Timothy Kang

BYOD Policy and Management so that the "D" Stands for Device and Not Disaster

Smartphones are a major part of today's world. It is no surprise since it is a computer at your fingertips that can be accessed from basically anywhere and at any time. Aside from just calling and sending short messages like in the past, one can now browse the internet, play games, create documents, and do a variety of other tasks with the millions of existing applications on the market. Companies understand the power of these devices and the term "Bring-Your-Own Device" or "BYOD" can be heard quite a lot, both within and outside the workplace. Similarly to most things, there are both pros and cons that can make this a blessing or a disaster. With more and more organizations making use of BYOD, understanding the risks and implementing proper policies and management procedures are vital in ensuring that the "D" in BYOD truly stands for device rather than disaster.

What exactly does BYOD mean in a corporate setting? Just like the name implies, it is the ability to bring your own device and use it for work-related purposes. In other words, this does not mean bringing a phone and watching television shows with no correlation to the job during work hours. Rather, this means using a device of their choice such as a smartphone, tablet, or laptop for purposes such as communicating with colleagues, working remotely, and being accessible (Rieders & Monroy, 2014). This is neither a new concept nor an unpopular existing idea. It is a growing market that is being utilized everywhere. At its current pace, "analysts are predicting that the global BYOD and enterprise mobility market will hit $360 billion by 2020" ("Security Issues May Hamper," 2016, p.12). Some history should be known to understand how the model of BYOD came about.

Before BYOD, many companies made use of COPE. This acronym stands for "corporately owned, personally enabled" (Scardilli, 2014, p.1). This involves the company giving an employee the proper device to use for work-related tasks. BYOD can be seen as a free-for-all where anyone can bring any phone or device, but COPE can be seen as a controlled environment where anyone can only use approved devices that are owned and provided by the business (Scardilli, 2014). Simply put, an organization might give you a choice of three phones that they approved and the one that you choose will be your COPE device. This model had started in the 90s when buying technological goods such as cellphones in bulk had many benefits. Since security wasn't a big issue at the time, buying more for less was a big win for many corporations. The early 2000s continued using this model as BlackBerries rose in popularity. The keyboard and the many functions it had made it desirable from a productivity standpoint. For a while, COPE had grasped the industry, but this would change in 2007 with the appearance and rise of the Apple iPhone (Scardilli, 2014). This highly functional and user-friendly smartphone could be bought by anyone and set up with ease to do work tasks. Companies understood the power of these miniature devices and its capabilities which brought forth the beginning of the BYOD model. However, this did not mean that the BYOD model was problem-free and completely superior to COPE.

With more and more security breaches being announced on the news, both big and small businesses understand the importance of cybersecurity when it comes to protecting company assets. Data being compromised can be detrimental and can possibly bring a company to ruin. There is obviously no fool-proof method to prevent this 100% of the time. However, lowering the risk to a minimum is possible and should be desired. With BYOD, one must take into account the manufacturer, model type, operating system, user-downloaded applications, and a

plethora of other factors that can increase the possibilities of such a risk. On the other hand, COPE allows for only equipment that is well-supported to be used since only approved devices will be offered. The company "can easily control and secure the data because it's the company's device" (Scardilli, 2014, p.36). This might not be enticing to the employee, but it does reduce security risks and have other company-related benefits such as increase in productivity once accustomed to. There could be a slight inconvenience due to being forced to carry around two devices, but COPE is a viable strategy that some places are returning to in recent times.

Unsurprisingly, this does not mean that BYOD is falling out of popularity. The perks of the BYOD model cannot be ignored by what COPE brings to the table. It should be noted that not all companies have the option of providing COPE devices. Jacob Poushter of Pew Research Center claims that in "a survey of cell phone ownership in the United States[,] 72 percent of adults in the United States who were polled owned a smartphone" (Ong'ele, 2017, p.5). With such a high number of individuals with personal smartphones, BYOD is the perfect model of taking advance of this. It truly is the age of smartphones. Comfort is another advantage of BYOD. Higher efficiency levels and increased productivity are possible when an employee understands and is comfortable with a device and the applications that they are accustomed to seeing and using ("Half of U.S. firms," 2016). Giving a new device to someone that is not comfortable with it will take time getting used to and decrease productivity and even satisfaction. Furthermore, reduced cost is the perk that many employers find enticing. COPE would require employers to buy the device and support it using the IT budget. This can be avoided with BYOD because employees are acquiring and maintain the devices themselves (Careless, 2013). One thing to keep in mind is that BYOD does not mean that the employee is only using their own devices for every task; they can still use company-provided devices such as laptops which shows

the flexibility of the model. For example, you can create a document on a company laptop and access this document for further editing on a personal smartphone at home. Cost saving, flexibility, comfortability, productivity and availability of BYOD devices explains the attractive nature of bringing your own device. Unfortunately, this is by no means a perfect system.

