JUNE 9, 2016

Legaltech® news

ONLINE

An ALM Publication

In Mobile E-Discovery, Tech Often a Barrier and Privacy Frequently Blurred

Beyond encryption, mobile e-discovery faces challenges with data retention, inaccessible custodians and ineffective BYOD policies

BY RICCI DIPSHAN

For all the ways technology has revolutionized discovery, the advancement of mobile devices has almost stopped it dead in its tracks. Though the FBI's legal battle with Apple is a pivotal moment for mobile e-discovery, the challenges of this practice go beyond recalcitrant manufacturers and encryption. For mobile devices are never used in a vacuum, and during discovery requests, attorneys have to consider everything from privacy regulations and organizations' "bring your own device" (BYOD) policies to each single data custodian's specific station.

"On a very simple, basic level, if you have to discover information, and that information happens to be on mobile devices around the organization," said Galina Datskovsky, CEO of Vaporstream, "one of the challenges you clearly face is getting the device to come back into the organization to begin with. And that can be quite a challenge."

Given corporate servers and cloud infrastructure, however, there are inevitably times when "discovery doesn't have to go back to your device, because I'm creating a record and putting it in my secure archive, and that's where I'm going to go to pick up the data," Datskovsky added.

But the reality is far more complex, for not all mobile data and apps are made to sync up to external servers. "The devices are unique," Datskovsky explained, because "there are things that only reside as mobile apps, like, for instance, text and chat or certain apps that may be apps that only reside on the device," and save data locally.

This in turn makes discovery a uniquely manual experience, where much depends on the data custodian's ability or desire to give up the device. This can make for a difficult situation, "especially if it happens to be an employee who left or quit or is not cooperative. And, yes, there are subpoenas and things you can issue but it just makes the processes fairly difficult," Datskovsky said.

"What's interesting is that to actually collect the device one literally just has to ask the person for its password," said Adi Eliott, vice president of market planning at Epiq Systems. He added that the discovery process largely relies

on custodian interviews, such as those "asking them what do you use to talk about business, what apps you discuss this matter or this situation on, and then you have to physically get their device, [and] unlock it."

Retention, In Theory

Data that solely resides on a mobile phone is data that can also be erased entirely, a real concern to discovery practitioners given not only a user's varying whims, but technical nuances of mobile devices as well.

"Phones aren't designed to preserve things," Eliott said. "You get different kinds of access, you get different results depending on the device, and even then there is some nuance of how far back the logging of text messages goes for instance. The iPhone has multiple settings. There's a setting of 'keep everything' versus 'not keep everything' and if you don't keep everything it just erases stuff on its own accord and you don't have rhyme or reason for it."

For e-discovery of corporate data on BYOD or corporate-owned mobile devices, Datskovsky believes that the problems of retention can be solved if organizations are clear in notifying employees that "there are certain applications they can use for work and certain applications that they do not use for work," and that employees should "try to keep those very separate."

In theory this should work if clearly stated in an organization's BYOD policy and enforced through a mobile management software. Datskovsky noted that some of these technologies, such as Mobile App Management (MAM), are effective because "they put a container [on the device] and that container has all the corporate data. Then [an organization has] a lot of control over what apps are allowed and where the data resides and how it is controlled."

"It certainly makes the e-discovery process simple," she added.

But Eliott noted that in reality, separating business from personal is far harder than it seems.

"We regularly counsel our clients that you have to educate [employees] on which apps to use to talk about business, primarily like email. If there's an internal instant messenger app that's officially sanctioned, use that, etc. The problem is that it's not necessarily how humans work. The friction that is required to record and communicate is almost nonexistent," Eliott explained.

"Even anecdotally if you think about it, if you and another person you know have WhatsApp, whether you're talking about personal or business, you're highly likely to fall into WhatsApp, if that just happens to be something you use because, there's no friction to it and you both have the app," he said.

Additionally, "We don't compartmentalize our communications anymore between business and personal," Eliott said. "Socially, I'm more likely to be doing something personal at work and I'm definitely more likely to be doing work on my personal time and asking us to compartmentalize by app is largely a human and a social challenge more than it is an e-discovery challenge."

Privacy, By Any Other Name

The blurred lines between private and business data create situations where "if there is discovery done on a device that is owned by [an employee] but has corporate data, some personal data can be looked at whether it's accidental or not," Datskovsky said. "The privacy can be jeopardized and they need to be comfortable with that concept."

Yet Eliott noted that this is not a big challenge in the U.S., as "when there is litigation and when the individual is involved there is far less likely to be privacy concerns raised. If you have BYOD policy and you are connecting [your phone] to the corporate network and you sign something that said generally that the corporation has access to it, people don't question that largely.

"And part of this is just social and the way Americans think, they are very likely to give up their password when asked and let their device be collected from. And in Europe it very much has to be contemplated deeply because [there] are lot of rules and regulations around," he said.

But the privacy landscape, it turns out, is fluid, and it is anyone's guess what role privacy will play in the months and years to come.

Datskovsky noted that "courts have started to rule on [the issue] and there are some cases that have been decided about who has the right to the phone and the privacy rights … but it's still an emerging set of cases that we are seeing."

Eliott added that with privacy issues, "in the U.S., things are evolving. … It's being talked about more," especially after the Apple and FBI legal battle.

"The conversations are being raised in a way in which they [were] before, and my opinion is that when you see conversations raised like this, there are generally downstream consequences from the consciousness shifting on an issue. And we don't yet know what that is going to be," he said.