Don’t Let BYOD Mean Bring Your Office Disaster

Southeastern Business Law Institute
October 24-25, 2013
Cumberland School of Law
Samford University

Richard C. Balough
BALOUGH LAW OFFICES, LLC
1 N. LaSalle St. Suite 1910
Chicago, IL 60602
312.499.0000
rbalough@balough.com
www.balough.com

Don't Let BYOD Mean Bring Your Office Disaster

By Richard C. Balough[1]

I. Is BYOD the New IT Norm?

Does your company allow employees to bring their own personal smartphones, iPads, netbooks, laptops, or other mobile devices to the office and allow them to access your computer network with those devices? Do you allow your employees to access your network *remotely* with their own devices? If so, you are not alone.

It's estimated that nearly two-thirds of businesses now allow employees to bring their own devices (BYOD) and use them as their corporate desktop or allow the mobile devices to access company data, including sensitive data, not just emails.[2] By 2014, the number of employee-owned smartphones and tablets will reach 350 million, compared with 150 million in 2012.[3] The touted benefits of BYOD include:

- Increased productivity and innovation.
- Employee satisfaction, including the benefit of not having to carry multiple devices.
- Cost savings by shifting costs to the user.[4]

---

[1] Richard C. Balough is a member of Balough Law Offices, LLC in Chicago, Il., practicing in the area of intellectual property matters. He can be reached at rbalough@balough.com. He is co-chair of the Mobile Commerce subcommittee of the Cyberspace Law Committee of the American Bar Association (ABA). This paper expands on research conducted by Mr. Balough and Theodore Claypoole, of Womble Carlyle, presented at the ABA's Business Law Section Spring 2013 meeting.

[2] KnowBe4 and ITIC Latest Study Reveal Companies Lack Security for "BYOD," September 4, 2012, available at www.prweb.com/releases/2012/9/prweb9858074.htm.

[3] Seven BYOD policy essentials, October 1, 2012, Networkworld, available at www.networkworld.news/2012/100112-byod-262932.html.

[4] BYOD: Bring your own device, Why and how you should adopt BYOD, available at http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html.

Many highly qualified employees simply refuse to work for a company that does not meet the worker's technology needs, which includes allowing them to use their own devices in the workplace with access to the company's network. Access to the network can take many forms, but the four basic models are:

- Unlimited access for personal devices;
- Access only to non-sensitive systems and data;
- Access, but with IT control; and
- Access, but without local storage of data on personal devices.[5]

II. BYOD Creates Legal and Security Risks.

Access to the network raises both security and legal risks. Company information is no longer held exclusively by the company on its secure network. "This loss of control clashes with the growth over the last decade of government regulations requiring companies to carefully protect the privacy and security of sensitive personal, financial, and health-related data. It also poses risks to the protection of a company's trade secret, proprietary, or confidential information."[6] Companies should identify and analyze the various risks to the enterprise – technology risk, obsolescence risk, data security risk, reputation risk, competitive risk, risk of system failure – when formulating a BYOD policy. In an ideal world, the policy should precede the technology.[7] However, many companies are playing catch-up by formulating a policy well

[5] BYOD: Bring your own device, Why and how you should adopt BYOD, available at http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html.
[6] The Bring Your Own Device to Work Movement, Engineering Practical Employment and Labor Law Compliance Solutions, May, 2012, available at http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf.
[7] The Ten Commandments of BYOD, MaaS360, available at http://www2.maas360.com/services/maas360-ten_commandments_of_byod_bring-your-own-device.php.

after employees already have brought their devices to the workplace and connected to the company's network.

