



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 10 | Number 2

Article 4


2015

The "Bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges

Carla J. Utter
University of Maryland University College

Alan Rea
Western Michigan University; University of Maryland University College

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Utter, Carla J. and Rea, Alan (2015) "The "Bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges," *Journal of Digital Forensics, Security and Law*. Vol. 10 : No. 2 , Article 4.

DOI: <https://doi.org/10.15394/jdfsl.2015.1202>

Available at: <https://commons.erau.edu/jdfsl/vol10/iss2/4>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



THE “BRING YOUR OWN DEVICE” CONUNDRUM FOR ORGANIZATIONS AND INVESTIGATORS: AN EXAMINATION OF THE POLICY AND LEGAL CONCERNS IN LIGHT OF INVESTIGATORY CHALLENGES

Carla J. Utter, Esq.

Adjunct Professor, University of Maryland University College
Current Employee, United States Federal Government
Washington, DC 20230
Cjutter.esq@gmail.com

Alan Rea, PhD

Professor of Information Systems, Western Michigan University
Adjunct Professor, University of Maryland University College

The first author of this paper is a lawyer, licensed in the State of New York and District Columbia and currently is a non-active adjunct faculty member at the University of Maryland University College and an employee with the Federal Government. Any comments can be addressed to the first author at Cjutter.esq@gmail.com. The views expressed in this paper by the first author are that personally of the first author and not the US Government.

Alan Rea is a Professor of Information Systems at Western Michigan University and an Adjunct Professor of Information Assurance at the University of Maryland University College.

ABSTRACT

With the expansion of technology and the desire to downsize costs within the corporate culture, the technology trend has steered towards the integration of personally owned mobile devices (smartphones) within the corporate and enterprise environment. The movement, known as “Bring Your Own Device” (hereinafter referred to as “BYOD”), seeks to eliminate the need for two separate mobile devices for one employee. While taken at face value this trend seems favorable, the corporate policy and legal implications of the implementation of BYOD are complicated by significant investigatory issues that overshadow the benefits of utilizing BYOD. In this paper, we set a context for the BYOD conundrum, then examine associated corporate policies, highlight the limitations to the digital investigator’s reach regarding digital evidence and review the investigatory challenges presented by BYOD. We conclude by offering recommendations such as implementing proper policies/procedures, utilizing Mobile Device Management, corporate owned devices, and enforcing agreements.

Keywords: Data, Employee, Policies, Device, Technology, Investigation, BYOD, BlackBag

1. INTRODUCTION

Around the year of 1970, Intel Corporation Co-Founder Gordon Moore predicted that the processor speeds and power of computers (based upon the number of transistors used in chips) would double approximately every 24 months (Intel Corporation). This correct prediction has encompassed standard computers, laptops and mobile devices alike including, but limited to, cellphones and tablets. As clearly evidenced by Moore’s law over the last 40 plus years, technology continues to evolve at this spectacular rate. Subsequently, policy, procedure and regulations are often ill-conceived or not timely enough to address the concerns that come with society’s co-dependence on the latest technology (and desire to use the latest product). Further, any technological advances to address regulatory and policy concerns are often stymied by the slow progression of the policy/regulatory reaction and the dynamic evolution of technological advances.

Despite delays many policies and regulations attempt to address some of the latest developments and trends; however a litany of other issues are created in the process. One such issue is the use of personal BYOD implementations in the corporate environment instead of utilizing corporate owned devices. The corporate environment is making the BYOD shift due to the realized cost savings; however, a comprehensive cost benefit analysis must consider and account for all of the regulatory/policy issues and investigatory pitfalls that ultimately will arise from the use of the personally owned smartphones and other devices within enterprise.

In this paper, the authors start with an overview of technologies normally included

with the BYOD framework, and then move into the advantages of disadvantages organizations of BYOD initiatives. The authors examine relevant prior implementations noting benefits and drawbacks. In the next section, relevant laws and their organization impact are discussed, looking at established cases that may set precedent that organizations should consider along with some mitigation and handling techniques for the digital forensic examiner (hereinafter referred to as “DFE”) for navigating in the realm of BYOD and corporate structure. Following that section, various mitigation techniques are discussed and addresses including both technical and administrative aspects.

2. LITERATURE REVIEW

In the context of this research, “BYOD” refers to a personal electronic device, mainly laptops, tablets and smartphones that can be attached to the corporate network and/or access corporate resources. In previous years, BYOD primarily focused upon cell phones (i.e., “dumb phones”), USB thumb drives and USB Hard Drives (such as removable storage drives). As more of the workplace now focuses on the evolved devices of the smartphone, tablets and laptops, not much focus will be given to the previous BYOD concerns. The author is not stating that all of the previous BYOD concerns are addressed by all companies these days, in fact, many private companies allow USB and other storage devices without any impunity (most Governmental organizations prohibit by policy and technical controls the access to these devices). Lastly, some research will be conducted in light up the new and upcoming technology, such as smart watches, smart cars and the like.

