Bloomberg BNA

Privacy and Security Law Report®

Mobile Devices

Employers are increasingly allowing employees to bring their own devices to work. However, ''Bring Your Own Device'' practices in the workplace can raise problems for businesses, including data breaches, the authors write. They outline the types of considerations a company should keep in mind when considering and drafting a BYOD policy.

"Bring Your Own Device" Policies: Issues to Consider

BY VERNON L. FRANCIS, VIVIAN A. MAESE AND THOMAS K. JOHNSON II

The ''Bring Your Own Device'' (BYOD) approach to mobile computing is now a fact of life for many of today's businesses. The increased popularity of mobile computing devices has fueled a highly competitive market that has produced a wide variety of products. Not surprisingly, users have developed preferences for certain products and have brought these preferences into their work environments. The BYOD trend also is being fueled by the demands of a workforce that is no longer tied to offices, cubicles or even a standard workday.[1] This mobilized workforce depends on devices to stay connected to their jobs. Together these trends have convinced some companies to give their

 ISSN 1538-3423

employees a greater say in what devices they use on the job, by embracing policies that allow employees to use personally owned devices to connect and interact with their employers' business networks.[2]

BYOD advocates claim that giving employees the choice to use their own products for work can make them happier and more productive. But it has also become clear that BYOD practices also can raise a number of problems for businesses. Data breaches are the most serious concern. According to a recent New York Times article, almost half of the companies that allow personally owned devices to connect to their corporate networks have experienced a data breach, either because of employee errors or intentional wrongdoing.[3] From a legal perspective, maintaining company and personal data on the same device can lead to misunderstandings and disputes between businesses and their employees about privacy and other issues. The company's loss of control over the devices its employees use for work can interfere with the company's ability to comply with various legal obligations or adequately monitor its operations for compliance purposes. If not handled correctly, moreover, a BYOD regime can threaten not only the security of data that the company is lawfully obligated to protect, but can also endanger the company's own intellectual property and business confidences.

If your company is considering moving towards a mobile computing model that would allow BYOD use, serious consideration should be given to a number of different factors. From a legal and compliance standpoint, the central component of a company's BYOD strategy should be the adoption of an appropriate policy to guide interactions between the company and its employees on mobile computing issues. This article outlines the kinds of considerations the company should keep in mind when considering and drafting such a policy.

Formulate a Mobile Strategy Before Drafting a BYOD Policy

A workable BYOD policy should start with the adoption of a mobile strategy that fits the organization's needs. To some extent, this is putting the cart before the horse—despite its growth in popularity, a BYOD approach to mobile technology will not be the right solution for every organization. For example, if preserving the security or confidentiality of the organization's internal communications is a major concern of the business, the risks that can accompany the expansion of BYOD usage may outweigh the organization's interest in the convenience or personal preferences of its employees and managers. Employees may come to resent the costs of maintaining a BYOD policy to them personally, and the company's information technology department may not appreciate the additional strains BYOD may put on its personnel and budgets.[4]

In the end, the formulation of a company's technology strategy and the role that BYOD might play in that strategy are primarily business decisions. But these decisions must be informed by the regulatory environment in which the business operates and, in particular, how that environment will respond to breaches or other threats to the integrity of the organization's data.

By working with compliance, IT, human resources and other relevant enterprise partners, the company's legal team should be able to identify the regulatory and business concerns that should influence the contours of a viable mobile integration strategy. Does the business have legal obligations to customers or clients that require special care with regard to preserving the confidentiality of information entrusted to it? Does the kind of data maintained by the business attract the attention of criminals, competitors or, increasingly, foreign governments, making the company's systems a particularly attractive target for hackers? What are the potential costs in terms of reputation and dollars should an attempt to breach the company's systems succeed? How much will the business have to invest in additional hardware, software, personnel and training to make a BYOD strategy successful from a data security standpoint?

It may well be that taking all of the relevant variables into consideration, a company may decide that a rule requiring that all of its business be conducted with company-owned technology is the better alternative. Or the company could decide to continue to rely primarily on communications through company-owned equipment, but allow BYOD usage to increase at a reasonable pace after a pilot program provides information on what would be needed to sustain BYOD use by company employees on a broader scale.

A company's business strategy and regulatory concerns must be the key drivers in shaping the enterprise's mobile technology strategies.

The point of this article is not to suggest any one particular strategy choice as a default option. Rather, it is to suggest that moving some or all of a company's mobile uses to BYOD should not be the product of casual decision-making. Nor should such a decision be solely or primarily driven by employee preferences or the technology department's fascination with a particular technology. As the growing popularity of mobile computing itself suggests, rapid changes in mobile technology and in the variety of mobile products available to users are to be expected. There will always be tech-savvy managers and employees who will want the newest innovations—like iPhones and Androids over Blackberries, or tablets over (or with) laptops. Some of these new products may even prove to be useful to the enterprise as a whole, while others will disappear with the next trend.

