

Avoiding BYOD Legal Issues

**Route1 Inc.
September 2013**

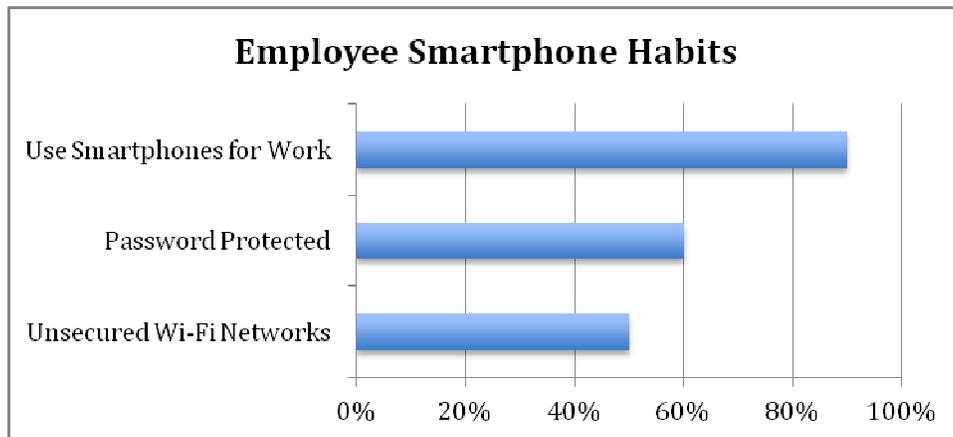
Avoiding BYOD Legal Issues

Today's business landscape is facing emerging legal issues stemming from bring your own device (BYOD) initiatives. The shift towards the use of personal computing devices (laptops, tablets, smartphones and now watches) to conduct business in theory is a win-win strategy for both the Enterprise and its employees. Enterprises avoid costs associated with providing devices and employees can work using the personal devices they are already comfortable with.

In reality, BYOD poses serious legal problems for the Enterprise.

Protecting Data or Breaking the Law?

BYOD is undoubtedly convenient, but it poses grave risks to Enterprise security. Simply put, BYOD devices are not currently used in a secure manner. Although 90% of American workers use their smartphones for work, only 60% use password protection to lock their device.¹ Perhaps more alarming, 50% frequently connect their smartphones to unsecured Wi-Fi networks.²



Poor BYOD security habits mean that sensitive Enterprise data is often unsecured and easily accessible to malicious third parties. Of course, Enterprises want to prevent their information from falling into the wrong hands. The question is: do security concerns give businesses the right to protect their data by remotely monitoring and wiping an employee's personal device?

^{1 2} Cisco: "BYOD Insights 2013."
<http://www.cisco.com/c/en/us/solutions/collateral/enterprise/enterprise-byod-190801.pdf>

Current Practice: Erasing and Tracking

BYOD means that employees often co-mingle personal and business information on their devices. Generally, device software has few measures to distinguish between sensitive Enterprise data and the owner's personal information.

When an employee's device is compromised (hacked, stolen, etc.), the Enterprise wipes *all* data on that device – both business and personal. Enterprises have no other option to protect their sensitive data, but the destruction of employees' personal property is legally ambiguous.

Another common practice is GPS tracking. If an employee's personal device contains confidential Enterprise information and is lost or stolen, the Enterprise may use the device's GPS capabilities in an attempt to locate it. Again, this strategy is legally unclear as it raises issues of monitoring employee whereabouts.

Various legal issues arise from these practices:

1. Current Legal Environment: Gray Area

As of now, the BYOD security strategies outlined above are not illegal. There is no current regulation nor is there case-law that has set precedent. What is becoming more common is the practice of asking employees to sign a waiver giving their consent to have their specific personal devices wiped or tracked should a security breach occur.