2.1 Interconnectedness

As with most technology, there are tangible benefits to be realized by an organization that utilizes BYOD. For example, by having all employees (or even a majority) connected to the network and/or corporate resources via BYOD, the side effect is having a more connected workforce for telework/telecommute and after-hours purposes. Further, cost savings may be realized by the organization in the absence of lease programs for the devices (via associated fees), fewer device purchases (hardware, less maintenance) and less IT management overhead (Hinkes, 2014).

Traditionally, corporate enterprises would allocate cell phones (i.e., Blackberrys) and laptops for its employees to use during travel and off-business time for his/her business usage. Another definition of BYOD is “any policy that allows workers to supply a platform that they connect to work through” (DiMarco, 2013). Depending on the policy of the organization, these devices are used by the employee for combined business and personal use or either strictly for business. Without a BYOD policy, an employee is generally in possession of at least two devices—one for business and one for personal usage.

2.2 Infrastructure

By utilizing BYOD, the company does not have to install and maintain an infrastructure for enterprise mobile solutions. This decision saves the company capital not only on the physical resources but Information Technology (“IT”) overhead resources as well. The realized savings could be larger due to multiple instances of BYOD utilization for smartphones as well as tablets and/or laptops. By leveraging the usage of the employee’s personal tablet or laptop as well, the company would realize hardware savings. It's important to note that the company will likely need to

contribute monetarily to the employee’s device cost or resource usage, however that cost would be a mere fraction of the upfront cost for the large scale purchase of company owned and maintained hardware. Moreover, there is also a perception of reduced operating expenditures in the total cost of ownership (McGrath, 2014).

2.3 Technological Advancements and Policies

When an employee uses his/her own devices, he/she has access to more up-to-date technology that, in turn, can benefit the organization. When an employee, based upon the company policy, exercises the BYOD provision, he/she has access to newer technology that said company may not necessarily have the same access to. Such technology and benefits thereof, in turn, can be realized and capitalized upon by the organization in additional productivity, streamlined operations and/or enhanced information technology uses.

Another indirect benefit for the company would be the absolute need to review existing policies in order to craft more robust, timely and appropriate policies in light of BYOD. An end result could be that additional training and/or security safeguards would be instituted, and add a positive benefit to the overall information technology security standpoint of the organization. It should be noted, however, that this list is not an all-inclusive list of the benefits associated with BYOD. The reasons a company may employ BYOD could vary greatly based upon the needs, goals and financial standing of same. Nevertheless, companies would most likely benefit from one or more of the aforementioned items.

3. LEGAL AND TECHNICAL ISSUES SURROUNDING BYOD

As more companies implement BYOD, Digital Forensic Examiners (DFE) will encounter a myriad of legal and policy issues of which they must be aware. These issues can range from privacy, 4th Amendment, ownership questions, liability and other legalities.

3.1 4th Amendment Issues

The 4th Amendment to the Constitution is the preliminary groundwork to any and all issues relating to search and seizure of an individual’s device. The 4th Amendment serves to protect individuals from unreasonable searches and seizures without due process (i.e., a trial) and a warrant is generally required to search a device. The warrant is a legal document that allows law enforcement to search an area or item for evidence of the alleged criminal activity (Nelson, 2010). In general, a warrant must be sufficiently and specifically worded for the seizure of the evidence. Once the warrant is signed by the Judge, it is executed against the individual and/or property for the items enumerated in the warrant (and other fruits of a crime in plain view). Essentially, under the 4th Amendment, a cellphone and computer are treated as a closed container wherein there is an inherent expectation of privacy of the data on said device by the owner. In the absence of a policy put in place by a corporation or a properly issued warrant, the 4th Amendment protections apply (this is a critical point to remember that will be addressed later on). The investigator is limited in the kind and amount of evidence he/she can collect in a BYOD enterprise by these elements—a policy, Court Order and/or the warrant. DFEs must be aware of the context in order not to invalidate

any evidence and open the company up to potential litigation.

Further solidifying the 4th Amendment right to privacy, the Supreme Court very recently reviewed a case regarding the police’s perceived right to search a cell phone without a warrant incident to the arrest of the accused. The Supreme Court ruled in *Riley v. California* (2014), that the police may not search cell phones belonging to suspects without a warrant and that said devices are not akin to wallets or vehicles (wherein the police can do a search after a lawful arrest, especially if “fruits of the crime” are in plain view) (Mears, 2014). This is important because it protects the ownership of the data on the phone and the device to the owner of same. The Supreme Court relied upon the 4th Amendment and the long standing law that police need a warrant to search one’s home and that cell phones differ from other objects that can be searched since they [cell phones] carry much different items on the person than a purse (Mears, 2014). Accordingly, the Justice Department plans to work with law enforcement to ensure that technology will be used to preserve the evidence on cell phones while the cases are pending for a warrant (Mears, 2014). This is important to the digital investigator because policies and standards will have to be developed and enforced in the corporate environment for consistent application of this evidence preservation technique and said investigator will need to have access and training to any applicable tools.

Additionally, DFEs need to be aware of potential exigent circumstances (thus alleviating the need for a warrant) that may still exist and there will need to be a consistent standard for the application of this exception (Mears, 2014). The DFE must be cognizant of

any pending warrants/cases for the individual who owns the subject phone and that any search of the phone may be deemed inadmissible if the DFE is seen as any agent of law enforcement (working in concert with or under the direction thereof). Proper boundaries and procedures must be enacted to protect the DFE and the integrity of the evidence, especially in this scenario.

