The Legal Implications of BYOD: Preparing Personal Device Use Policies

By David Navetta, Esq. – ISSA member, Denver, USA Chapter

This article lays out the key considerations security professionals, lawyers, and compliance personnel should take into account when creating personal device use policies and outlines some of the important provisions that are often found in such policies.

Security, privacy, and incident response issues are often important drivers in a company’s decision to pursue a bring-your-own-device (BYOD) strategy and set the scope of personal device use within their organization. If the risks and costs associated with BYOD outstrip the benefits, a BYOD strategy may be abandoned altogether. The failure to address these risks can result in legal compliance complications and potential liability. One of the primary tools (if not the most important tool) for addressing such risks are BYOD-related company policies. Sometimes these policies are embedded within an organization’s existing security and privacy policy framework; more frequently, however, companies are creating separate personal device use policies that stand alone or cross-reference existing company security, privacy, and incident response policies. This article lays out the key considerations security professionals, lawyers, and compliance personnel should take into account when creating personal device use policies and outlines some of the important provisions that are often found in such policies.

General personal device use policy development considerations

Genie out of the Bottle?

One of the assumptions often reflected in conversations about BYOD is that the organization has the luxury of creating a BYOD strategy based on a blank slate. The reality, however, is that the BYOD genie is already out of the bottle for many organizations. A recent survey of organizations conducted by Cisco1 found that 95% of surveyed organizations were permitting employees to use their own devices in some form in the workplace. According to the same study, each “connected worker” will have as many as three devices connected to employer networks by 2014.

Therefore, from a policy development point-of-view, organizations should first analyze what BYOD-related activities may already be occurring, including:

- Who is using personal devices?
- What kind of information is being stored/processed/transmitted on those devices?
- How are personal devices connecting to the organization’s internal networks?

The first rule of policy development and compliance is to create policies that can be followed and will be followed when implemented. Policies should not be aspirational but should reflect the “reality on the ground” as closely as possible. If certain BYOD activities are already taking place, it may be necessary to develop policies that reflect those activities or terminate or limit certain activities on a going-forward basis. Ongoing BYOD activities will influence the development of

the company’s ultimate BYOD strategy and the decisions on the scope of BYOD use. Ideally, these decisions should occur before policy drafting begins (although in some cases the exercise of drafting policies can help clarify issues and shape BYOD strategy).

Control mix and policy flexibility
BYOD-related policies should also be viewed as only one control amongst many types of controls that can be used to reduce risk. Technological controls also need to be considered in this context because policy-based controls are only effective to the extent the policies are followed by individuals. A violated policy is essentially just a piece of paper (or worse, a piece of paper arguably establishing a legal standard of care that is not being followed). More significant risks may need to be addressed with technological safeguards to take out some of the “human element” (e.g., establishing an encrypted virtual private network (VPN) connection to company networks; setting up a “sandbox” for corporate information on a personal device; implementing location and or wiping technology). Overall, the policy and control set around BYOD should be made flexible enough to deal with unusual situations. This is especially important in the BYOD context because personal device technology and risks are constantly evolving at a very rapid pace.

BYOD and existing policies
In many (or most) cases, an organization already has certain policies in place that may relate to or address some BYOD concerns, including acceptable use policies, mobile security policies, encryption policies, password policies, social media policies, wireless access policies, incident response policies, and human resource policies and handbooks. Companies considering BYOD need to review these existing policies and determine if they impact their BYOD strategy and policy development.

The crucial concern at this point is consistency between existing policies and BYOD policies. For example, many mobile device security policies dictate detailed configuration and security requirements, all of which are possible when the company owns and centrally controls the device. These policies may apply to all mobile devices, and from a definitional point of view the policies may not make a distinction between company-owned devices and personal devices.

If not adjusted, the company could be setting the same standard for personal devices as company-owned devices, and that standard may not be achievable (individuals do not, and often cannot, secure their mobile devices the same way a company can). At the same time, drafting different policies for personal devices could result in two different standards, which could pose liability risk to the extent the standards related to personal devices are less rigorous.

As such, a fine balance needs to be struck, and organizations should strive to meet their security, privacy, and other compliance obligations when it comes to personal device use, despite differences between company-owned and personally-owned devices.

Ultimately, a review of existing policies will illuminate the organization on how to develop its personal device use policy framework. Potential choices in creating and maintaining a BYOD policy include:

- Relying on and modifying existing policies to address BYOD concerns
- Creating a completely separate stand-alone Personal Device Use Policy
- Creating a separate Personal Device Use Policy, but cross-referencing it against, and relying upon, relevant existing policies where appropriate

Regardless of the choice made by the organization on policy structure, in many cases existing policies will need to be modified to ensure that proper distinctions are being drawn between personal and company-owned devices, and that existing policies are not over- or under-inclusive when it comes to addressing BYOD issues.

