New York Law Journal
GC New York
WWW.NYLJ.COM
An ALM Publication
VOLUME 248—NO. 114
THURSDAY, DECEMBER 13, 2012

TECHNOLOGY IN THE WORKPLACE

Integrating Employees' Smart Devices Into the Workplace

By **Cynthia Larose**

And **Narges Kakalia**

Companies are increasingly permitting employees to BYOD, or bring (and use) their own smart devices. Being able to use the latest, fastest, sleekest, coolest device promotes a level of employee satisfaction, and it cuts the company's overhead for devices, data, and sometimes IT support as well. But it's not entirely a win-win, because BYOD also creates practical and legal problems that every employer needs to be aware of and guard against. This article provides some practical tips on how employers can limit risk and mitigate potential losses from BYOD.

Risks Associated With BYOD

The practical and legal problems associated with BYOD arise because the device, the data stored on it, and the networks that the devices access all belong to different owners with varying degrees of security and sophistication. At a BYOD company, for example, the device belongs to the employee, who has the ability to store potentially proprietary, privileged and confidential company information on it. If the employee is a service professional—an accountant, attorney, auditor or even doctor, for example—the information the employee stores may belong to clients or patients rather than the employer. Without centralized control of data devices and the information stored on them, companies lack the ability to take traditional security measures to protect their data.

Sensitive information on the device may be stored alongside personal videos of junior league soccer and Angry Birds, which the employee's 4-year-old daughter plays daily. One mis-swipe, or wrong button hit, and the work data could be corrupted, lost or accidentally transmitted to the entire junior league. The device could be lost, stolen or hacked, leaving sensitive data in the hands of unauthorized and possibly unscrupulous individuals. The employee may back up the data to a cloud or home network, storing employer-related information alongside personal information in a potentially unsecure environment.[1] Each of these scenarios leaves a company exposed to significant liability.

BIG STOCK

To BYOD, or Not?

So what is a company to do? Some companies prohibit BYOD entirely. Others limit the number or level of employees permitted to BYOD. Still others limit the kind and quantity of data that can be transmitted, accessed or stored on an employee's device. For those that permit BYOD, some of the greatest challenges lie in balancing the need to protect data against the need to avoid privacy-related disputes with employees. Since respect for privacy is usually accompanied by a commensurate risk of data loss,

CYNTHIA LAROSE *and* NARGES KAKALIA *are partners at Mintz Levin Cohn Ferris Glovsky & Popeo.*

companies are strongly urged to draft and implement comprehensive electronic data and device use policies that put employees on notice of the risks inherent to BYOD and the consequences to the employee and the company should anything happen to the data on the BYO-device. It likely will take the combined efforts of a company's Human Resources, Information Technology, Finance and Legal departments to draft a policy that is comprehensive, realistic and enforceable. The policy should be widely disseminated, easily available for review and/or the subject of company-wide training.

Different Technical Paths

Companies can integrate smartphones, tablets and other mobile devices in a number of different ways. The most secure approach to BYOD involves "virtualization," wherein a company provides remote access to its servers. While an employee can access and use the company's data remotely, the data does not actually get stored on the employee's device, thereby eliminating the risk that the data will be lost if the device is, and minimizing the possibility of data corruption. Another method involves the so-called "walled garden" approach, wherein company-owned data is segregated from personal data in a separate, secure application. The walled garden minimizes the risk of an employee's 4-year-old daughter accidentally editing company data or emailing it to the junior league. The third option, called "limited separation," is the least secure. It permits company information to be intermingled with personal information. A comprehensive policy, however, can minimize a company's exposure from limited separation BYOD.

Ownership and Eligibility

As an initial matter, BYOD policies should set forth all eligibility requirements with specificity. Will all employees be permitted to BYOD, or only certain ones? Are all devices, platforms and networks permitted, or only ones specified by the policy?

A BYOD policy also should, at a minimum, specify corporate ownership of company information, and the company's ability to both access and control that information and data, even when it is temporarily housed on an employee's smartphone. And a policy should expressly reserve the company's right to remove all company data from an employee's device—including contacts and calendar events—upon the employee's departure from the company.

A recent First Department decision offers a cautionary tale for employers and employees alike. In *AllianceBernstein v. Atha*,[2] an investment firm sued a former employee, alleging that he had misappropriated confidential client contact information, which he then used to solicit the firm's clients in violation of his employment agreement. At his deposition, defendant admitted that during his tenure at the firm he had used his iPhone to contact clients. Plaintiff sought document discovery regarding the data stored on the iPhone, defendant resisted on privacy grounds, and the trial court intervened, ordering that the iPhone itself be delivered to plaintiff's counsel.

On appeal, the First Department vacated the trial court's order, stating that it was beyond the scope of requested discovery, and "tantamount to ordering production of [defendant's] computer." But the First Department also acknowledged that plaintiff had a right to review the non-personal information on the iPhone. In an unusual move, the First Department ordered that "the iPhone and a record of the device's contents shall be delivered to the trial court for an in camera review to determine what if any information contained on the iPhone is responsive to plaintiff's request."

The *AllianceBernstein* case is a reminder that companies should take rigorous steps to protect their confidential data, and to retrieve it from BYO-devices before an employee leaves the company. So too is it a reminder to erstwhile employees that mingling the personal and the professional can put personal information at risk of disclosure.