3.2 Electronic Communications Privacy Act

As technology evolves, more relevant [to BYOD] laws and regulations have been formulated such as the Stored Communications Act (hereinafter referred to as “SCA”) as part of the Electronic Communications Privacy Act (hereinafter referred to as “ECPA”). ECPA serves to protect cellular telephone, e-mail and other electronic data transmissions from unauthorized search and seizure (and serves to amend the Federal Wiretap Act) (Spinello, 2011). In particular, the SCA of ECPA serves to protect a user’s electronic communication from being viewed, altered or otherwise interfered with while it is in electronic storage with an ISP/service provider (internet service provider) or similar entity. However, there is no warrant necessity to get communications from third parties, such as ISPs, etc. This does not necessarily mean there is not a Court Order or Subpoena requirement to get the information from third parties. The DFE must be cognitive of stored communications and if he/she should have access of them from information gleaned from the imaging or if a formal request to a third party will be necessary (or if litigation will be needed to get the information). At this point, the DFE must cease the capture of the protected third party information and look for further direction. As such, on a BYOD device within an

organization, the third party communications with the party are protected conversations and the Digital Forensic Examiner may breach rights of other parties and subject a company to liability.

3.3 Commingled Data and Stored Communications Act

Organizations using BYOD should be aware of potential challenges. Commingled data is one of the most obvious consequences. Simply stated, commingled data refers to the employee’s personal data being mixed in amongst the business-owned (and/or proprietary) data. Some examples of commingled data include but are not limited to: text messages, photo galleries, email, web browser history, metadata, and call history. The commingled data issue is of utmost importance to the DFE because of the corporate policy limitations, as well as consent to search and the challenges to the search that could be mounted by the employee. In all fairness, it would be remiss to not at least note that commingled data (and the problems that come therewith) are also present in standard enterprise environments without BYOD. However, with BYOD, the device ownership issue along with technology evolution complicates the digital forensic examiner’s job significantly. As such, the DFE runs a high risk of capturing the employee’s personal data and/or being accused of wrong-doing (such as inappropriate viewing or accessing). Further, having the access to an employee’s personal data is ripe for exploitation if the involved investigative parties are not scrupulous and methodical in the collection efforts.

A great example of this sort of commingled data exploitation is the case of *Lazette v. Kulmatycki*, wherein the Plaintiff Lazette was employee of Defendant’s that was assigned a

company owned Blackberry mobile device for use in the scope of her employment. She [Lazette] used the company owned Blackberry to access her personal email account that was linked to said Blackberry (Konvisser, 2013). When the Plaintiff terminated her employment, she deleted her personal email account from the device and returned same to the personally named Defendant Kulmatycki (as an agent of the employer). However, despite her [Plaintiff’s] best efforts to delete the commingled data, the Defendant recovered the personal email account off of the device and read her [Plaintiff’s] private email (hosted on another, unrelated cloud platform) over the subsequent months (Konvisser, 2013). Since the Defendant read these personal emails that was stored on infrastructure owned by a provider (such as Google), he was found at fault under the SCA for the unethical act (Konvisser, 2013). Further, the employer was found vicariously liable for the defendant’s action despite the fact that the device was owned by the company (Barnes, 2013). The SCA covers the activities of an individual intentionally accessing, without authority (or exceeding granted authority, such as privilege/access escalation), a facility that provides an electronic communication service and/or obtains, alters, or otherwise prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system (Cornell University Law School, 2015). The punishment ranges from fines, to imprisonment up to 10 years for repeated offenses (or a combination of both) (Cornell University Law School, 2015).

Even in the cases where DFEs have no intent to abuse their access to the information, commingled data still looms as a troublesome pitfall. For example, SMS messages (texts) and MMS (picture messages) are inherently

commingled on the device, thus, rendering the collection of them in the same commingled format. Thus, even if the DFE does not have the malicious intent to access the information stored in another location by an electronic service provider, the DFE may nonetheless breach SCA by intentionally trying to gather all information off of the device (thus, obtaining the other provider may have that they person accessed on the device) or by trying to capture other information that leads to the other provider.

3.4 Common Law

The common law tort known as “the expectation of privacy” comes into play with a BYOD enterprise. In evaluating the common law tort known as the reasonable expectation of privacy, the court looks to several factors such as: did the employee have a reasonable expectation of privacy (consent to monitoring, private property, etc.), was the monitoring justified and if there was an emphasis on minimal intrusion by the employer (Schweik, 1995). The DFE must keep in mind that in BYOD cases where the corporate policies are weak, questionable or even non-existent, the employee may try to assert the expectation of privacy as an affirmative defense to surrendering the device (and contents thereof) for analysis.

3.5 Ownership Issues

Additionally, data and device ownership questions pose serious issues for the company as well as any DFE involved in a BYOD investigation case. Upon termination of the employee, the question of data and device ownership and spoliation becomes a factor. In the case of a company owned device, the employee typically destroys all of the “personal data” on the device upon return of same.

