative's resignation, his employer remotely wiped the employee's personally owned iPhone of all personal and business information, resetting it to its original factory settings. The employee then filed suit for the loss of his personal photos and videos, text messages, notes, e-mails and his cell phone contacts that he had built up from 2009-2013, all of which he collectively valued at over $100,000. The Southern District of Texas court, without mentioning whether or not a company BYOD policy existed, dismissed the plaintiff's claims of negligence, misappropriation and conversion. The court also found that the Computer Fraud and Abuse Act (''CFAA'') and Electronic Communications Privacy Act (''ECPA'') did not apply, because the loss suffered by the plaintiff was not considered a ''loss'' under the meaning of the CFAA, and that information on a smartphone was not ''electronic storage'' under the ECPA. While the employer prevailed before this particular court, it is a good practice to avoid, whenever practical, deleting employees' personal information. Companies should also incorporate into their BYOD policy the proviso that employees are responsible for backing up any personal information they wish to keep.

There is no one-size-fits-all BYOD policy. When adopting a BYOD policy, legal and IT departments should each provide input and the policy should be tailored to the unique business needs of the company, with consideration for appropriate industry concerns, legal risks and the company's IT structure and capabilities.

How Can Companies Address E-Discovery of BYOD Devices?

In virtually any litigation or investigation, at least some electronically stored information (''ESI'') is likely to be relevant. Courts have held that ESI may be collected from personal devices when the device was used for business purposes and contains relevant information. For example, in *Genworth Fin. Wealth Mgmt. v. McMullan*, 267 F.R.D. 443 (D. Conn. 2010), the defendants were required to provide forensic images of their personal computers to determine whether or not they had downloaded and subsequently transferred proprietary information and trade secrets.

In the recent case of *Small v. Univ. Med. Center of S. Nevada*, the defendant did not have a formal BYOD policy in place, and no litigation hold was issued despite the admission that many key employees used their personal devices for business purposes. As a result, over 25,000 potentially relevant text messages were lost on company-issued Blackberries, and two years of ESI on personally-owned devices. The e-discovery special master in that case recommended that a default judgment be entered against the defendant for its ''intentional and willful spoliation . . . that grievously and wantonly damaged the integrity of the discovery process.''

Companies need to ensure that their employees subject to a legal hold understand their preservation duties,

   ISSN 2330-6300

and that all ESI relevant to the matter may be discoverable, regardless of whether such data is stored on BYOD devices. Given the expense and complexity of collecting information from smartphones, much less the searching and review of smartphone data, once a legal hold is issued, corporate counsel should advise all employees to refrain from discussing, in texts or voicemails, any matters potentially relevant to the hold.

The legal landscape for BYOD is still developing, and additional cases will address associated issues in coming months and years. In the meantime, corporate counsel are well advised to enact a company policy that sets forth the employer and employee's rights and obligations with regard to ESI created or stored on personal devices. In addition:

- Companies should have written BYOD policies that employees must consent to before being allowed to participate in the BYOD program.
- It is a best practice to instruct employees to segregate their personal data from business data, given that business data is more likely to be subject to review and/or production.
- IT and legal departments should consider consulting with outside counsel regarding technological and policy-driven solutions that protect company data and mitigate risk.
- When implementing a legal hold, do not forget about potentially relevant data on personally owned smartphones, laptops and tablets.
- In each legal hold notice, remind all employees that text messages are not the appropriate medium for discussing or creating data that is subject to a legal hold.
- Do not automatically assume that data must be forensically collected from all personal devices in every litigation or investigation or that such data will matter. Cost and proportionality factors should be considered, especially if most relevant information available from the personal devices merely duplicates information more easily available elsewhere, such as on company e-mail servers.