In order to manage risks, risk evaluation is necessary to quantify and qualify "the consequence of hazardous operations through some risk metrics" (Ganiyu & Jimoh, 2018, p.50). A list of risk factors and security controls that are available to the company should be defined. Patterns can be understood by the risk management team so that risk can be evaluated (Ganiyu & Jimoh, 2018). Threat sources of different potency levels can be found so that proper countermeasures can be put into place. In simpler terms, the first step to fixing a problem is to find it and the best way to fix a problem quickly is to know about it and prepare. When it comes to BYOD, one must address the many dangers and concerns that it brings.

As stated earlier, security risks are an important area of concern especially for BYOD. Data leakage, loss, and theft is high on the list when it comes to security risks. In a survey of 800 cybersecurity professionals by Crowd Research Partners, more than 70% "cited data leakage or loss as their top BYOD concerns" ("Security Issues May Hamper," 2016, p.12). Personal phones and laptops can be taken anywhere outside the workplace and valuable corporate data can be stored within them. There is no guarantee that this data is safe from an outsider nor is there a guarantee that the data is safe with the owner of the device. Leaving a device unattended for a few seconds could be the perfect opportunity for a thief. Human error is also possible; one might accidentally press send without double checking who the data is being sent to. While some pieces of data are miniscule in terms of negative impact, there are others that can be extremely damaging. In a setting that deals with medical information, this can be a HIPAA violation if

medical records are leaked (Ong'ele, 2017). In addition, a company dealing with credit card or social security numbers can take an unrecoverable hit in reputation which can result in customer distrust, litigation, and the fall of a company. While physical theft is possible, there is always a possibility of a disgruntled employee that can be a source of an insider attack. This type of employee can take advantage of BYOD and their access to confidential information to allow unauthorized people to obtain that information. Reasons for such a behavior differ from person to person but can range from revenge from getting terminated to monetary gain. Even minor information such as employee names and emails which might not be seen as significant can be used for attacks like phishing. These attacks do not have high success rates when faced with a person that understands what a phishing email is, but one mistake from a less experienced employee can open the door for more problems. Data loss and theft are not the only data concerns of BYOD; there are other aspects of data that can be seen as a concern.

Data access is another concern of BYOD. Many questions arise when it comes to data access but the main one is the following: Who should get access to what? Obviously, the position of the employee should be taken into account when deciding this. A person from the HR team shouldn't have access to networking diagrams and other IT information. But their position cannot be the only factor that should be considered. Two people from the same team could have two completely different BYOD devices with different levels of security measures (Careless, 2013). One can be highly secure while the other is relatively insecure. Not addressing this concern can have a negative impact in the long run. Clearly, this is not a concern with one clear-cut answer that is set in stone.

Data holds great power in a corporate setting which is why it must be treated with tremendous amounts of care. Proper data removal is another concern that can be put on the same

level as proper data access. This applies to both current and past employees. “Deleting data on smartphones is not always easy and often is not done properly” (“Used Smartphones,” 2016, p.8). In other words, just clicking and dragging an application or file into the garbage bin does not mean the data is now unrecoverable. In fact, the hard drives can continue to hold onto residual data which can range from emails to texts to videos. Applications such as forensics tools can be used to discover such data. A survey of 122 second-hand phones by Blancco Technology Group and Kroll Ontrack revealed that 48% of hard disk drives and solid-state drives had residual data and 35% of phones had leftover emails, call logs, texts, photos, and videos that were retrieved (“Used Smartphones,” 2016). In addition, 57% of used mobile devices and 75% of used hard drives had unsuccessful deletion attempts (“Used Smartphones,” 2016). These numbers are not to scoff at especially for companies utilizing BYOD. This means that a phone that an employee supposedly cleared out before selling could still be holding onto remnants of confidential data that are now in the hands of an unauthorized user. Without any intervention to ensure proper deletion, this can be an unfortunate case of a data breach. It would not be surprising if hackers or other people with evil intentions take advantage of this fact and search for used phones being sold on the market.