Arguably, since the device was not the employee's, likewise all of the data contained therein did not belong to him or her. Unfortunately, the employer has no control over employee's direct destruction of the data; however said employer may assert an ownership claim over the data and the device. Once all the data is destroyed, it is may be up to the DFE to recover it with any number of tools, however, then the data commingling and exploitation risks become inherent.

However, in the case of BYOD, the company does not assert ownership against the device, only some of the data contained therein. The employee may either wrongfully destroy or withhold all of the company's information on the device upon termination. Once again, the company is exercising ownership rights over the data however said data is housed on a device that said company has no ownership in. As such, the employee could successfully delete or disseminate the data while maintaining the device. The DFE, in either circumstance, is put in the precarious position of finding ways to recover the deleted data and it is highly conceivable that the device will not be available. The employee could sue and/or claim that his privacy was breached and wrongful search and seizure if the proper policies and procedures are not put into place.

3.6 Evidence Spoliation

Evidence spoliation can take several forms, especially in the case of BYOD. A terminated employee (i.e., a disgruntled employee) may take any number of actions to make the company data--and thus, any wrongdoing by the employee in regards to the company data--unavailable. For example, in the case of *Barrette Outdoor Living, Inc. v. Michigan Resin Representatives*, the plaintiff's former

employee was accused of doing wrongdoing in the course of his employment (Haney, 2013). The former employee took his commingled BYOD and promptly turned it into his mobile service provider and obtained a new cellphone (Haney, 2013). Since the original cellphone was not available, the Plaintiff sought the recovery of a digital image of the defendant's laptop computer. During litigation pendency, the defendant deleted 270,000 files from the laptop (Haney, 2013). The Court stated that the Plaintiff incurred extra discovery costs in trying to obtain the evidence, however it was not noted whether or not the Plaintiff was able to recover any of the lost evidence (Haney, 2013). Instead, the Court and Jury were allowed to infer that the Defendant destroyed the evidence because he was lying, was involved in malicious conduct, etc. (Haney, 2013). Another example (admittedly not as blatant as the previously enumerated example) of spoliation that may happen in “BYOD” situations is when a personally owned device is heavily used, it may over-write some of the business data (such as text messages or items in memory). Once again, the company would have no control over this. The investigator would be hard pressed to recover the original, over-written data under these circumstances.

3.7 Inadequate Policies

Noteworthy, another consequence of BYOD is the very likely possibility of inadequate organizational policies to cover BYOD issues, ethical obligations, and conflicting client expectations with the laws that direct and dictate the behavior of those conducting the investigation. For example, the DFE could be put in the uncomfortable middle position of whether to “obey” the wishes of the employer (either direct or contracted employer) within the scope of an investigation or to follow any applicable legal regulations and/or subpoenas.

DFEs will find themselves in this situation when the Court Order is overly broad and/or vague. As a result, the DFE must manage the client’s expectations, in light of the Court Order and within the realm of laws and liability. At best it becomes a test of the DFE’s patience and moral compass as well as in-depth knowledge of the legal limits.

3.8 Technology

Keeping up with device advances becomes a major DFE challenge as well. As the devices become more sophisticated, new mechanisms are put into place to “safeguard” the consumer’s data. For example, many current device manufacturers deploy default encryption on the devices to prevent the theft of the data. These safeguards may be insurmountable by the DFE and make it impossible to gather the image or data in a complete state (if at all). In the case of Apple device encryption, the investigator can get Apple involved, however anytime a third party is involved, more chances for tainted and incomplete evidence exists. Further, Apple has recently stated it will not release any encryption keys and/or perform any analysis on devices with passcode locked iOS8.0 devices (Apple, 2014). For any documents stored in the iCloud that are encrypted, Apple has stated it will not release any keys (Apple, 2014).

In the case of a Blackberry and/or Android device encryption or security mechanisms, the investigator can possibly pull the chip data (binary file) in the absence of the pin code (Hunter, 2014). Further, it is not illegal to date for manufacturers to deploy these products on devices despite law enforcement pleas to the contrary.

In order to balance the need with encryption and the need for organizational data access, some device manufacturers (such

as Apple) have devised a program that allows one computer to have the complete administrative control and syncing abilities for any number of deployed enterprise devices. The controlled devices are configured to be controlled by the administrative machine via the use of the administrative device’s MAC address (media access control address) and the device UID. One such program is known as Apple Configurator.

Apple Configurator has the ability to do any number of tasks and settings, such as setting the lock screen, wallpaper and name, controlling installed apps and documents, setting configuration profiles, integrating with Mobile Device Management solutions and applying updates (Apple, Inc., 2014). While taken at face value, the Configurator seems like a great feature, this is not necessarily the case for the DFE. Per Forensic Analyst and Instructor Bruce Hunter of BlackBag Technologies, one of the major problems he encounters on a regular basis with the Configurator is the inability to dump the information from the suspect machine since it is linked to an administrator/supervisor machine (Hunter, 2014). The consequence of this application usage is that the “investigated device” is unable to connect to the forensic workstation (Hunter, 2014). The glaring detriment of having the administrator computer “in charge” of all syncing and “dumps” is what happens in the case wherein the DEF does not have access to the administrative computer and/or one of the suspect computers is the administrator computer? Such a scenario could render the DFE without any recourse or method to copy or dump the device to the forensic workstation.