A. Allowing BYOD raises legal issues.

There are many legal questions that arise from employees bringing their own devices to the workplace. For example, everything an employee does on her personal iPhone could be used as evidence in a lawsuit against her employer.[8] If the employee buys a new device, what happens to the information stored on it? If the employee quits, does all the smartphone-stored data go with him? The company may not be able to discipline an employee for loose treatment of the company secrets unless the company has a written policy in place to address worker responsibility related to smartphones and tablets. A personal device may have software under a personal, not business license, or even a program that is not properly licensed. A business may be putting itself at risk for intellectual property infringement without even knowing.[9]

Various laws and regulations impact the use of employee-owned devices. They include:

- **Employment law.** If the employee-owned device is used by a non-exempt employee and the non-exempt employee checks her email or other work-related documents, then the employee should keep track of her off-the-clock time related to these activities and be paid for it pursuant to the Fair Labor Standards Act. The relevant time includes all time that employees are "suffered or permitted" to perform work.[10] Is the employer required to monitor employee-owned devices to

[8] 6 Risks Your BYOD Policy Must Address, Information Week, Nov. 19, 2012, available at www.informationweek.com/smb/mobile/6-risks-your-byod--policy-must-address/240142320.
[9] BYOD could open businesses to copyright litigation: BSA, February 4, 2012, available at www.zdnet.com/au/byod-could-open-businesses-to-copyright-litigation-bsa-70000010533/?s_cid=e539.
[10] 29 U.S. C. §§ 203(g) and 207(a).

ensure that there are no violations of any equal employment opportunity violations, including discrimination and harassment?

- **Workplace safety.** If an employee suffers injury such as repetitive stress using the employee-owned devices, is the employer liable under the Occupational Safety and Health Act of 1970?[11] If an employee is distracted by the employee-owned device while driving, is the employer liable for any resulting accident or damage?
- **Computer Fraud and Abuse Act (CFAA).**[12] If an employer improperly accesses an employee-owned device, can the employer be liable under the CFAA for unauthorized access or access exceeding authorization?
- **Stored Communications Act (SCA).**[13] If an employer accesses an employee-owned device, can the employer be liable under the SCA? A business may not be able to exert the kind of control it needs over its own data without the employee acknowledging and accepting such control as a precondition to using the employee's own equipment.
- **Copyright Act.**[14] If an employee has unlicensed software on his employee-owned device, can the employer be subject to an action for contributory infringement by allowing the employee to use pirated software for work?
- **Litigation holds.** Is the information on an employee-owned device within the possession, custody, or control of the employer? If an employer is sued, is the information on an employee-owned device subject to any litigation hold?

[11] 29 U.S.C. § 651 *et seq.*
[12] 18 U.S.C. § 1030 *et seq.*
[13] 18 U.S.C. § 2701 *et seq.*
[14] 17 U.S.C. § 10l *et seq.*

- **Trade secrets.** If an employee using an employee-owned device has access to and downloads trade secret information of the employer onto the device, has the information lost its trade secret classification? What happens if the BYOD policy does not contain reasonable measures to maintain the confidentiality of the trade secret information?
- **Privacy.** When an employee uses an employer-owned device, the general rule is that there is no expectation of privacy for the employee. But if the employee uses his own device, does the employee then have a reasonable expectation of privacy for what is on the employee-owned device? What personal information about the employee can the employer gather by accessing the employee-owned device, such as private medical information?

Each of these legal risks should be evaluated and addressed when drafting an effective BYOD policy.

B. Allowing employee-owned devices in the workplace may create security risks.

In addition to legal issues, allowing employees to bring their own devices to the workplace and connect to the network raises security issues. Because the devices are not under the control of the company, there is a risk that the devices can be used by the employee to improperly use data, allow the data to be exploited by others, cause a security breach, or introduce malware into the company's network.

By allowing company data to be downloaded and stored on an employee's device, the company loses control over the data. An employee may use his device to access the network via a public Wi-Fi connection, exposing the data to third parties. While a company may have enterprise level security measures, that level of security may be lacking on an employee-owned

device, creating huge security holes.[15] Security also could be compromised if the employee loses the device or loans it to a third party. Moreover, there is a security risk because some apps obtain data from other apps, which could lead to security breaches.

A company BYOD policy should address the security issues in a manner that protects the company while allowing the employee to bring his own device.