Another disadvantage deals with legal concerns. There are many laws in place that can be construed differently since it was not originally designed to accommodate the extremely volatile nature of technological changes. For example, there may be overtime issues under the U.S. Fair Labor Standards Act; if an employee accesses corporate data outside of working hours, the question of whether it is overtime that must be compensated has to be answered to avoid litigation (Rieders & Monroy, 2014). One must be careful about BYOD so that scenarios like this and violations such as HIPAA complaints can be avoided.

Privacy concerns can also be tied in with legal concerns. BYOD devices can contain both private employee data and corporate data. An average user would most likely reject a company from seeing the private data stored on the phone. This becomes an issue for employers and employees when deciding what information an employer is allowed to access without infringing on employees' rights (Teare & Glynn, 2014). A scenario dealing with an internal company investigation can bring this concern to light. If an employee was sexually harassing another employee, an investigation might wish to see the text messages of the harasser (Teare & Gylnn, 2014). However, this can be seen as an invasion of privacy and a lawsuit might be unavoidable. This concern must be carefully taken into consideration when allowing BYOD to prevent any outcomes that can be consequential for both the employer and employee.

Under BYOD, devices brought from home are allowed to connect to the corporate network. Many companies even allow the device to remotely connect to the networks from outside the office. These devices can serve as a possible foothold to compromise the network. COPE devices would have strict rules that block access to certain websites and unauthorized downloads. Contrastingly, BYOD devices do not have such rules imposed on them. An employee can unknowingly connect to a malicious WiFi network or download an unsafe application that contains malware or a virus ("Security Issues May Hamper," 2016). When this infected device is brought onto the network, that "infection" can spread and can result in numerous undesirable outcomes. This can range from a person with evil intentions quietly stealing information or a virus bringing a network down. For some companies, a few seconds of downtime can be equivalent to millions of dollars of revenue loss. This is not something that would be desired by a company using BYOD to cut down on costs. One in five organizations were affected by mobile security breaches from malware and malicious WiFi ("Security Issues

May Hamper," 2016). This is a very high number when considering the possible effects of this vulnerability. Whether it was intentional or not, this is a high priority risk that can affect a company's livelihood.

The diversity of devices should not be forgotten when using BYOD models. "Even if every BYOD smart phone, tablet and laptop were secure, the sheer volume of options also provides headaches for IT departments" (Careless, 2013, p.13). There are way too many different types of devices which makes supporting every one of them an almost impossible task without sinking a lot of money into the IT budget. For example, Android phones have multiple versions, different functions, and are made by different manufacturers which makes each model different from one another (Careless, 2013). Different vendors have different risks and therefore, mitigating risk can be a daunting task for BYOD devices.

Aside from these many security risks, lack of policies is another huge danger that plagues many organizations. Simply allowing anyone to bring any device, connect to the corporate network, and access any information they want is a recipe for disaster. Policies are a must to prevent this but many are lacking or barely beneficial. In a survey in 2015 of 447 U.S. businesses, "53% haven't implemented a formal [BYOD] policy to protect their data" and "more than one-fourth admitted to having no systematic security approach" ("Half of U.S. firms," 2016, p.13). These policies are designed with the purpose of protecting confidential data, preventing unauthorized access, and safeguarding any risks of using BYOD. For example, a policy might have no words that enforces multifactor authentication, lock outs after sign in failures, and strong passwords. Critical information being obtained by unauthorized personnel can be prevented by incorporating and enforcing these practices into the policy ("Half of U.S. firms," 2016). Many

problems and concerns can be avoided with properly worded and well thought-out policies that the employee signs and consents to.

Security is, without a doubt, an issue that cannot be taken lightly. Yet, actions speak louder than words for many businesses. There is an apparent lack of increase in security funding despite the importance of security. The number of breaches, threats, and regulations are increasing at an insurmountable pace but according to the Crowd Research Partners survey, 37% of organizations have no plans on changing the budget, only 30% said they are increasing their budget, and 7% said it will be decreased (Burt, 2016). New vulnerabilities are not rare occurrences but with no extra funding, a costlier outcome would not be shocking. This will only result in more problems that will require even more money to clean up. One of the perks of BYOD was to have reduced costs but the opposite of this can occur without proper funding and countermeasures. Security should definitely be a higher priority.