BYOD and the personal device use policy implementation process
When developing personal device use policies, the work does not stop at drafting the policy itself. Organizations also need to consider the process around implementing, training on, and enforcing those policies. For example, many companies establish a process for registering, authorizing, and inventorying personal devices that will be used for company purposes. This allows an organization’s security and investigation teams to track devices and data, and understand the true scope of the company’s computing resources and network.

A process for presenting personal device use policies and training employees is also important. Companies will want their employees to understand the limitations surrounding the use of their personal devices after they start using them for company reasons. Training takes on a bigger role in this context because it is necessary to reverse the “personal device mind set” and have employees think of their personal devices more like they do company-issued devices. Organizations also need to consider how to implement and notify employees concerning changes to their personal use policies, including training on new material changes to the policies.

Companies must also consider the process for executing a BYOD consent/waiver agreement with employees. This consent and waiver should address some of the more sensitive is-

---

The Legal Implications of BYOD: Preparing Personal Device Use Policies | David Navetta

sues surrounding the company’s personal device use policies (e.g., expectations of privacy, investigations and device and data access, responsibility for loss, and damage and loss of use), and require employees to agree to limitations of liability. It is not unusual to require employees to reconfirm their consent and waiver on a regular basis and when personal device policies materially change.

**Personal device use policy provisions**

BYOD implicates a wide range of compliance and legal issues, and some of these issues will vary depending on the scope of a company’s BYOD strategy, the information processed by personal devices, and industry-specific issues and legal requirements. The following discussion concerning potential personal device use policy provisions is not intended to be comprehensive, and the presence of particular provisions will vary depending on the specific circumstances and BYOD strategy of an organization. Nonetheless, many of these provisions commonly appear in personal device use policies.

**Key definitions**

As mentioned above, for policy purposes, companies will often have to make distinctions between company-owned devices and personal devices. Therefore, the definition of personal device, including distinguishing what constitutes a personal device (e.g., a personal cell phone free of any company restrictions on access to certain webpages, use of third party applications, etc.) versus a company device (e.g., a company-issued smartphone, a laptop with keystroke monitoring, company firewalls, network access restrictions, etc.), is an important part of any personal device use policy.

Another important definition relates to “prohibited information.” Many companies are allowing personal device use, but are prohibiting the storage of certain sensitive personal or company information on those devices. The definition of prohibited information can be used to set this limitation via policy, in which enforcement of such prohibitions may include methods such as deactivation and removal of access credentials from company networks, as well as disciplinary action. However, many companies are realizing that it is also important to buttress policy restrictions with technology that disallows the processing of certain information on personal devices.

Finally, as discussed further below, the definition of “security incident” is important for the purpose of adequate incident response policy. The definition of security incident should include the concept of reasonably suspected security incidents (where a device owner is responsible for reporting any actual or reasonably suspected incidents of hacking or unauthorized disclosure of information contained on the device) and address lost devices (regardless of whether there has been any evidence of unauthorized access to the lost device).

**Personal device system requirements, configuration, and limitations**

While an organization may not be able to mandate detailed system and configuration requirements for personal devices, it is not unusual to require minimum basic requirements in a personal device use policy. Device configuration requirements may include enabling wiping (also known as “brick-ing”) capabilities of a device, disabling automatic back-up or cloud storage of data stored on a device, prohibiting the use of a personal device as a mobile hotspot, requiring or prohibiting certain application installations, enabling auto-patching for operating systems and applications, and prohibiting jail breaking or unauthorized modding of devices. The policy will often also require employees to install mobile device management or other software on personal devices. These system, software, and configuration requirements often vary depending on the particular type of personal device and/or operating system, and may need to be updated when new devices are being used or new security vulnerabilities discovered.

**Personal device security requirements**

Personal device use policies should address security requirements and concerns. Legally speaking, the security policies and controls around personal device use should strive to reach a level of “reasonable security” and address applicable regulatory or contract requirements. The challenge in the personal device context is checking the company’s existing security policies, and even if personal device use is not consistent with those existing policies, the company should still design personal device policies that reflect reasonable and compliant security in the personal device context. Ultimately, many companies will have a different control set for personal devices, and that is fine as long as the company can still argue that those controls are reasonable (despite not matching existing policies) in the context of maintaining adequate measures to safeguard the privacy and security of confidential information as required by law, regulation, and/or contractual provision.

Significantly, employees are responsible for the security of their devices and this should be indicated in the policy. Other key security provisions include limiting permissible connectivity to company networks and laying out wireless access limitations and requirements. In addition, the policy will typically identify “prohibited information” that cannot be stored on personal devices. It is also not unusual for security requirements in personal device use policies to address encryption, antivirus, and password/passcode/patterncode requirements (to the extent general policies may exist, it is not unusual to see cross-references to such general policies). The personal device use policies also may prohibit the sharing of any personal device (e.g., between the employee and

---

18 – ISSA Journal | November 2012 ©2012 ISSA • www.issa.org • editor@issa.org • Permission for author use only.
spouse, children, friends, etc.) – this is a good example of a policy that may go against the typical expected use of a personal device.