The DFE and organizations must keep abreast and aware of the technology changes that are coming into play. For example, smart watches (such as the Apple Watch and other

models of the like) are an up and coming trend. These devices carry a whole host of issues for a DFE and organization to grasp. For example, these items are even more portable and concealable than a smart phone, tablet or laptop. Hence, the theft of this device in an immediate fashion is easy. Further, since these devices are so new, there are not many applications out there that the DFE can use to grapple with the data. Hence, the DFE is limited to what they are able to retrieve from the device. What’s more, is the inherent characteristics of the device make it a prime target for commingled data in so that is used for many personal transactions, such as fitness monitoring (logs heartrate amongst other personal health factors), wallet and credit card transactions, photos, location information, GPS and tracking of the individual wearing the watch. The DFE would encounter all of this private information in an investigation. The watch raises many security concerns including the use of Bluetooth (easy to hack and eavesdrop) in addition to Wi-Fi.

Further, the DFE may have a hard time retrieving instant messages sent on the watch, depending on the amount of storage. For example, the Apple watch allows its users to send sketches and instant messages—this could become key in a case where trade secrets are stolen.

3.9 Third Party Applications and Services

The influx of cloud services and third party applications can cause issues in a BYOD environment and make it difficult for a DFE to conduct the investigation. Cloud applications have some legitimate uses such as for document and photo storage, virtual environments, disaster recovery and/or backup purposes (e.g., Dropbox, iCloud, etc.).

Organizational information may be stored or encrypted in a cloud or in another third party application (such as LinkedIn, Facebook, etc.) to the detriment of the enterprise with the BYOD usage. For example, many personal device users knowingly or unknowingly back up their data to a cloud by the virtue of a checkbox selected when the cell phone or tablet is set up (or the device sends it to the cloud automatically for the “convenience” of the consumer) (Manes, 2013). As the company has no control over any manufacturer proprietary cloud or third party applications, the courts would have to be involved (despite any policy put in place by the company). The enterprise IT team must be cognizant of confidentiality and privilege issues that may exist within the enterprise and realize that these responsibilities may be compromised in a BYOD situation through the use of cloud and other applications (this also includes Personally Identifiable Information spills) (Manes, 2013). Furthermore, the company would have no control over the uses of the data (e.g., Data mining, marketing, theft) and would have to seek an injunction after the damage has been done.

Of course there are no guarantees of successful litigation in a BYOD situation dealing with outside vendors and/or third parties. In this scenario, the DFE will need to testify in court as to what files he/she wishes to recover and how same are relevant. It is highly probable that the DFE will miss evidence and/or not be aware of all of the contents backed up or contained or even encrypted within the application. In the case wherein the data between the device and application is encrypted, that data would be unrecoverable. Additionally, some applications may even be hidden, disguised or disabled, thus making it harder for the DFE (by limiting

or hiding other items, tasks) to have a grasp on what data exists (BlackBag Training Team, 2012).

Lastly, the employee may knowingly back up information to a cloud services provider and/or third party (social media, etc.) with reckless abandon (such as in sabotage, etc.) and ignorance to the consequences that may come to the company. The employee may be ill-informed, ignorant or simply not care if company information is stored at these other locations (or sadly, may actually think they are doing the company ‘a favor by backing up’ the data).

3.10 Manufacturer Backdoors

Another security element that has to be taken into account by an organization and a DFE is the possibility of the manufacturer of the device having a backdoor installed on the device. In concert with the typical security concerns with backdoors, same [backdoors] carry the potential for evidence to be changed, altered, deleted and/or stolen by an outside party that learns how to use the backdoor. At the minimum, data (private, company data) on a BYOD could be sent to the device manufacturer via usage of the backdoor. An example of such a backdoor has come to light and is alleged with Apple products. Please note, the authors are not proving or disproving these allegations, just what has been asserted by other professionals in the field. The following backdoor programs have been found on Apple products as of July 2014 by professionals in the industry:

come.apple.mobile.pcapd;
 come.apple.mobile.file_relay;
 com.apple.mobile.house_arrest (O’Grady, 2014). Apple has asserted that these packet capturing, copying and transferring accesses are there for troubleshooting, support and diagnostic purposes and are not backdoors for

nefarious purposes (O’Grady, 2014). Another company accused of installing backdoors on their products is Google (Ossowski, 2014).

Further, to prevent against access via manufacturer backdoors, it may actually serve as an impediment to the DFE. For example, with the Apple backdoor issues alleged earlier, the following solution has been proposed in the industry (other than Apple removing these files): set a complex passcode in iOS, use the Apple Configurator product discussed in this article to set up the Mobile Device Management restrictions and enable pair locking (Hodgkins, 2014). While this blocks third-party forensics applications (sorry, DFE), Apple will still be able to do a forensic examination on it which can hinder an organization both in terms of time expended, expediency and costs.

4. SUGGESTED MITIGATION TECHNIQUES

As with most technology and organization challenges, Digital Forensic Investigators will find no one silver bullet to fix the pitfalls that plague investigations in the BYOD arena. An oversimplified approach is to simply remain completely educated and flexible in his/her approach to the BYOD issues and mobile forensics, but this is no small task in itself. Instead, the authors offer the major issues that must be considered and addressed.