Evidently, the reality of BYOD is that it is by no means perfect. Employers do not have full control over the devices and can only define and control the levels of access of the BYOD device (Careless, 2013). The level will determine the devices' access to the networks, applications, and data of the company. This will prevent anyone from wreaking havoc without proper permissions. Employers must also understand the thought process of both employees and employers when choosing a device for corporate use. Under COPE, employers would prioritize job functionality, security, and ruggedness (Careless, 2013). After all, their purpose is to increase productivity and save money for the betterment of the company. They would not want a phone or laptop that cannot run all necessary applications, is insecure, is beyond affordable, and is easily breakable. This thought process would not pertain to an average consumer who would in this case be the employee. They would "tend to buy devices based on fashion, peer pressure, and

even downright whim" (Careless, 2013, p.13). This difference in mentality can be dangerous if it is not taken into consideration since assuming that all devices are compatible in the given work environment can lead to future troubles and headaches.

Ignoring these threats and risks essentially becomes a gamble to the business. If luck is on their side, nothing detrimental might happen. But chances are, that will not be the case at all. Surveys revealed that security threats can take a toll on IT resources and helpdesk workloads ("Security Issues May Hamper," 2016). The threatened security can result in both reductions of productivity for the employee and business as a whole. Litigation or network problems can be extremely costly to deal with which counteracts the perk of using BYOD to reduce costs. Taking this gamble is not even worth considering. Actions must be taken without a doubt, so possible problems can be spotted before it happens and dealt with accordingly.

The first step is to create proper policies and make sure that it is enforced. A popular mobile game called Pokémon Go gives good reason for a strong policy to be required and enforced for BYOD. The game is quite simple; you hunt for virtual monsters called Pokémon and try to catch them so that they can be used for battle against other players. What does this game have anything to do with BYOD policies? BYOD policies cannot restrict downloading games to an employee's personal device ("Pokémon Go," 2016). However, this game has full access to a player's Gmail, files, and location details which is clearly stated in the privacy policy as being used as an asset of the developer ("Pokémon Go," 2016). Corporate data is at risk when accepting this game's policy which is why a strong policy should be written to combat Pokémon Go and other phone applications that require similar access. Firstly, this includes training employees on proper device usage so they understand what these privacy permissions mean and to not spend time on the game during work hours. The phones should not be jailbroken when

accessing corporate network to prevent unauthorized running of applications. Jailbreaking a phone deals with gaining access to the operating system and running applications that are not allowed can bring the network concerns stated earlier to light ("Pokémon Go," 2016). All corporate data and devices should be encrypted. In the world of IT and anything dealing with confidential data, encryption should not be questioned. Finally, network access should be restricted if employees refuse to install security tools ("Pokémon Go," 2016). This is just a quick overview of possible policy considerations for this phone game. But there are many more important things to consider when creating a BYOD policy.

Considerations for BYOD policy are not set in stone and can differ from one business to another. There are many factors such as the size of the business, the type of business, possible scenarios, and employee positions that must be taken into account when incorporating it into a policy. "The first step in deciding whether to BYOD or not to BYOD should be to weigh the potential productivity concerns against the potential productivity benefits" (Rosenberg, 2016, p.26). After all, someone who is working in a manufacturing plant that does not need a phone for the job has no need for a BYOD policy while someone in the sales team would benefit from having their own BYOD device (Rosenberg, 2016). Once that is decided, many aspects of the policy should be considered.

Employee productivity and consent is an important consideration that states why the BYOD model is being used and whether the employee will consent to the policy. This can include limitations on how the personal device can be used while the user is employed (Rieders & Monroy, 2014). For example, the BYOD device might be used for meetings with colleagues and receiving or sending important emails. The acceptable use terms might specify that watching Netflix or browsing Facebook and Reddit is not allowed.