III. Only a Small Percentage of Employers Have a BYOD Policy.

Of the companies which allow BYOD, unfortunately only a small percentage have BYOD policies. One survey found that only 13 percent have specific BYOD policies in effect and another nine percent are working on a policy.[16] A 2013 survey found the number was 36 percent with a BYOD policy, another 32 percent expect to have a policy in the next 12 months, and 16 percent have no current plans for a policy.[17]

Executives of those companies without BYOD polices should feel a sense of urgency about developing and implementing them. In addition to the risks identified above, allowing employees to tap into the company network with uncontrolled devices can lead to significant regulatory risks. Highly regulated companies in the financial services and healthcare industries must account for personal information wherever it sits within their systems. For example, in the healthcare sector, a BYOD policy must comply with security standards under the Health Insurance Portability and Accountability Act of 1996 (HIPPA), as well as amendments to the HITECH Act of 1999. Failure to properly implement a BYOD program may result in increased

---

[15] Dealing with BYOD Security Risks, Redmond Magazine, May 14, 2013, available at http://redmondmag.com/articles/2013/05/01/byod-empowers-users.aspx.
[16] *Id.*
[17] Rachel King, Cisco, BY Survey: Only 36 percent of companies have a BYOD policy, Between the Lines, June 6, 2013, available at www.zdnet.com/cisco-bt-survey-only-36-percent-of-companies-have-a-byod-policy-7000016432.

penalties for HIPPA or HITECH violations.[18] If the personal information can reach the edge of the network and slip out to employee-owned technology, then the company likely has regulatory reporting requirements. Such data could be considered to be exposed or even lost under certain data breach notice laws and regulations.

Another significant risk resides with the information that an employee keeps on his handheld device. Without the ability to block access to certain websites, a company is more vulnerable to finding risky information like the trade secrets of a worker's previous employer or even child pornography, and acquiring legal liability for the possession of such information. For example, possession of child pornography is a strict liability offense, and a company that finds such information on its system gains, at the very least, the responsibility for notifying the proper authorities about the discovery.[19] If there are a competitor's trade secrets held on a new employee's iPad or even a thumb drive and that company has an ambiguous BYOD policy, then this situation could impute liability to the company.

Mobile technology is also more vulnerable to government confiscation and review, especially when crossing borders. The United States Department of Homeland Security's Customs and Border Protection has unambiguously declared that it will exercise its right to analyze the data and databases contained on mobile technology arriving at the U.S. border, from demanding access codes to laptops to insisting that smartphones be switched on and turned over to the border guards.

---

[18] Attorneys Detail BYOD Issues in Health Care, HealthData Management, September 24, 2012, available at www.healthdatamanagement.com/news/mobile-computing-devices-security-hippa-hitech-45007-1.html.

[19] *Jane Doe v. XYC Corporation*, Superior Court of New Jersey, Appellate Division, December 27, 2005, No. A-2909-04T2, finding that an employer, upon finding that an employee was viewing child pornography on a company computer, had a duty to act by either terminating the employee or reporting his activities to law enforcement authorities.

A company's BYOD policy should address these risks and seek ways to minimize the risks while meeting the desire of employees to bring their own devices and connect to the company's network.

IV. Formulating a BYOD Policy Is a Team Effort.

Solving a company's BYOD issues involves a detailed examination of the company's technology, its priorities, its employment guidelines and procedures, and its willingness to impose corporate wishes onto its workforce. A policy also must take into account the employee's expectation of privacy. A recent study found that 82 percent of employees are concerned about employers tracking the websites they visit on their personal devices and 86 percent are concerned about the unauthorized deletion of personal data.[20] In other words, any old policy will not do. Grabbing a generic BYOD policy off the Internet and forcing it upon employees is not a real answer. The company should ask a number of important questions. The company's management should understand the technology and identify management priorities. Only then can a truly effective policy be implemented by the company.