Anthony Davis, who runs IT for a manufacturing company in Seattle, elaborates, "We actually have a one-page waiver that says, you know, if you're going to connect your personal phone to the corporate e-mail system, that we do have the capabilities if the phone is lost to remote wipe it – and we will – and then have the employee agree [to] and sign that form."³

When an employee is fired or leaves the Enterprise on their own, retrieving Enterprise data from the personal device becomes an issue. It is unclear if an organization has the right to remotely track or wipe an ex-employee's personal device. Once fired, an ex-employee is just that: no longer employed by the

³ NPR: "Wipeout: When Your Company Kills Your iPhone."
<http://www.npr.org/2010/11/22/131511381/wipeout-when-your-company-kills-your-iphone>

Enterprise and thus potentially not bound by the Enterprise's BYOD policy. The legality of this scenario remains in a gray area.

Such waivers are legally questionable. If an employee agrees to sign one, they have no choice but to have their personal information tampered with or have the location of their device monitored should a security situation warrant it. If they refuse to sign, the employer has no other option than to fire them on the spot. Additionally, there are concerns as to whether or not these waivers are legally binding, and it is unclear how an Enterprise enforces them.

Lewis Maltby, president of the National Workrights Institute, notes, "Now, you have this gray world in which everything overlaps, and everything that's personal is business and vice versa, and now it's a mess."⁴

Even when an employee has given his written consent to BYOD security policy, the Enterprise can still be liable under certain circumstances. If a security breach occurs and the Enterprise feels the need to remotely monitor an employee's device, the employer could mistakenly view personal information that it is not legally allowed to see. For instance, the Genetic Information Non-discrimination Act of 2008 prohibits employers from collecting genetic information about their workers. Another example: the Enterprise may see something about an employee's disability – information that is legally protected under the Americans with Disabilities Act.

This waiver system raises serious questions about employee rights, and the threat of litigation is growing steadily more serious.

John Marshall, CEO of AirWatch, an enterprise mobile device management vendor, states, "I anticipate a bunch of little [lawsuits], then something big will happen that'll be a class action and become headline news."⁵

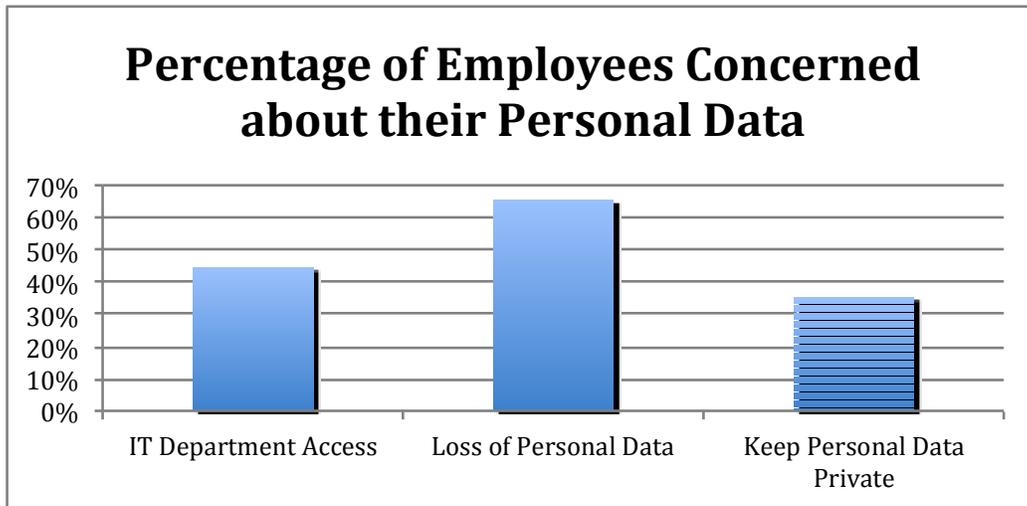
The growing tide of employees disgruntled over BYOD security practices reinforces Marshall's prediction.