As *AllianceBernstein* teaches, a company should take special care to include confidentiality and nondisclosure language in its policy, address the proprietary nature of the information and data, and include specific and comprehensive information about the consequences of misappropriating or otherwise compromising company data or information, whether by accident, negligence, recklessness or intentional misconduct. Consequences can and should include loss of BYOD privileges, loss of device data, employee censure, suspension, termination and/or civil or criminal action, depending on the employee's conduct and/or the magnitude of loss or potential loss to the company or its clients.

Ethical and Acceptable Use

A company should prohibit employees from modifying the device hardware and software, including jailbreaking or rooting iPhones and Android devices respectively. While jailbreaking and rooting[3] have dubious legal credentials (it is arguably illegal to jailbreak a tablet but not a smartphone), there is no doubt such device modifications can compromise a device's security features, sometimes with potentially serious consequences.

A company's policy also should address the applicability of the company's general acceptable-use policy to BYOD usage. For example, if a company ordinarily prohibits employees from viewing online pornography on company-owned computers, does the same prohibition apply to the employee-owned BYOD? If not, is it acceptable for the employee to use his or her smartphone from the company's premises to engage in uses that otherwise are prohibited by the acceptable use policy?

Security Measures

A comprehensive use policy should require employees to undertake at least a few non-invasive safeguards against the risk of data loss. Such safeguards may include mandating PIN- or password-protection, and self-locking within a few minutes of inactivity. The policy can also require employees to ensure that they install anti-virus and anti-corruption software that meets the employer's standards; and the policy should very clearly state whether the cost of the software (installation and upgrades) shall be borne by employer or employee.

More stringent measures to protect data may include requiring account-locking after a certain number of failed login attempts, and specifying rigorous password-strength, password-rotation and other means of preventing data loss. A company may also consider prohibiting employees from backing data up to a cloud or other unsecure network.

Preemptive Measures

BYOD is a privilege and a company should explicitly retain the right to rescind BYOD privileges at any time and for any reason.

A more rigorous and comprehensive policy also should address how data stored on a BYOD will be treated when the device is decommissioned—either because it was replaced, destroyed, lost or stolen, or the employee's tenure at the company terminated. The most comprehensive way of mitigating losses is by requiring the installation of mobile device management (MDM) software on the device. MDM can provide many different security considerations, including some very invasive ones that permit employers to remotely "wipe" devices clean of data in the event of a breach, theft or loss.

MDM frequently employs GPS tracking devices. On the one hand, such devices are useful in pinpointing the location of the employee's hardware to determine where the device is located, thereby increasing the possibility of retrieving lost devices. And it can remotely wipe clean devices that have been stolen, thereby decreasing the likelihood of a significant data breach. But they can, of course, also foster the unpleasant perception that Big Brother is always watching, even when the employee is off the clock or on vacation.

To avoid potential privacy challenges, companies employing MDM should require employees to consent to MDM installation and use by express agreement to opt in to a BYOD program. Such an agreement would have employees provide informed consent for the company's use and implementation of GPS trackers and other mobility-tracking devices, as well as the company's ability to remotely wipe clean an employee's device. Such a contract should incorporate by reference the company's use policy, and both in turn should clearly reserve the company's right to access employees' devices and protect proprietary data, even when access is only possible through the most invasive means available.[4]

Finally, a company should clearly and explicitly disclaim any liability for the loss of Angry Birds, junior league videos and any other personal apps, information and software stored on an employee's device. If a BYOD is accidentally left on the soccer field or at a gaming convention, an employer's ability to remotely wipe the device should not be deterred by consideration for the employee's personal data.

While some newer and more sophisticated (and commensurately more expensive) MDM can distinguish between employer- and employee-owned information, others may not. And therefore, an employee should be willing to pay the price of risking personal data loss for the privilege of being able to use the latest, fastest, sleekest, coolest device.

Ultimately, most of the steps outlined above will be ineffectual against a planned, targeted and intentional attack on a company's proprietary data. But in all other instances—accidents, employee negligence, etc.—the steps outlined above will go a long way toward protecting company information from the hazards of BYOD.

1. While the litigation and electronic discovery risks of BYOD are clearly beyond the scope of this article, it bears noting that BYOD implicates more than just the security of a company's data. When data is backed up to a home network along with an employee's personal photographs, videos, games and financial spreadsheets, that data may no longer be subject to a company's regular data-retention policy, may become discoverable in litigation, and may put at risk of discovery the employee's other personal information stored alongside it.

2. *AllianceBernstein v. Atha*, __AD3d__, 2012 NY Slip Op. 07766 (1st Dept. 2012).

3. Jailbreaking and rooting are colloquial terms that usually refer to the process of hacking into a smartphone or tablet's operating system in order to use the device with an unapproved telecom carrier, or to add programs, apps or software that are not approved by the manufacturer for use on that device.

4. Other privacy concerns may also be implicated in specific industries or geographical areas. Companies should consult counsel about how their policies may affect, and be affected by, statutory concerns involving the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the Americans with Disabilities Act and by the laws of individual states and countries where their employees live and work.