Next thing to consider is related to security and what must be done to ensure that the BYOD device is up to security standard. This includes encryption of corporate data and using malware protection or antivirus software. Antivirus and antimalware software will not guarantee complete protection but will still provide an extra layer of protection for both the device and network that it is being connected to. A strong password and multi factor authentication to authenticate a user should also be required. Using long alphanumeric passwords with symbols that is enforced to change every few months can be annoying to the employee but mitigate any security concerns. Also, using a multifactor authentication such as using both passphrases and fingerprint scans can further mitigate these concerns. For certain organizations, it might be necessary to enforce the ability to log, monitor, and report devices ("Security Issues May Hamper," 2016). This can fall under the policy concern so it must be well thought-out. Data segregation should be considered so personal data of the user is separate from corporate data. This will allow employers to easily define the owner of the data and in the case of device theft, remote-wipe can be a possible solution (Rieders & Monroy, 2014). The approved storage methods should be considered in the policy. This will prevent data from being shared onto risky cloud services or stored locally with no protection (Rieders & Monroy, 2014). As stated before, network access should be restricted accordingly based on how the company sees fit. Possible future litigation must be considered so that the company is protected in all scenarios. These future litigation scenarios can comprise of considerations dealing with how a personal phone is dealt with during termination or when the policy is violated (Gatewood, 2012). Cost should be considered so employees know exactly what the employer will cover and is liable for (Hinkes, 2013). This would include things like phone replacements, roaming charges, service fees, etc.

As one can see, there are many things to consider so that a BYOD policy "that balances the company's needs with employees' protected rights" can be created (Ong'ele, 2017, p.6). The strictness of the policy can be adjusted based on the organization's needs. Restricting use of certain carriers, prohibiting and limiting software, and determining how "organizational policies will be audited, assessed, and enforced" will greatly differ from one place to another (Gatewood, 2012, p.28). Despite the differences, it should be clearly stated in the policy. There should be no gray area for these policy considerations or it will spell trouble for both the employee and employer. When an employee consents to a BYOD policy and signs it, they should understand exactly what they are getting into. This is why training is such a vital part of employing someone in a BYOD environment.

Copies of the policy should be given to an employee and training should be given so they truly understand the meaning behind policies and how it will be enforced. The importance of compliance should be stressed. If the employee is not on the same page as the employer, the BYOD policy will be useless (Hinkes, 2013). Also, not everyone has a degree in cyber security or is knowledgeable about the field and its dangers. Training should not only include the proper use of the mobile devices but also include teaching the security risks of BYOD and how to prevent such risks. Proper onboarding and training systems that are in place can be helpful for everyone involved.

For many people, data segregation might be a confusing topic. It must be considered when dealing with BYOD devices and corporate data. Simply put, it separates the company assets by placing it in a secure location on the phone. This can be done with something known as mobile device management software or MDM for short (Rosenberg, 2016). Just using this software for separation is not enough for a strong BYOD policy. These tools should also be used

for remote monitoring and wiping if the situation calls for it; by having this as a prerequisite, it is possible to protect against many of the security concerns that were listed before (Rosenberg, 2016). The Crowd Research Partners survey revealed that 43% of 800 cyber security professionals had workplaces that used MDM tools which is not an overwhelming number (Burt, 2016). More companies should make use of this tool to protect company assets from the wrong hands. By "containerizing" data and giving "visibility and control over that content," according to Mark Lorion of Apperian, legal and technical challenges can be addressed and overcome when it comes to data ("Proliferation of BYOD," 2017, p.11).

Once all considerations for a BYOD policy have been thought out, the next step is to actually get started with actually creating it. Stakeholders should be involved so that input from multiple teams can be incorporated. The IT team cannot pull this task off by themselves. It should be a "joint participation of legal, management, compliance, risk, and IT" teams to ensure that the governance strategy is up to par with what the organization is looking for and for nothing to be missed (Hinkes, 2013, p.2). Next step is to address the issue of data and network access by giving access using the principle of least privileges. An employee should not be able to access every part of the enterprise unless that privilege is required (Careless, 2013). Doing the opposite will only serve as additional risk to using BYOD. The next phase involves thinking outside the box or in this case, thinking outside the network schema. "Proprietary data [should] stay proprietary" which might not apply when data is uploaded onto a public cloud (Careless, 2013, p.13). Uploading that data can result in ownership moving to that cloud operator. Once again, the importance of data ownership is emphasized and should be stressed in the policy. The fifth step is to document vulnerabilities of the possible BYOD devices. Each device has its own weaknesses and understanding that can make or break a company from utilizing BYOD fully. If

the dangers outweighs the benefits, the policy should completely prevent the usage of that device. It is not worth the risk to the organization. Lastly, there is no such thing as a problem-free world so every possible problem should be accounted for (Careless, 2013). How to act when a phone is lost and how to adjust network or data access based on situations like a demotion or transferring to a different group are all things that should be incorporated. This will allow the organization to continue functioning when the problem surfaces. This would include specific protocols to follow like who to contact (Gatewood, 2012). Once all of these strategies have been incorporated into the BYOD policy, one must decide whether that policy is sufficient.

