BYOD:
A Matter of Policy

LLM LIQUID LITIGATION MANAGEMENT, INC. | Logical Solution. Legendary Service.

Gone are the days of Dolly Parton's "working 9 to 5." For many, when the morning alarm goes off the workday begins with the drowsy scrolling through of emails and texts.

It can continue through lunch with a phone in one hand and fork in the other, and extend well into the evening with any number of personal devices hosting company emails and information to review and respond to before the alarm goes off again hours later. This blurring of professional and personal lives through Bring Your Own Device (BYOD) programs can not only be problematic for employees seeking work-life balance, but also for companies pressed to provide adequate data security on those same devices, especially in advance of possible future litigation.

The proliferation of digital device options, designing and customization of company apps, optimization of company websites for mobile, and advancement of technology are here and on the move. Through such advances that were once unthinkable, companies can now experience increased efficiency and higher productivity. Rather than try to stifle employees' (or a company's) adoption of technology or limit it to company-issued devices, a company would be best served by learning how to adapt.

This white paper will explore how companies can reduce legal and liability risk through a sound, enforceable security policy while still enjoying BYOD benefits, including hardware cost-savings and a more efficient and productive workforce that chooses to work wherever they are.

THE CASE FOR POSSESSION, CUSTODY OR CONTROL

Under Fed. R. Civ. P. 34, whether discovery obligations are tied to employees' personal devices depends on whether those devices are within the "possession, custody or control" of that company. While pertinent case law is not particularly ample, there are a handful of significant cases that address discovery of data on personal devices used for business purposes.

Rather than try to stifle employees' (or a company's) adoption of technology or limit it to company-issued devices, a company would be best served by learning how to adapt.

In the pharmaceutical case of *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation* out of the Southern District of Illinois, the court found that in order to preserve text messages that might be relevant to a lawsuit, a legal hold should also apply to personal and company-issued devices.

> "The defendants raised the issue that some employees use their personal cell phones while on business and utilize the texting feature of those phones for business purposes yet balk at the request of litigation lawyers to examine these personal phones. The litigation hold and the requirement to produce relevant text messages, without question, applies to that space on employees cell phones dedicated to the business which is relevant to this litigation."[1]

The court did not agree with the defendants' argument that "text messages are a less prominent form of communication and that the production of text messages is too burdensome" and issued sanctions totaling nearly $1 million dollars for failure to preserve those text messages and turn off the company's auto-delete function of text messages during the legal hold as well as other "egregious" acts.[2]

Where employees' personal devices are not used for business purposes, however, some courts have ruled that those devices are, in fact, not in the "possession, custody, or control" of that company.

BYOD programs can also generate other issues, including when software for deletion of data may applied to employees' devices that have been lost, stolen or surrendered as well as whether employee consent is required to retrieve data on devices.

For example, in the employment discrimination case of *Cotton v. Costco Wholesale Corp.* the District of Kansas denied the plaintiff's motion to compel production of text messages from employees' devices. The court ruled that because the plaintiff could not show either that the defendant issued employees' devices or that the employees used the devices for business-related matters, those devices were not within Costco's "possession, custody or control."

> "Mr. Cotton does not contend that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand. Accordingly, it appears to the court that Costco does not likely have within its possession, custody, or control of text messages sent or received by these individuals on their personal cell phones. Mr. Cotton's motion to compel is denied with respect to this request."[3]

A third case turns from personal phones to laptops. In *Han v. Futurewei Technologies, Inc.* (the defendant's d/b/a is Huawei Technologies), the defendant in a harassment case in the Southern District of California sought an order requiring the plaintiff to allow it to copy the hard drives off her personal computer devices because she had deleted the files from her company-issued laptop. That request was denied.

> "... Huawei's request to copy the hard drives of Han's personal computing devices is premature. It is premature not only because Huawei presently does not have a counterclaim pending against Han, but because Huawei has not demonstrated that obtaining mirror images of Han's computing devices is necessary or justified. Huawei has not established that Han is in the wrongful possession of an company documents, or that the copying and 'wiping' of files from her work laptop was improper or malicious."[4]

As these three cases reveal, in addition to establishing "possession, custody or control," companies' BYOD programs can also generate other issues, including when software for deletion of data may applied to employees' devices that have been lost, stolen or surrendered as well as whether employee consent is required to retrieve data on devices.