Elements that a company should consider when devising its BYOD policy include its own data privacy and security, its preference for technological control over all devices, and its employees' rights and desire to bring their non-business lives into the company's workplace. As expressed by the United States Supreme Court in *City of Ontario v. Quon*, 560 U.S. 746 (2010), even a public employee may have a reasonable expectation of privacy in certain emails and messages sent and received on city-issued mobile devices. The court there was not even addressing the complex data capacity of today's smartphones, but considered only two-way pager devices that were issued to employees a decade ago and that would likely be deemed

[20] BYOD Privacy: Are You Being Watched? October 2, 2012, Networkworld, available at www.networkworld.com/news/2012/100112-byod-privacy-are-you-being-262950.html.

antiquated by today's teenagers and young professionals. At the very least, a company considering whether it wants employees to supply their own devices and accept work correspondence on those devices must consider the following questions:

- *Does the Company want to embrace and encourage employee-owned devices at work, will it be neutral but allow employee-owned devices, will it discourage employee-owned devices but allow them sparingly, or will it simply prohibit employee-owned devices?*

The general terms of an employer's BYOD policy will likely be driven by how deeply the employer embraces the BYOD concept. For example, if the employer allows only certain members of its sales force to supply their own devices for use in the workplace, then it is likely to build a policy around the needs of its sales team, and not be concerned about the risks involved with other workers. Conversely, if the business allows only certain members of the executive suite to use their personal iPads for work purposes, the risk profile is entirely different. Clearly, prohibiting employee-owned devices keeps much better control over company data, while allowing broad use of personal smartphones and tablets in the business raises numerous questions. Enthusiastically embracing such technology usually means integrating the employees' devices through company-issued software, and building policy statements and procedures into the company's employee handbook.

- *What qualifies as an employee-owned device and what may or must the device contain?*

Many levels of personal data devices can be included within a company's BYOD policy, and the types of devices allowed within the business set the boundaries for the company's policies. Most businesses allowing employee-owned devices speak directly to smartphones and

many issue company software that may be (or must be) downloaded onto those phones. Conversely, the policy may prohibit using some programs. For example, IBM banned its employees from using Dropbox and Apple's iPhone assistant Siri.[21] Many businesses do not allow outside laptops within their enterprise security firewalls, choosing instead to issue company-managed laptops. However, there is no reason that laptops could not fall within a BYOD policy. Some early adaptors of the BYOD movement have addressed smartphones, but have not yet adjusted for the rise of tablets, which are a more robust work platform and raise additional risks. Finally, some companies build employee-owned thumb drives into their BYOD policies because taking electronic information outside the firewall on a thumb drive is similar to sending it to your personal smartphone or tablet.

- *What is the company's device encryption policy?*

When and to what extent does the business require encryption? Does the business require encryption of all information on smartphones and tablets? Does it require encryption of company data at rest and in motion? Must the employees use company-issued encryption, or does the company offer standards for the level of encryption allowed on employee-owned devices? Encryption is becoming the standard for all businesses and will likely be nearly universal for responsible businesses, so a company's decisions on encryption of mobile devices are likely to affect its liability for data loss. Such encryption is already legally significant in jurisdictions like California, where data on a lost device is not considered exposed if the device was adequately encrypted.

[21] BYOD Risks and Rewards, Sophos, *supra*.

- *How much technical control does the business want to exert over its employees' devices?*

A business must decide to what extent it wants to use new technologies to control employee devices used at least in part for company purposes. Is the business comfortable allowing employee-owned devices into its enterprise architecture without any business-protective software? Many corporations will allow employee-owned devices, but only if those devices include business software that monitors use of the device, location of the device, and management of the data on the device. Some businesses will not allow employees to introduce smartphones into the business system without the company installing software that provides the ability to remotely wipe all information off the smartphone when it is lost or stolen. Of course, if a company wishes to install such remote-wipe software, it should include notice of this fact in the employee handbook or a separate BYOD policy. The company should insist that employees sign a "permission to be wiped" statement in exchange for the right to use their own devices with company data to avoid a later dispute as to whether permission was obtained. Often there is not a convenient and consistently effective method of wiping the business data off a device without wiping the employee's personal data as well – her music, her contact list, her pictures. This deletion risk should be disclosed to employees.