⁴ NPR: "Wipeout: When Your Company Kills Your iPhone."
<http://www.npr.org/2010/11/22/131511381/wipeout-when-your-company-kills-your-iphone>

⁵ CIO: "BYOD Lawsuits Loom as Work Gets Personal."
http://www.cio.com/article/732156/BYOD_Lawsuits_Loom_as_Work_Gets_Personal

2. Employee Reaction

Recent studies show that American workers have major concerns about BYOD security policies that invade their privacy. Of those surveyed, 45% worry about their employer's IT department having access to their personal data; 66% are concerned about losing personal data when using their own devices for work; and 36% want to keep all of their personal data hidden from their employer's IT department.⁶



Unsurprisingly, employees do not want the Enterprises they work for to view their personal information. In fact, 46% of American workers would feel “violated” if their IT department accessed personal data on their devices, and 20% would react with anger.⁷

Current BYOD security policies are legally questionable and invasive. Employee discontent is growing across many sectors, including the federal government.

3. Freedom of Information Act

Employees of private Enterprise are not the only members of the American workforce concerned with BYOD security. Federal government workers are equally threatened by the invasion of privacy stemming from the current practice of tracking and wiping personal devices. The Freedom of Information Act states that

^{6 7} Aruba Networks: “Employees tell the truth about your company’s data.”
http://www.arubanetworks.com/pdf/solutions/EB_mdmreport.pdf

any person has a right to obtain federal government records. If a federal employee uses their personal device for work, any GPS monitoring of said device must be recorded by the government agency and can be publicly disclosed.

Given this, federal workers have to worry about the general public accessing their private information via the Freedom of Information Act. Current BYOD security policies threaten the privacy of Enterprise *and* government employees, leading to growing discontent and the potential for union involvement.

4. Union Backlash

Workers' privacy rights are increasingly threatened by BYOD security policy. Negative employee response will continue to grow if the wiping and tracking of personal devices goes unabated. History shows that as the American workforce galvanizes around an issue, labor unions inevitably become involved. Labor unions are committed to representing their members and protecting them in any and every way. Specifically, unions work tirelessly to defend workers' privacy rights.

If unions take action against BYOD security in favor of employee privacy, the Enterprise may face a prolonged and expensive legal battle. Unions have the resources to mobilize their members, file lawsuits and draw a significant amount of negative publicity, potentially causing serious reputational damage to the Enterprise.

5. Government Litigation

Lawsuits from current or former employees are not the only legal issues facing the Enterprise regarding BYOD. In many instances, if sensitive information is leaked from an employee's personal device, an Enterprise can face penalties from the government. For example, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), healthcare organizations are required to safeguard protected, electronic health information. The U.S. Department of Health and Human Services has recently obtained seven-figure settlements from healthcare organizations that failed to protect patients' health information.

Additionally, businesses that store Social Security, drivers' license, credit and debit card and financial account numbers have strict information security obligations in many states. For example, Massachusetts requires encryption of such information when stored on mobile devices. But, when an employee accesses the encrypted data

to work on it remotely, he must decrypt that information, thereby leaving it susceptible to hacking or malware. The loss of decrypted information, in theory represents a failure to comply with state security obligations regarding sensitive data. The Massachusetts Attorney General has recently obtained monetary penalties from Enterprises that have failed to meet these requirements. A breach of security on an employee's personal device can lead to government enforcement actions, civil penalties and litigation.

Another Approach: Standing Pat

Some Enterprises are well aware of the potential legal pitfalls of BYOD security policy. These Enterprises recognize that current practice *could* potentially lead to litigation, which they want to avoid for a myriad of reasons.

Enterprises in this camp are unsure of what to do regarding BYOD security and do not want to tread on employee rights. These Enterprises do not attempt to wipe or track personal devices, nor do they ask employees to sign waivers. While this strategy avoids legal issues, it leaves sensitive Enterprises data unprotected.

BYOD security concerns leave Enterprises in a difficult position. Enterprises either use legally ambiguous means to protect their data or they avoid the issue altogether, leaving their information unsecure and vulnerable to cyber theft. Either way, the potential for financial loss is grave.