What makes it a good policy? First off, the risks of utilizing BYOD should be reduced by properly "outlining preventive controls, emphasizing security, and informing employees of their responsibilities for keeping data safe" (Rieders & Monroy, 2014, p.38). The policy should not be so strict to the point of absolutely no freedom. That would be both difficult to enforce and an infringement on the employees' rights. There should be a balance between not jeopardizing integrity and confidentiality of corporate data and allowing the user to customize and download as they please as long as it is compliant with the policy (Armando et al., 2015). A good policy will take into account other company policies for BYOD. For example, preventing discrimination and harassment while using a BYOD device (Rosenberg, 2016). Safety should also be considered to prevent safety violations or accidents due to phone usage while doing tasks like driving (Rosenberg, 2016). Lastly, attention must be given to the fact that "technology grows quickly and in unanticipated directions" (Teare & Glynn, 2014, p.16). This is not something can be thought up in a day or two. Careful consideration, team collaboration, and smart planning is a necessity and not optional for a good BYOD policy.

Without a doubt, BYOD is here to stay. Smartphones, tablets, and laptops are an integral part of our lives and it is hard to imagine a world without them. Organizations of all shapes and sizes understand this and are ready or have already started implementing BYOD devices. It "enables information pervasiveness by allowing employees to perform both official and unofficial activities" on a personal device (Ganiyu & Jimoh, 2018, p.49). There are many advantages and disadvantages that an organization must consider if they plan on using the BYOD model. The shortcomings might be unappealing to some people, but by understanding the concerns and risks and incorporating this information to create and enforce a strong BYOD policy, the benefits will outweigh the drawbacks. Both the organization and its employees can benefit greatly and continue its course to success.

References

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2015). Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*, *14*(2), 123–140. https://doi-org.ezproxy.gl.iit.edu/10.1007/s10207-014-0252-y

Burt, J. (2016). BYOD brings greater productivity--as well as security issues. *EWeek*, 1.

Careless, J. (2013). Establishing a realistic BYOD governance policy. *KM World*, *22*(1), 12–22.

Ganiyu, S. O., & Jimoh, R. G. (2018). Characterising risk factors and countermeasures for risk evaluation of Bring Your Own Device strategy. *International Journal of Information Security Science*, *7*(1), 49–59.

Gatewood, B. (2012). The nuts and bolts of making BYOD work. *Information Management Journal*, *46*(6), 26–30.

Half of U.S. firms lack formal BYOD policy. (2016). *Information Management Journal*, *50*(1), 13.

Hinkes, A. (2013). BYOD policies: A litigation perspective. *Corporate Counsel Litigation*, *27*(2), 2–7.

Ong'ele, M. (2017). BYOD: Practices and policies to promote preservation. *Health Law Litigation*, *14*(1), 5–7.

Pokémon Go proves that companies need strong BYOD policies. (2016). *Information Management Journal*, *50*(6), 6.

Proliferation of BYOD leads to e-discovery headaches. (2017). *Information Management Journal*, *51*(4), 11.

Rieders, L., & Monroy, M. (2014). Does your practice have a mobile device policy? *Urology Times*, *42*(13), 38.

Rosenberg, S. (2016). Bring your own device? Make sure to cover your security and liability concerns, too. *Workforce*, *95*(9), 26–27.

Scardilli, B. (2014). BYOD or COPE: The best mobile strategy for the workplace. *Information Today*, *31*(2), 1–36.

Security issues may hamper BYOD adoption. (2016). *Information Management Journal*, *50*(4), 12.

Teare, T. D., & Glynn, C. P. (2014). Technology and employee privacy concerns: The current state of uncertainty. *Employment & Labor Relations Law*, *12*(4), 12–16.

Used smartphones often hold past users' data. (2016). *Information Management Journal*, *50*(1), 8.