- *What disciplinary regime will be triggered by failure to comply with the company's BYOD policy?*

Policies are only as good as a company's enforcement of them. Is the business willing to fire a salesperson for surreptitiously bringing his device into the enterprise network? Would this be true for a senior executive who does the same? Companies should include a clear and consistent policy on what will happen to an employee who breaks company BYOD rules. A

company might consider removing BYOD violations from the standard disciplinary regime and treat violations in a separate set of rules, so that violators are encouraged to come into the fold and follow the rules, rather than hide their transgressions. This is especially true for those companies that do not actively advertise their BYOD policies and procedures.

- *How will the company divide costs for the employee's device?*

Often, the right to exercise control over an employee's smartphone or tablet is reinforced by company payments supporting that device. Handheld computers are expensive, and employees will incur costs for purchasing the device, for connecting the device to telephone systems, and for data usage on the device. The company could choose to cover some or all of these costs, for example, granting employees reimbursement for data usage to cover business activities on the handheld computer. Providing some or all of the payment for purchase or use of an employee's device can make for an easier argument that the employer should have the right to remotely wipe the device in times of trouble or otherwise control it.

- *What business information will a company allow to be stored and processed on employee-owned devices*?

When a personal device is used for business purposes, it will inevitably contain company information. A company can choose to allow employees to access only email on their personal smartphones, but otherwise not have access to company databases and documents. It could allow access to only certain systems, but not others. A personal mobile device can be a full extension of the company's network and systems, but it may be substantially more limited in access. Many businesses have sophisticated access controls where access is allocated by personal identification or by the type of device requesting data access. The company's decisions about how much of the company network is accessible by the employee's personal device will affect its BYOD policy.

Thoughtful companies will write their solutions into policy so that they can assure consistent and careful treatment of the technology and people using it. Ultimately, the success of a BYOD policy is measured by the employees' willingness to use their devices within the policy rules.[22] In other words, a viable BYOD policy must recognize the expectations and desires of their employees to bring their own devices, must protect the integrity of the IT environment, must address a potential minefield of legal issues, must be clear and understandable, and must be embraced and followed by those affected by the policy.

[22] BYOD Risks and Rewards, Sopha, *supra*.

SAMPLE
FOR ILLUSTRATIVE PURPOSES ONLY
NOT INTENDED TO BE A FINAL POLICY

COMPANY
Bring Your Own Devices (BYOD) Policy
Dated: _____

Purpose

The purpose of this policy is to provide guidelines for COMPANY employees who bring their own electronic devices to access applications, data, computers, and networks maintained by COMPANY (COMPANY).

Policy

COMPANY is committed to maintaining the integrity of its computer network, its data, the data of its customers, and all COMPANY confidential, proprietary, and trade secret information (COMPANY Data) that may be hosted or stored on servers, applications, or computers owned and maintained by COMPANY (COMPANY System). Pursuant to this policy and the restrictions herein, an employee may bring his/her own Device (BYOD), such as laptops, netbooks, tablets, and smartphones (collectively, Devices) to access COMPANY Data and the COMPANY System. The employee must act in a legal, ethical, responsible, and secure manner with respect to the rights, privacy, and protection of COMPANY, its customers, COMPANY Data, and the COMPANY System. In the event an employee does not comply with the policies and procedures in this BYOD policy, or other COMPANY policies and procedures, COMPANY, in its sole discretion, reserves the right to revoke such BYOD privileges and, if necessary, take appropriate action against any employee who violates this BYOD Policy.

Inappropriate use of Devices to access COMPANY Data or the COMPANY System exposes COMPANY to risks including compromise of COMPANY Data or the COMPANY System, legal issues, financial loss, and damage to reputation. The purpose of this policy is not to impose restrictions that are contrary to COMPANY's established culture of openness, trust, and integrity, but to protect COMPANY, its employees, and customers from illegal or damaging actions either knowingly or unknowingly by individuals.

Procedures

An employee may use only COMPANY approved Devices in conjunction with this BYOD Policy. An employee shall not access any COMPANY Data or the COMPANY System using a Device without first receiving written consent from _____. Therefore, prior to purchasing any Device for use under this BYOD Policy, the employee should contact _____ for approval of the specific device. The consent is for each individual Device and for a specific unique device identifier (UDID). COMPANY shall not reimburse an employee who purchases his/her own Device for use at COMPANY, nor shall COMPANY reimburse an employee for any usage contract or other service provider expenses. The employee will be personally responsible for all such costs.