4.1 Address Commingled Data

Commingled data must be addressed in an organized manner while adhering to the prevailing regulatory documents (Court Orders, Corporate Policies). While it is true that it can be difficult to sift through the data to determine what is business vs. personal

data, DFEs must demonstrate due diligence. Some investigators may subscribe to the belief that they should make a copy of all of the data on the device without searching same, however, one could argue that there would be potential liability concerns for accessing all of the data (under SCA, privacy laws in absence of company waiver, etc.) if a bitwise copy has been made. How the DFE decides to handle the commingled data is up to the company and the investigator (and any applicable employment contracts) in light of any Court Order.

4.2 Implement Mobile Device Management

Many companies use mobile device management (hereinafter referred to as “MDM”). Historically these management applications are not able to make a distinction between personal and corporate data (McGrath, 2014). In response to this issue, some vendors have designed applications that work to secure the data itself (not so much the device) and offer them under the category of mobile application management (hereinafter referred to as “MAM”) (McGrath, 2014). Many of these devices include a “virtual infrastructure” such as “virtual silos” for the data on BYOD. If a company uses MAM—either in totality or piecemealed—it can help to sort out the data, but not prevent all commingled data. For example, Blackberry 10 devices provide two desktops—personal and work—that do not talk to one another (although texts may still be commingled) (Hunter, 2014). Another example is the chamber concept that is used by Windows Phone and Surface (chambers isolate data). There are other vendors, such as Citrix, that also rely on the zone/container/chambers model for products.

It should be noted; however, all MDM and MAM products should not be completely relied upon, as they do not always resolve ever-changing BYOD issues. Some products have attempted to meet the needs of enterprises deploying BYOD to include tools such as remote wiping and partitioning (likely analogous to the MAM virtual silos) (DiMarco, 2013). While one may think that MAM and MDM products may be the BYOD solution, said products are not able to be configured (and therefore the enterprise may not be able to control) for devices with non-traditional operating systems and or “jail broken” devices running modified systems (Gatewood, 2012).

Either way, the use of these products may help contain some, but not all, of the data in appropriate compartments and simplify the process of the forensic copying. By the use of a MAM or MDM, the BYOD may be limited in the usage of a cloud service and/or other applications. If the use of these other applications is limited and/or prevented, it can help narrow the scope of the data for the DFE review and also assist in limiting the amount of proprietary corporate data that is leaked out. The aforementioned Apple product that allows all devices to be configured to one administrator device is a form of proprietary, vendor specific MDM. Further, Apple has also instituted encryption and activation locks on its mobile devices to help prevent theft of data if a device is activated as a “stolen” device. This could be useful in the case wherein a BYOD is an Apple device with critical, sensitive information on it. It is imperative to note that, at a minimum, a BYOD environment must have managed data, environments and encryption incorporated within a MAM and MDM.

4.3 Limit or Sandbox Important Mobile Applications

Of course, in a BYOD scenario the device owner may dispute the limiting of applications on the device. It is likely that the device owner would be successful as the Courts routinely look at the ownership of the device as the controlling factor. It may be worthwhile for a company to narrowly craft a policy that would justify the limitation of a certain application instead of a blanket limitation on any non-enterprise owned applications. Further, many issues would need to be addressed by adequate policies such as ownership of data and the device to help prevent spoliation of the evidence.

The enterprise must retain the right to remote wipe the device, regardless of the device ownership and have a mechanism in place to prevent the employee from engaging in remote wiping (such as if the device was confiscated from the employee and he/she desires to delete text messages). In addition, in an investigation, the enterprise should make sure to send a preservation notice to the investigated party to not destroy any of the data (or device) and copy the applicable investigator on same to give notice (and to also alert the investigator to the action and possible destruction of data). This will help preserve any challenges in Court if the device and/or data become subject to spoliation litigation.

4.4 Educate Employers

Another item that may assist the DFE in the long term is to educate the employers/clients on the legal and investigatory issues that surround the forensic collection of the data in a BYOD environment. While education is always a positive benefit, it by no means is a complete solution. In MAM and MDM deployments, education is a necessity due to the staff

integration that must take place. Bruce Hunter summed this need up well in his description of “management devices make it a minefield... [You] must have the IT person on board to help you [investigator] navigate through” (Hunter, 2014).

Further, the employer should and must consult with a security expert to determine which BYOD products in the future are ‘safer’ bets than others. Some devices, such as the watch and even smart cars (in the making), may prove, in fact to be too risky even for the most prepared organization.

4.5 Formulate Policy

We cannot stress enough the importance of strong policies to assist the DFE in a BYOD investigation. Absent Court Orders and/or Warrants, organizational policy dictates the rights that an investigator has to the device and data. Moreover all policies must comply with any applicable Court Orders and that said Order is prevailing over any contradicting policy. Organizations should note that there are certain elements that must be covered by the organizational policy such as notice to the employee that he/she does not have a complete expectation of privacy on the device containing company data, regardless of ownership of the device (to defeat 4th Amendment violation claims).

