JANUARY 16, 2014

LTN
LAW TECHNOLOGY NEWS

An ALM Publication

Vendor Voice: BYOD Is the No. 1 E-Discovery Challenge for 2014

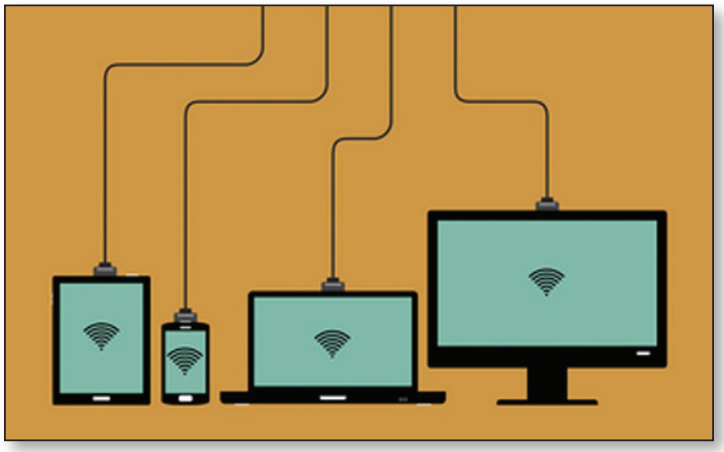
In a survey of inside counsel at Fortune 1,000 companies, FTI Consulting found that the number one e-discovery challenge listed for the coming years is "bring your own device" to work.

By Erik Hammerquist

The trend of "bring your own device," to the workplace has been a growing topic of interest for legal and IT professionals. BYOD both impacts a company's current and future IT decisions and is changing the landscape for forensic investigations and e-discovery. It brings new complexity, processes and nuance to what many people think is a relatively straightforward, technical exercise. In a survey of inside counsel at Fortune 1,000 companies, FTI Consulting found that the number one e-discovery challenge listed for the coming years is BYOD.

We have worked on a number of cases involving personal devices in the workplace that were later needed for collection of electronic data. In one matter involving alleged IP theft, the people in question regularly used personal thumb drives to facilitate working from home on personal computers. When these custodians left to join a different company, their home computers came into scope for analysis. Other matters have required data collection from a personal computer to take place in a custodian's home. These sensitive—and sometimes awkward—situations raise many important considerations for companies to address BYOD through policies before opening systems up to personal devices.

The best way to walk this line is to define clearly the types of data that could become responsive to investigations or discovery and understand any limitations that may exist with each device in question. But most importantly, steps must be taken in advance of a matter to proactively protect both the employer and the employees and define what rights each have when it comes to personal devices being used for business communications.



idspopd - Fotolia

BYOD EVOLUTION

In the past, personal cell phones were more frequently ruled out of investigations unless call activity was relevant. This was because the majority of such use was limited to company email and any local content would typically be duplicative of their server mailbox, which was far more convenient to collect. However, the tide is turning on this as people are increasingly using text messaging for substantive business communications.

In one such recent case, the cell phone owner in question happened to be the client's chief of security, perhaps helping to explain why no one at the client company wanted to pressure him for his phone. Most of the BYOD discussion focuses on mobile devices, but personal computers and thumb drives can't be left out of consideration. We've seen the BYOD phenomena

bring several personal computers into play. For example, on the restatement of a financial statement, the way a custodian described to counsel how he worked from home required him to drive me, in his own car, to his home so we could collect data from his personal computer.

FOUR IMPORTANT STEPS

The main focus for IT and legal departments trying to address BYOD concerns is to think down the road to the worst-case scenario that could happen with an employee using a personal device for work. If something goes terribly wrong in the company, or employees are doing something illegal, companies need to have a well-thought out policy as well as technology systems in place to ensure access to relevant data without excessive expense or difficulty. Policies should be developed by stakeholders in legal, IT, human resources and compliance, and be in place before the company's systems are opened up to personal devices. Ideally, employees would sign plain-English contracts agreeing to adhere to these policies in advance.

BYOD policies should clearly answer questions such as: What will BYOD users be allowed to access? How will IT extend and control this access? What reach into personal devices will the company have in times of litigation or when someone leaves the company? The last question can get sticky without a policy in place.

Second, it is key to thoroughly investigate the available options to protect data on these devices. There are solutions available now that allow companies to extend enterprise management to personal devices. One very attractive feature is the ability to segment company from personal data, keeping the employee's own information private. The main thing to look for when evaluating these types of technology packages is that the solution can effectively execute on what has been outlined in the personal device use policy, and that the technology isn't going to inadvertently do anything that is not disclosed in that policy. This helps the company maintain trust with employees while also covering all necessary ground for protecting important data on personal devices.

Third, always keep data privacy laws in mind. Both U.S. and non-U.S. citizens who work for your company abroad are highly likely to have different data privacy rights than those based in the U.S. and violating those could be a very expensive and painful ordeal. This may very well extend to non-U.S. citizens who work for your company in the U.S. Further, there are many legal issues with moving data internationally, which pose a problem for collecting data from employees who are U.S. citizens but working in another country, and which may not be properly addressed in a blanket manner by policies signed at the start of someone's employment. Additionally, several U.S. states have their own data privacy laws and many U.S. legislators are considering moving to a more European data privacy model. Take time to understand the privacy laws that may impact your company, stay abreast of their continuous evolution and be sure to account for those in all policies and technology implementations.

Finally, consider your scope and limitations. Now that you can no longer rule out personal mobile devices, how do you fulfill your preservation and collection responsibilities without violating the custodian's privacy or trust? The best way to walk this line is to define clearly the types of responsive data required and understand any limitations that may exist with each device in question.

The collection model for a computer hard drive, aka image it now and cull the data later, isn't always an option with mobile devices, especially personal devices. Each device is different and may have built-in security measures that prevent the extraction of certain information. What's worse, those measures can literally change overnight and that there is little to nothing you can do about that. Cellular providers and device manufacturers push updates over the air when it suits them. Therefore, data that can be easily extracted today could be encrypted and inaccessible tomorrow.

Improper handling of BYOD in the workplace can create a multitude of headaches for legal and IT. In the case mentioned earlier involving the need to access text messages on the CSO's personal cell phone, the company ultimately had to involve a second law firm to specifically, and singularly, deal with the matter. The company had to spend additional expense on the issue and was further exposed to the various risks of either finding a way to access the texts, or pay penalties or sanctions for not producing that data.

BYOD has many advantages, including increased productivity and reduced data plan expenses. However, companies are best served by holding off allowing personal devices in the workplace until all of the necessary steps and safeguards have been put into place first.

Erik Hammerquist *is a senior director of the computer forensics segment of FTI Consulting's Technology practice and is based in Los Angeles.*