BYOD Devices accessing any COMPANY Data or the COMPANY System must:

1. Have approved encryption features and such encryption features must be activated at all times.
2. Have installed and operating COMPANY's mobile device management software.

3. Must be password protected at all times with a password containing a minimum of six characters including at least one letter and one number (except on devices that cannot accept alphanumeric passwords). Passwords must be changed at least every 90 days.
4. Must automatically lock after ten failed attempts to enter a password and the Device may be subject to being wiped clean remotely by COMPANY.
5. Must lock at least every 30 minutes, requiring reentry of the password.
6. Must operate an updated version of an antivirus program approved by COMPANY, unless such device is incapable of having an antivirus program installed.
7. Must utilize only browsers approved by COMPANY.

BYOD Devices will be subject to (a) monitoring for harmful programs and applications; (b) content filters and quarantining of harmful content and materials; (c) Device tracking in order to support recovery efforts in the event of lost or stolen BYOD Devices; and (d) periodic inspections, audits, and examinations to confirm use of Devices in accordance with this BYOD Policy and other COMPANY policies and procedures. As a result, an employee has no expectation of privacy in the data or information on any Device under this BYOD Policy.

An employee using an approved BYOD Device shall not:

1. Use any camera function or Bluetooth capabilities while on COMPANY premises.
2. Permit others to use the BYOD Device, even if such use is intended for non-COMPANY purposes.
3. Take any BYOD Device across an international border.

4. Erase or delete any information or data on the BYOD Device if the Device is subject to a litigation hold.

COMPANY may remotely wipe a BYOD Device without notice to the employee in the event: (a) an employee loses the BYOD Device; (b) the employee leaves COMPANY either voluntarily or involuntarily; (c) COMPANY detects a virus, malware, or any data or policy breach involving the DEVICE; (d) an incorrect password is entered into a BYOD Device ten consecutive times; or (e) an employee informs the COMPANY of the employee's intent to return, sell, destroy, dispose of, or otherwise transfer a BYOD Device.

In the event a Device is lost or stolen, the employee must immediately notify _____ within 12 hours of realizing that such Device has been lost or stolen. In the event that the Device is not recovered within 24 hours of the notice, COMPANY may wipe the BYOD Device, including all COMPANY applications, programs, and content and some or all of the Device's non-COMPANY content.

An employee seeking to use a BYOD Device shall execute a release of liability that releases COMPANY from any claim of damages to the Device or its content as a result of any wiping of the Device by COMPANY, a crash of the operating system, errors, bugs, viruses, other hardware or software failures, or programming errors, which could render the Device inoperable.

SAMPLE
FOR ILLUSTRATIVE PURPOSES ONLY

RELEASE OF LIABILITY AND DISCLAIMER TO USERS OF PERSONAL DEVICES

You hereby acknowledge that, by using your BYOD Device in connection with COMPANY'S business, such device will be exposed to certain risks for which you, as the user, assume full liability. By signing below, you agree to accept the risks and to fully release and discharge COMPANY from any claim by you for any actual, direct, indirect, or consequential damage arising out of or in connection with your use of your BYOD Device. The risks include the partial or complete loss of data, including your personal data, as a result of a crash of the operating system, errors, bugs, viruses, other software or hardware failures, or programming errors, which could render the BYOD Device inoperable. You recognize that participating in the BYOD Program is a privilege and that COMPANY may revoke your privileges under the program at any time, in its sole discretion. You further understand and agree that the COMPANY may install a program or app on your BYOD Device and, at any time and without prior notice to you, may remotely wipe the COMPANY'S data from your BYOD Device, if the COMPANY reasonably believes that the BYOD Device may have been compromised or you are in violation of the COMPANY's BYOD Policy. Such remote wiping of the COMPANY's data may also result in the wiping of any personal data on the BYOD Device.

_____

DATE: _____