Businesses have shown that they can adapt to these technological changes, but integrating them into the operations of a business takes time and planning. Especially in an environment like this one, where new products are introduced constantly, a company's business

[2] *See* Nicole Perlroth, *Bolstering a Phone's Defenses Against Breaches*, N.Y. Times, Oct. 13, 2013, *available at* http://www.nytimes.com/2013/10/14/technology/bolstering-a-phones-defenses-against-breaches.html.

[3] *Id.*

[4] *See, e.g.*, Steve Ranger, *BYOD: 10 Reasons It Won't Work for Your Business*, ZDNet, July 5, 2012, http://www.zdnet.com/byod-10-reasons-it-wont-work-for-your-business-7000000050/.

  PVLR ISSN 1538-3423

strategy and regulatory concerns must be the key drivers in shaping the enterprise's mobile technology strategies.

Adopt a Policy—Then Train

Once your company has decided on a BYOD strategy, it needs to adopt a policy. The policy should be clear and complete, and readily available to all employees in places where they can reach it. Although these policies will apply to everyone in your organization, keep in mind that they will be most important to the managers and employees who are least likely to work from a desk in one of the company's offices, much less its headquarters.

The adoption of a BYOD policy should serve at least three important purposes:

1. *Notice*—For the employees who choose to use their personal devices for work purposes, the policy communicates their employer's expectations with regard to how the device will be used and maintained, and how company data stored on the device will be utilized and protected. Notice of the employer's intentions with regard to monitoring compliance also can allow employees to make informed decisions about what personal information to store on a dual-use device.

2. *Consent*—To the extent that the employer seeks the right to search and, when necessary or appropriate, to remove content from an employee's device, obtaining the employee's consent in advance to such interventions is crucial. Courts have held that employees have no legitimate expectation of privacy in their workplace computers when the company makes it known that its network will be monitored.[5] But this type of consent does not extend to an employee's *personal* e-mail accounts or to information stored on the employee's own equipment.[6] Employers can risk violating computer privacy, data protection laws and common law tort liability if these devices are accessed without proper authorization.[7] Thus, access to an employee's personal accounts or device must be expressly covered in the employer's policy to be effective.[8]

3. *Communication*—The company's presentation of its BYOD policy should be viewed as an opportunity for communication and discussion about the employee's technology and support needs, and should cover concerns they may have about the policy. Such discussions may reveal that for some employees, using the same device for personal and business purposes is not the right solution for them, and some other approach is needed.

For BYOD to work, employers and employees must see themselves as partners in managing the company's data utilization and protection strategy. A good policy can help to promote this partnership. The right kind of policy, coupled with training and adequate communication, can encourage employees to be vigilant about avoiding the security risks inherent in smartphone and tablet use. For their part, companies can encourage their employees to ''buy in'' by making sure their employees are educated on the policy, by ensuring that employees' technical and support needs with regard to company-based applications are met, and by taking steps to protect their employees' privacy, including obtaining consent before monitoring practices are implemented.

Contents of the Policy

An effective BYOD policy should promote cooperation between the employee and the company with regard to the use, maintenance and security of the employee's mobile equipment. The policy should ensure the employer has reasonable access to the device for legitimate business purposes whenever needed, while assuring the employee that the company will make reasonable efforts to respect his or her interest in privacy and to protect his or her personal information from deletion or corruption wherever possible. The point is to anticipate potential problems and, through proper application of the policy, implement workable solutions to the issues that can cause confusion or misunderstandings in advance, so that employees can work productively and without surprises and the company can feel confident that its business interests are being adequately protected. Key areas of concern are:

Access

Employers need reasonable access to the BYOD user's device to install and upgrade software, and to retrieve documents or other information when necessary to comply with subpoenas for discovery purposes, to conduct internal investigations or for other legitimate business purposes. The company may also want to seek the right to inspect the employee's device periodically to be sure that the employee's use of the equipment is consistent with company policies.

The company should warn employees using BYOD that bringing their personal devices in for service and/or inspections will be a routine occurrence under the policy. Both employer and employee will have to work together to make these interactions run smoothly and efficiently—a good policy will facilitate this cooperation. Understanding that the interactions will occur regularly might also encourage employees to comply with company policies regarding joint uses of mobile equipment more conscientiously.

Employers have to be transparent about the access they seek to their employees' devices. It has to be clear when they are monitoring employee communications and what employee communications they are

[5] *See, e.g.*, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 559–60 (S.D.N.Y. 2008).

[6] *See id.* at 560–61.

[7] For a discussion of these issues, *see* Philip Gordon, ''Managing the Evolving Challenges of Workplace Privacy and Information Security,'' *Recent Trends in Privacy and Data Security* *4–*5 (Mar. 2013).