Further, the policies should include the consent for the capture of all text messages and photos as it alleviates the DFE's burden when attempting to sort through these items. The policy must be clearly defined, posted and should detail such provisions as: employer has access to text messages and photos, employer may remote wipe under specific circumstances (such as theft, loss, commingled data, etc.), employer can investigate at any time, that the employee gives informed consent, regulations

on confidential trade secret information, policy parameters to protect client confidentiality, acceptable use provisions (i.e., an approved application listing), security and monitoring measures engaged in by the enterprise, etc. (Hinkes, 2014). This policy should be signed by the organization and the employee prior to the employee starting to engage in work for said organization or having his/her device accessing work product.

Additionally, the employer can have the policy drafted in such a way to attempt to prevent any SCA claims. The SCA provides that, “whoever intentionally accesses without authorization a facility through which an electronic communication service is provided...and thereby obtains, alters or prevents authorizes access to a wire or electronic communication while it is in electronic storage... shall be punished as provided...” (Barnes, 2013). As such, this would apply to email stored somewhere else (such as with Google, etc. or in another data center) and could open up the DFE to liability if he/she accesses email or other stored photos, text messages, etc. As a work around, SCA does allow for third party access to communication when the consent is provided by the user (Barnes, 2013). As such, if consent is given within the policy parameters by the user to access text messages, stored documents and photos, this will likely insulate the DFE from SCA liability concerns.

5. COMPANY POLICY MITIGATION TECHNIQUES

5.1 Roles and Responsibilities of Policy

Even with all the challenges and potential pitfalls with a BYOD environment, the authors envision more companies taking this approach because of the benefits. Once the decision to move in the direction of BYOD has been made, the first step is to start planning and create policies. Although the authors cannot offer specific wording due to the myriad of organizational environments, there are basic concepts that must be in place.

Corporate policies play a substantial role in how employees as well as the Digital Forensic Examiner will handle and react within the BYOD environment. First and foremost in the absence of any policy, the new policy must clearly establish that the employee (regardless of device ownership) does not have an expectation of privacy on the device in regards to the corporate information contained therein. The language in the contract should encompass both statutory and common law expectation of privacy claims (i.e., there is no inherent right to privacy with the phone as employee is waiving that right, consent to monitoring, etc.). The company should also include provisions that there is no expectation of privacy in regards to the commingled data, text and photo messages in particular.

Further, a company must protect itself via the use of a policy against SCA claims. As previously mentioned, the company policy should also encompass and detail that the employee (user) is granting third party access to the stored communications to the employer and waive any action under the SCA. The policy should clearly state under what circumstances monitoring and searching of the device may take place and that the company does not search and review arbitrarily—there must be a legitimate need for same.

Along the same lines, the policy must clearly and unequivocally state what the

acceptable use provisions are for the BYOD in the enterprise environment. The Acceptable Use provisions can include, but not be limited by, such elements as: acceptable use of applications (including third-party and cloud applications), what type of websites can be viewed or associated with the company data, duty to protect the device and company data stored therein, prevention of commingling of data, just to name a few.

Other practical aspects of the policy and BYOD element must be addressed in the policy, such as storage of company information on the device, password and encryption requirements, reimbursement plans, the requirement to give any a passwords or access tokens to the company, as well as the loss, sale or trade in of the device, etc. The employee should sign a release, consent to policy and any applicable waivers prior to instituting the BYOD plan.

On the company side, the following internal elements should be addressed prior to permitting the use of BYOD: allocation of IT help desk and other support for BYOD, what sort of support and overhead will be dedicated to BYOD, procedure for device retrieval and legal preservation (in the case of either a terminated employee or a legal hold), resources and company system permissions, consequences for non-compliance, training on proper BYOD security and security best practices required by the company and overall awareness training for all stakeholders (Gatewood, 2012). In addition, the company must take into account the specific privacy, accountability and reporting concerns that are associated with its industry, such as HIPAA, Sarbanes-Oxley, Gramm-Leach, just to name a few. The policy must cover what is to be conducted on the devices and how the information is to be handled by the employee and the company in a BYOD

environment to protect the organization from liability.

6. CONCLUSION

BYOD is a trend that will increase in popularity as more employees want to bring the latest device to work. Organizations will continue to adopt a BYOD mindset as it offers them perceived potential costs savings with increases in employee satisfaction. Although it would be more secure to not create BYOD environments, current trends suggest that this is a losing battle.

We would caution those organizations who are planning on implementing BYOD to consider the potential policy, as well as other infrastructure changes to protect against comingled data, lost devices, etc. For those organization already in a BYOD environment do look to mitigate considering many of the items and approaches we have suggested.

Remember that there will be pitfalls and potential litigation issues that could obliterate any realized savings by the company. In addition, the DFE is disadvantaged in a BYOD scenario because of the device diversity, third party applications storage potential and legal ramifications that are evitable. Further, as evidenced above, there is no single mitigation solution to address these issues in order to protect an enterprise (and do not forget the clients as well) in a BYOD situation. Further, in an ordinary situation, difficult for an enterprise to have a complete grasp on trade secrets and other confidential information. A BYOD scenario would compromise the enterprise and would make it even more difficult for the enterprise to navigate through the technology advances and investigations in light of the numerous issues such as device ownership, portability, third party stakes, legal protections, etc.

