Proskauer

Transcript:

An Interview with Kristen Mathews at the IAPP Global Summit: Issues Companies Face with Allowing Employees to Use Their Personal Devices for Work Purposes

Speakers: **Kristen Mathews – Partner, head of the Privacy & Data Security Group**

Caption: *What are some of the issues companies face with allowing employees to use their personal devices for work purposes?*

Mathews: There's a host of issues, but let me give you a few of them. For one thing, if you don't address BYOD head-on – in other words, if you just let it happen – there's going to be a lot of default scenarios that aren't quite desirable from the company's perspective. As an example, if you think about it, all of the private information of the employee will naturally be in the same place on the device, mixed together with the work-related stuff. And therefore if the company later wants to separate them for any number of reasons, it'll be difficult for them to be able to. Another example, if left to his own devices, no pun intended, he could – the employee could set the password, add a very weak password on the device, or to no password at all. Another example, without any solution in place, if the company has a situation in litigation and needs to ask that the employee hand over the device to the employer – maybe there's a litigation-hold situation – or an e-discovery request – it will be difficult for the employee to be required to do that, given that it is the employee's own device in question.

Caption: *What are the solutions to these issues?*

Mathews: The solution is twofold. It's a combination of a technology solution and a legal solution. Let me tell you about the technology solution first. It's called MDM, or mobile device management. Another term which is similar is mobile application management. But in both cases, it's essentially technology that is installed on the machine by the employer that enables the device to be controlled from a security standpoint. So, as an example, it forces complex passwords to be used on the device. It partitions the device between personal and work, so that if needed later, the employer can do something with the work side without doing something with the personal side. It also enables the employer to remotely wipe the device clean, under various circumstances. And some MDM technologies enable the employer to wipe just the work side of the device clean without touching the personal side, or they can wipe the whole device clean.

Caption: *For BYOD (Bring Your Own Device) you need a combined solution, both legal and technology.*

Mathews: On the legal side however, there's another host of solutions, and you can't do one without the other. You need both. So on the legal side, you're going to want a policy, at least, or maybe even a terms and conditions that's agreed to by the employee, that agrees to certain things up front. For example, the employee would agree in advance that, under circumstances, they're going to have to turn over that device to the employer. They're also going to acknowledge that the employer is going to be – is going to have the right to monitor certain usage of the device.

Caption: *Are there any other issues that are difficult to address with legal or technical solutions?*

Mathews: A lot of employers at first blush would think that their ability to wipe that device clean remotely is a solution to a lot of the problems. However, if you think about it, if a thief, for example, were to turn airplane mode on on the device, after having the device, suddenly the ability to wipe that device clean remotely disappears. Another example is, one would think that that partitioning of the device between the work side and the personal side would be a solution, but a lot of times it's not an absolute partition. For example, there may be the ability to copy and paste from one side to the other. Or you might be able to open up a document from an email, such that it opens into an application on the other side of the partition. Another example is thinking about backups. The employee goes home and backs up the device to his or her home computer. Suddenly, there's a lot of company information on the employee's home computer, which isn't exactly desirable. And then thinking further about that is iCloud, or other Cloud backup services. All you have to do is say "yes" on the device, and suddenly, again, the material from the device is being stored not only on the employee's home computer, but on a third-party Cloud system, and if the employer doesn't have some kind of corporate agreement with that third party, the third party has the data with no agreement in place to protect it.

Caption: *Will regulations in this area get stricter?*

Mention: I do not actually anticipate us seeing any legislation that becomes enacted in this country on this point. This is the type of thing that, in my experience, our Congress lets the industry deal with, self-regulation.