[8] *See Sitton v. Print Direction, Inc.*, 718 S.E.2d 532, 2011 BL 333203, 535–38 (Ga. App. 2011) (employer not liable to discharged employee under relevant statutory law or in tort for viewing and printing e-mails from employee's personal account and from employee's personally owned laptop computer where at the time of the access the computer was linked to employer's network and company's computer usage policy authorized employer's access under circumstances presented) (10 PVLR 1463, 10/10/11).

monitoring.[9] Employers risk both liability and the loss of their employees' trust if they fail to appreciate the importance of transparency.

Finally, it is especially important when thinking about access issues to remember that a policy is not just something to be pulled out and dusted off in an emergency. Policies are supposed to be blueprints to guide interactions on a daily basis. Part of the purpose of training on the policy is to integrate the policy into the routine of the business to minimize disruptions and misunderstandings. This is especially important when it comes to access issues.

Security

The company will want to consider including provisions in the policy on where company data can be stored when using the device, restrictions on who can use the device and other requirements related to data security, such as requiring the use of passwords. If there are particular kinds of software or applications that should be avoided by BYOD users because they pose risks to the company's data or operations, or software applications needed to protect the security of the company's network, the policy also should include provisions that address these issues.

Two security provisions are of particular importance. First, employees should be required to report the theft or loss of their devices immediately, so that the company may take steps to protect its data and company systems in a timely fashion. Second, employers should secure their employees' consent through the policy to ''wipe'' at least the company's data from the employee's equipment at any time, but especially in the event of theft or loss of the device. If some or all of an employee's personal information may be lost as a result of the employer's decision to ''wipe'' a personally owned device, the employer should inform employees of this specific risk through the company's BYOD policy.

The company's policies also should require that departing employees turn their devices over for removal of the company's data before leaving the company. This part of the policy can result in uncomfortable situations if the employee is leaving because he or she has been terminated, and especially if the termination is being contested in some fashion. Hopefully making employees aware of the requirement at the outset of their tenure with the company will reduce some of the tensions that might result under more difficult circumstances.

Company Policies

Employees should be reminded that when using even their personal devices for company purposes, they will still be expected to follow all other company policies governing the use of communications systems, such as prohibitions on the texting or forwarding of sexually or racially harassing or otherwise inappropriate material. They also should be reminded that while their device is being used for dual purposes, the company expects them to follow all laws related to use of the equipment (e.g., no texting while driving, etc.).

Once mobile, the intellectual property assets of the company are now widely accessible. Specific reminders of the company's intellectual property ownership interests and the employee's obligations to keep company information confidential are especially important to articulate.

Other Important Provisions

If the company as part of its strategy offers to finance or partially finance the employee's purchase of his or her mobile equipment, the terms under which the company will provide the financing should be clearly outlined, as should any agreements about who has rights of ownership in the equipment at any given point, and the timing of any attendant changes in ownership. If the company decides that it will support only certain kinds of devices for BYOD use or that it will only support the use of particular carriers for BYOD equipment, these limitations should be communicated through the policy as well. Again, the point of a good policy is to minimize the potential for misunderstandings and disruption of the business through litigation or other adverse occurrences. Being as clear as possible about who will pay for what can only help in this regard.

Mobile policies have to be viewed as a central component of an organization's overall data retention and security regime.

Training

Finally, adopting a policy is not enough. Mobile policies have to be viewed as a central component of an organization's overall data retention and security regime. Training that explains the key points of the policy and how BYOD fits into the company's overall scheme for utilizing and protecting its data is vital if the company's resources are to be protected adequately. Moreover, a framework should be in place to monitor employees' and the company's adherence to these policies, and to respond to employee questions or concerns as they occur. Technical, security and other staff charged with supporting BYOD users must be trained on the company's policies and subject to appropriate supervision.

Conclusion

Evaluating the appropriateness of BYOD as a business tool and drafting an appropriate BYOD policy will require time and careful review by many stakeholders in the company. Some of the core considerations listed above can help a company get started with the process, but they are only a beginning. In the end, an effective policy must be adapted to the company's particular needs, obligations and practices, as well as the data pri-

[9] For discussions of these issues, *see, e.g.*, Steven Musgrave, *BYOD—Security Risks and Policy Solutions*, 18 No. 9 Cyberspace L. 6 (Oct. 2013); Pedro Pavón, *Risky Business: ''Bring-Your-Own-Device'' and Your Company*, Bus. L. Today *1–*2 (Sept. 2013).

  PVLR ISSN 1538-3423

vacy and security concerns of its customers or clients. The best policies will allow employees flexibility, while encouraging and enabling them to act as partners in protecting the enterprise's data security interests.

  PVLR ISSN 1538-3423