Global Data Privacy and Security Team

Privacy and Bring Your Own Device: At A Glance

Many companies permit their employees to use their personal mobile devices, such as smartphones and tablets, to access company-specific information, such as email, under a Bring Your Own Device ("BYOD") policy. BYOD policies can be popular for employee that want to use their hand-picked device and for employers who avoid the cost of providing, and maintaining, company-owned devices. Nonetheless, the use of company data on non-company devices implicates both security and privacy considerations, and companies should consider several questions when deciding how best to balance the two.

People who will bring smartphones to work by 2017, according to research firm IDC.[1]	Estimate by a multinational company of increased employee time by adopting a BYOD policy in 2009.[2]	Organizations that currently allow or plan to allow BYOD.[3]
328 MILLION	**$300** MILLION	**74%**
Percent of employees in the US that use their personal smartphones for work purposes.[4]	Percent of employees that log onto their business email while on sick leave.[5]	Percent of companies that report having complete awareness of what devices access their networks.[6]
90%	**42%**	**<10%**

Consider the following when deciding upon a BYOD policy:

✓ Is the scope of the company's control over the employee's mobile device consistent with and limited to the company's interest? Companies should consider why they have an interest in knowing about their employees' mobile devices; that interest should be the basis from which the BYOD policies should emerge. If the company simply wants to allow an employee to access work email on a mobile device, then the policies and restrictions should proceed with that focus.

✓ To what extent and for what purpose does the company monitor employees use of mobile devices? Many servers create logs showing when an employee's device accessed the company server using certain authentication credentials. As security measures such logs are often appropriate. To the extent that the company wants to monitor more substantive actions by an employee on a mobile device, such monitoring needs to be in-line with an appropriate purpose.

continued on back

[1] http://www.computerworld.com/article/2487005/byod/with-byod-smartphones-on-the-rise--it-headaches-will-become-migraines.html
[2] http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/Cisco_IT_Insight_BYOD.pdf
[3] http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
[4] https://iapp.org/media/pdf/knowledge_center/Cisco_BYOD_Insights_2013.pdf
[5] http://www.clicksoftware.com/globalassets/aasite_assets/images/infographics/power-of-mobile-infographic.pdf
[6] http://www.ingrammicroadvisor.com/big-data/23-byod-statistics-you-should-be-familiar-with (Aug. 18, 2015)

For more information on state data breach notification laws or to subscribe to the Bryan Cave Breach Notification Survey contact:

John C. Bush
Associate
john.bush@bryancave.com
One Atlantic Center, 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
phone: 404 572 6600

Carolyn K. Rincon
Associate
carolyn.rincon@bryancave.com
1290 Avenue of the Americas
New York, NY 10104-3300
phone: 212 541 2000

BRYAN CAVE

Consider the following when deciding upon a BYOD policy: (continued)

- What procedures are in place to restrict the transfer of data from the company's network by way of the mobile device? Companies often protect against the risk that company data will be "floating" on multiple devices by (a) limiting the types of data accessible to mobile devices (e.g., email) and (b) restricting, to the extent possible, how that data can be used on the mobile device (e.g., policies on copying and requiring certain security settings).

- For security purposes, does the company require a minimum versions of the operating system and/or software before the employee can use a mobile device? Minimum versions ensure that certain security protections and bug fixes are present on the device.

- Can data on a mobile device be remotely wiped? By whom? A best practice for devices that contain confidential or sensitive company information is to ensure that the data can be remotely deleted from the device if needed.

- What procedure is in place for an employee to report a missing mobile device? Accidents happen to everyone, but their aftermath can determine whether they become catastrophes. Employees should report a missing device to someone – perhaps the IT department or help desk – so that the company's device removal policy can be followed.

- What steps does the company take to proliferate its mobile device policies? Companies often rely on their IT staff, self-help materials, employee certifications, and a combination of these approaches to ensure (a) employee awareness of company policies and (b) enforcement of company policies.

- Do the security measures in place match the sensitivity of the data accessed through the mobile device? For some employees that receive non-sensitive information minimal restrictions may be appropriate. For employees that receive sensitive or confidential information higher restrictions may be called for.

- Is BYOD required of the employee? Although BYOD programs are widely lauded for increased productivity and "off-the-clock" accessibility, this very benefit can expose employers to potential wage-and-hour issues where the BYOD user is a nonexempt employee.