Employees should be put on notice that copies of all of their data may be obtained by the organization in the event of an actual or reasonably suspected security breach.

**Personal device policy provisions**

The personal device use versus corporate device use dichotomy is the most stark when it comes to privacy. An employee that has used his or her personal device may consider many of the activities and information on that device private, including personal account numbers, identification numbers, social security numbers, photos, videos, web-surfing history, chat history, personal emails, personally identifiable information, usernames, passwords, and financial information. Moreover, according to one study, 82% of employees that are subject to BYOD policies consider the ability to be tracked “an invasion of their privacy.”

For example, in the public sector context when it comes to investigations of employees, we have seen case law arguing for an invasion of privacy related to the personal use of a company device.

When a personal device is used for company purposes, any expectation of privacy will need to be disclaimed in the personal device use policy. These policies will often indicate that the organization has a right to monitor personal device use, including while connected to the company network, on the device itself, and potentially data transmitted from the device. Personal device use policies should also put people on notice that any information on their device may be accessed or viewed by the company, especially in the context of security incident situations and investigations, audits, and litigation. Nonetheless, even with proper expectations set, most companies will strive to avoid employee information on personal devices when possible.

**Investigations and incident response**

A personal device use policy should lay out expectations and requirements related to security incident response and company investigations. The main difference in the personal device context, as compared to company-owned devices, is that the devices are owned and possessed by the employees. This can make prompt access to and investigation of devices and data residing thereon difficult.

It also raises potential privacy issues. For example, in a normal data breach situation it is typical for a forensic investigator to take an image of the entire device. It may be difficult, or even impossible, to distinguish between data relevant to the investigation and personal employee information, as every bit of data is captured in the image and it is often necessary to broadly investigate a personal device to discover the cause and scope of a data breach. Employees should therefore be put on notice that copies of all of their data may be obtained by the organization in the event of an actual or reasonably suspected security breach.

The personal device policy should identify the types of incidents and investigations where possession and access to a personal device may be necessary (e.g., internal assessments, investigations and audits, security incident response, forensic assessments, subpoenas, court orders, and discovery requests). The policy should require employees to promptly provide their device when requested for an investigation, and should also mandate that employees provide passwords to access their device and decrypt data stored on a personal device, if necessary. In addition, the policy should put the employee on notice that he or she may not be able to use the device during the course of an investigation. This may be problematic to the extent an employee relies on his or her device for personal use reasons.

---


Another aspect of incident response involves locking, brick-
ing, disabling, and wiping lost or stolen personal devices. The configuration requirements of the personal device use policy should already mandate the enabling of such capa-
bilities (and many companies develop internal processes for confirming that configuration). The incident response sec-
tion of the policy should require employees to cooperate and refrain from interfering with efforts to wipe, lock, or disable a device. Alternatively, depending on the capability to alter functions on the device, the company may have the option to “sandbox” areas of the phone that relate to confidential information, such that those areas where confidential information is stored are subject to complete company control re-
garding tracking, wiping, and bricking. Under this method, using software, the company may be able to dictate to the device when and where certain data should be maintained on the device, and set different controls and rules for that data, including the ability for the company to remotely wipe the “sandbox” while leaving the rest of the data maintained on the phone untouched.

The personal device use policy should also put employees on notice that wiping a device could result in the permanent loss or corruption of their personal data and software. In addition, the company should reserve the right to wipe devices that are sold, retired, re-provisioned, released, reassigned, or disposed of by the employee, or that are no longer being used for company purposes.

**Liability and damages**

It is important for the personal device use policy to indicate that the organization is not responsible for any damage, data costs, corruption or deletion of data or software, loss of use, or liability associated with the use of a personal device for company reasons, including the risk of the device being in-
fected with malware (i.e., viruses, unwanted third-party software) being introduced onto the personal device via the company network. The policy should notify employees that use of a personal device for company purposes is voluntary (assuming that this is true) and at their own risk. These important provisions should also be present in the consent/ waiver agreement executed by each employee.

**Conclusion**

Unfortunately, implementing a BYOD strategy and developing personal device use policies is not a one-size-fits-all exercise. In most cases significant privacy, security, and legal challenges exist, and those challenges will vary depending on a multitude of factors that are specific to the organization, its industry, and the scope and substance of its BYOD strategy. Most organizations will have to analyze their existing IT environment and policies to ensure that specific BYOD issues are being adequately addressed, and that the organization’s internal policy framework is relevant and consistent to the rapidly changing mobile device environment. Developing a personal device use policy will help legal and compliance personnel focus on key challenges, and hopefully will help to reduce risk to an acceptable level.

**About the Author**

David Navetta, Esq., CIPP/US, is one of the founding partners of Information Law Group LLP (www.infolawgroup.com). David has practiced law for over fourteen years and focuses on technology, privacy, information security, and intellectual property law. He has previously served as a co-chair of the American Bar Association’s Information Security Committee, has spoken and written fre-
quently concerning technology, privacy, and data security legal issues, and can be reached at dnavetta@infolawgroup.com.