Endpoint Security Software: The Bottom Line

Current BYOD security policy requires the Enterprise to purchase endpoint security software, specifically mobile device management (MDM) software, for all mobile devices in the network. The effectiveness of such software is dubious, as the average malware detection rate for leading anti-virus software brands is only 19%.⁸ Despite its ineffectiveness, MDM software is expensive. The hard costs for purchasing, implementing and upkeep, depending upon the size of the Enterprise, can easily reach hundreds of thousands of dollars per year.

Besides being unreliable and expensive, MDM software for mobile devices is a nightmare for IT departments. Repairing, replacing and managing mobile security consumes a considerable amount of an IT desk's time. MDM software is an

⁸ Lumension: The True Cost of Anti-Virus: *How to Ensure More Effective and Efficient Endpoint Security*.
<http://www.slideshare.net/LumensionSecurity/the-true-cost-of-antivirus-how-to-ensure-more-effective-and-efficient-endpoint-security>

ineffective and expensive BYOD security option that wastes countless hours that could be devoted to other projects.

Fortunately, another option for BYOD security exists.

Effective and Legal BYOD Security

The underlying cause of the BYOD security issues outlined above is the concept of allowing Enterprise data to be downloaded and saved on a personal device. Employees must not be able to extract data from the Enterprise network. Removing data from behind the Enterprise firewall and storing it on a smartphone or tablet allows an organization's information to be at risk of falling into the wrong hands. Whether it is hacking for profit or cyber-terrorism, mobile data security is a serious and rapidly growing issue.

Given today's fiscal and global environment, employees must be able to telework without storing sensitive data on their personal devices. Doing so allows for secure use of BYOD, preventing breaches and legally ambiguous responses by the Enterprise. The best approach is to use mobility technology that prevents Enterprise information from ever leaving the office.

MobiKEY

MobiKEY is Route1's flagship technology. Using a smartcard enabled, cryptographic USB device, it ensures that an employee leaves no trace or evidence of their computing session on their personal device. All Enterprise files stay within the Enterprise firewall, simplifying security policy enforcement.

If MobiKEY is lost or stolen, Enterprise networks cannot be compromised in any way – unlike other portable devices that can be used to store sensitive Enterprise data and can easily put organizations at risk. Just as a credit card or cell phone service can be suspended or cancelled when loss or theft occurs, digital certificates issued to MobiKEY can be temporarily suspended or revoked.

MobiKEY allows Enterprises to protect their data in a BYOD environment without risking mass litigation. Sensitive information never falls into the wrong hands, and there is no need to tamper with employees' devices.

Conclusion

BYOD is a growing phenomena. With MobiKEY, Enterprises can be assured that BYOD is secure and complies with legal standards. MobiKEY eliminates data breaches and the potential of litigation while ensuring financial stability.

For More Information Contact:

Tony Busseri, CEO

+1 416 814-2635

tony.busseri@route1.com

© Route1 Inc., 2013. All rights reserved. Route1, the Route1 and shield design Logo, SECURING THE DIGITAL WORLD, Mobi, MobiSecure, MobiLINK, Route1 MobiKEY, Route1 MobiVDI, MobiKEY, MobiKEY IBAD, DEFIMNET, MobiNET, Route1 MobiNET, TruOFFICE, TruFLASH, TruOFFICE VDI, MobiKEY Fusion, MobiNET Aggregation Gateway, MobiNET Switching Array, MobiNET Secure Gateway, EnterpriseLIVE, EnterpriseLIVE Virtualization Orchestrator, MobiNET Agent, MobiKEY Classic and MobiKEY Classic 2, are either registered trademarks or trademarks of Route1 Inc. in the United States and or Canada. All other trademarks and trade names are the property of their respective owners. The DEFIMNET and MobiNET platforms, the MobiKEY, MobiKEY Classic, MobiKEY Classic 2 and MobiKEY Fusion devices, and MobiLINK are protected by U.S. Patents 7,814,216 and 7,739,726, Canadian Patent 2,578,053, and other patents pending.

Other product and company names mentioned herein may be trademarks of their respective companies.