Until these issues can be mitigated further and more easily managed by an investigator, a company should tread the BYOD waters with great caution as a remedy may be hard to find. We recommend strong policies, procedures, and education as the best approach at this point in time.

REFERENCES

- Apple, Inc. (2014). *Apple Configurator Help*. Retrieved July 07, 2014, from Apple ConfiguratorHelp: <http://help.apple.com/configurator/mac/1.5/#cadf1802aed>
- Apple, Inc. (2014). *Legal Process Guidelines: U.S. Law Enforcement*. Retrieved January 2015 from <https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf>
- Barnes, N. M. (2013, September 26). *BYOD: balancing privacy concerns against employer security needs*. Retrieved June 10, 2014, from LEXOLOGY: <http://www.lexology.com/library/detail.aspx?g=1109490a-6895-40f0-a7a3-afc714316165>
- BlackBag Training Team. (2012, February 23). *iPhone Forensics: iPhone and iPad Forensics in a BYOD Enterprise Environment*. Retrieved June 10, 2014, from BlackBag Technologies: <https://www.blackbagtech.com/blog/2012/02/23/iphone-forensics-iphone-and-ipad-forensics-in-a-byod-enterprise-environment-2>
- Cornell University Law School. (2015). *U.S. Code, Title 18, Part I, Chapter 121 §2701*. Retrieved online at <https://www.law.cornell.edu/uscode/text/18/2701>
- DiMarco, C. (2013). Who's Afraid of the Big Bad BYOD? *Insidecounsel*, 62-64.
- Gatewood, B. (2012). The Nuts and Bolts of Making BYOD Work. *Information Management Journal*, 26-30.
- Haney, C. (2013, November 05). *Spoilation of Electronic Data Results in Severe Sanctions*. Retrieved June 23, 2014, from American Bar Association Litigation News.: http://apps.americanbar.org/litigation/litigationnews/top_stories/110513-spoilation-electronic-data.html
- Heaton, B. (2013, October 7). *The Legal Implications of BYOD*. Retrieved June 10, 2014, from Government Technology: <http://www.govtech.com/The-Legal-Implications-of-BYOD.html>
- Hinkes, A. (2014). *BYOD Policies: A Litigation Perspective*. Retrieved June 10, 2014, from ABA Section of Litigation: Section Annual Conference: http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2014_sac/2014_sac/byod_policies.authcheckdam.pdf
- Hodgkins, K. (2014). *Forensic Expert Questions Covert 'Backdoor' Services Included in iOS by Apple*. MacRumors. Retrieved online at <http://www.macrumors.com/2014/07/21/covert-backdoors-ios/>
- Hunter, B. (2014, July 01). Forensic Analyst/Instructor. BlackBag Technologies. (C. Montroy, Interviewer)
- Intel Corporation. (n.d.). *Moore's Law and Intel Innovation*. Retrieved June 13, 2014, from Intel.com: <http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html>
- Konvisser, J. B. (2013, August 08). *Personal Email Privacy in a BYOD Environment-a View from the Bench*. Retrieved June 11, 2014, from Lexology: <http://www.lexology.com/library/detail.aspx?g=3fac96b7-b1f2-43af-a83b-0520bc4a613c>

- Manes, G. W. (2013, March 027). *Avansic Whitepaper: Bring Your Own Device*. Retrieved June 10, 2014, from Avansic: <http://www.avansic.com/News/Story/217/>
- McGrath, S. (2014). Create A Mobile Device Policy Your Employees Can Trust. *Computer Weekly*, 25.
- Mears, B. (2014, June 25). *Supreme Court: Police need warrant to search cell phones*. Retrieved June 26, 2014, from CNN.com: <http://www.cnn.com/2014/06/25/justice/supreme-court-cell-phones/index.html?iref=allsearch>
- Montana, J. (2005). Who Owns Business Data on Personally Owned Computers? *The Information Management Journal*, 36-42.
- Nelson, B. P. (2010). *Guide to Computer Forensics and Investigations*. Boston: Course Technology.
- O'Grady, J. (2014). *Apple Refers to iOS 'Back Doors' as Diagnostic Capabilities*. The Apple Core. Retrieved online at <http://www.zdnet.com/article/apple-refers-to-ios-back-doors-as-diagnostic-capabilities/>
- Ossowski, Y. (2014). *Wyden: No More 'backdoors' in Americans' Computers, Phones*. Fox News. Retrieved online at <http://www.foxnews.com/politics/2014/12/08/wyden-no-more-back-doors-in-americans-computers-phones/>
- Romer, S. A. (2013, September 04). *Federal court Applies Stored Communications Act protection to Employee Social Media Pages*. Retrieved June 11, 2014, from Lexology: <http://www.lexology.com/library/detail.aspx?g=155e106e-2bf9-4822-925f-7aa8c6aaa835>
- Schweik, C. (1995). *Electronic Mail, Privacy, and the Public Sector: Guidelines for Public Employees and Organizations*. *Employee Responsibilities and Rights Journal*, 275-293.
- Spinello, R. (2011). *Cyber ethics: Morality and Law in Cyberspace*. Sudbury: Jones and Bartlett.