CREATING AN ENFORCEABLE BYOD POLICY

The first step to creating a sound, enforceable security policy for BYOD that can help reduce legal and liability risk is to examine the current security policy or policies in place, including:[5]

- mobile device security policies
- password policies
- encryption policies
- data classification policies
- acceptable use policies
- antivirus software policies
- wireless access policies
- incident response policies
- remote working policies
- privacy policies

Are there inconsistencies? As David Navetta of the Information Law Group advises, if so, "organizations need to be ready to explain, why, despite the failure to follow policies that apply to similar devices, the security of an employee's personal device was still reasonable."[6]

After reviewing current policies in place and identifying any inconsistencies, a company should determine whether the BYOD policy will be voluntary, mandatory or a combination of both. Scott A. Milner and James P. Walsh, Jr. of Morgan Lewis advise that factors determining this should include what type of business and data are involved, what positions are eligible for BYOD, the nature of the employee's work and cost considerations.[7]

Next, laying out the scope, specific devices supported and security requirements — a who's who and what's what. A company must decide which employees will be required to follow the policy, which devices are permitted and the parameters — limitations, system requirements and configurations — and what the security requirements are, including whether to utilize a mobile device management (MDM) solution.[8]

Part of the enterprise mobility management (EMM) approach, an MDM solution enables companies to protect and manage mobile devices remotely. They can configure and update devices through defined security policies that ensure the devices remain compliant. Policies and features include device settings, user authentication, encryption of data, and support for backing up or remotely wiping corporate data. Some mobility solutions go beyond device configuration and offer corporate application and content management as well. Additionally, the system is not static. The management frameworks allow organizations to respond to any future changes to the BYOD or information security policies by pushing them to the devices. [9]

More on security: Because personal devices don't have the protection of a 24-hour security system like for devices in-house, additional measures like biometrics (fingerprints) are becoming increasingly available. Employees must be encouraged to keep their security software updated and to avoid the common "keep me signed in" login option. While many advise that access to the device should be restricted to employees only — no friends or family — this is not often practical. Think: kids and YouTube. Microsoft has the following recommendation on how to address family use when crafting a BYOD policy.

> "Personal Devices often shared around the family – think of the laptop or tablet which Dad shares with the kids, for example. Even a watertight acceptable use policy can't be signed on behalf of other family members. Your employees cannot be held responsible for their kids' use of a family device: if that affects your attitude to data, then it also ought to affect your attitude to BYOD."[10]

This is where the implementation of an MDM solution or app-specific work on a device could alleviate such security concerns.

We arrive at the matter of consent. It's advisable that "employees should affirmatively consent and waive the employer's access, review and collection of data on the personal device." It should clearly address the company's potential legal or technical needs in the future. Furthermore, the policy should inform the employee that privacy — even of personal information — cannot be expected.[11]

As mentioned earlier, a company should have a process in place that allows for the remote deletion of business data in the event the device is lost or stolen. Other possible policy criteria include having a device and data procedure in place when the employee exits the company

(and it's important to inform employees that there is the potential that in addition to business data, personal data may be deleted from the device upon separation from the company); reimbursement to the employee for BYOD use; and what technical support, if any, will be available to the employee.[12]

In addition to the recommended criteria, it's important to consider how rigid the policy is and whether employees will be able or want to comply. Also, being as transparent as possible with employees about what type of monitoring the company will be doing of personal devices is important to gaining employees' buy-in to the policy. Most important of all, is this policy enforceable? If steps are not taken to ensure employees are meeting the requirements, then the careful crafting of the policy is moot and the company is open to great legal and liability risk.

BYOD AND LEGAL HOLDS

How should employees who engage in BYOD react when a legal hold is issued? They should view their phone, tablet or laptop like a company-issued desktop and take steps to preserve all pertinent company data on these personal devices as if they were seated in the office. A timely, thorough response to maintain compliance is critical. While employees "should" view their device in this way, whether they actually "do" is another matter. Therefore, it's important that the user's duty to cooperate and preserve in the event of a legal hold is clear and undeniable in the policy.

CONCLUSION

As new devices roll out with more bells and whistles and productivity demands on employees increase, the professional and personal lines will continue to blur. Companies can choose to catch up, stay current and ensure their employees are compliant all along the way or get left behind and be at great risk for sanctions. While there have been many recommendations offered, it's essential that a policy that best fits a company's personality, work and security needs is created and — above all — that the policy is enforceable. Without an enforceable policy, the BYOD policy is moot.

REFERENCES

[1] *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation, 2013 BL 347278 (S.D. Ill. Dec. 9, 2013),* at 18.

[2] *Id.* at 5.

[3] *Cotton v. Costco Wholesale Corp., Case No. 12-2731-JWL, (D. Kan. July 24, 2013),* at 11.

[4] *Han v. Futurewei Technologies, Inc., No. 11-CV-8310-JM (JMA), 2011 WL 4344301 (S.D. Cal. Sept. 15, 2011),* at 6.

[5] David Navetta, *The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device),* Information Law Group, available at http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/.

[6] *Id.*

[7] Scott A. Milner & James P. Walsh, Jr., *Key Elements of an Effective Bring-Your-Own-Device Policy, The Legal Intelligencer (October 2013), available at* http://www.morganlewis.com/index.cfm/publicationID/77681f29-c7f8-434b-8b5f-5cd7048053eb/fuseaction/publication.detail.

[8] *Id.*

[9] Kasia Lorenc & Fritz Nelson, *Mobile Device Management: 2014 Vendors and Comparison Guide,* Tom's IT Pro (June 10, 2014), *available at* http://www.tomsitpro.com/articles/mdm-vendor-comparison,2-681.html.

[11] *Id.*

[12] *Supra* note 7.