BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

Opinion

November 15, 2013

Technology: Embracing the use of mobile devices in e-discovery

Employees' use of mobile devices for both work and personal matters is accelerating and is likely irreversible

By Gareth Evans

What are the implications of mobile devices for e-discovery? Let's face it. Mobile devices are a disruptive technology. That smartphone in your pocket — like the tablet in your brief case — is more powerful than a Cray 2 supercomputer, the world's fastest computer just a quarter of a century ago. It was the size of a large washing machine.

Blurring the line between work and personal life, smartphones and tablets have become all-in-one devices. Tablets are fast becoming an alternative to PCs, and smartphones perform many of the same functions as tablets. Gartner predicts tablets will outsell PCs by 2015. Previously perceived largely as devices for content consumption, tablets are increasingly being used for content creation.

The use of consumer-oriented devices and applications for work, referred to as the "consumerization" of IT, is also now being referred to as its "appification." Apps are increasingly popular for work tasks on mobile devices. Social networking and, seemingly, everything else that we used to do solely on computers can now be done with an app on a smartphone or tablet. Mobile versions of many of the applications we use on PCs are available. If not, there is usually an app that performs the same functions.

Combined with Wi-Fi access, mobile devices are profoundly changing how many people work. The traditional PC and company server architecture is yielding to mobile devices always connected to the Internet and to various forms of cloud storage. Consequently, "Bring Your Own Device" often means "Bring Your Own Cloud." Many users store documents in online repositories such as DropBox so they can access them on the fly from various devices. Apps also may sync and store users' content over the cloud. Text and instant messaging, of course, are also particularly popular on smartphones.

Employees' use of mobile devices for both work and personal matters is accelerating and is likely irreversible. One option for companies that want to accommodate employees' desire to have their own dual-use devices is to provide them with a greater variety of corporate-owned mobile devices and to loosen restrictions on their use for personal activity. Another increasingly popular option is to allow employees to use their personally-owned devices and to implement a BYOD program.

A slew of articles have been written about BYOD, many suggesting it is best avoided, with titles such as *Bring your own discovery nightmare* and *Is BYOD a B-A-D idea?*. But many BYOD issues, such as communications and content residing outside of corporate

servers and firewalls, can be inherent to mobile devices regardless of ownership. Granted, having employees agree that the company has the right to access and extract data from employee-owned devices is important. And having the ability to control what apps may be installed on a company-issued device can be helpful. But there is some evidence that employees — particularly those in Generation Y — may nevertheless find a way around restrictions.

According to Fortinet's recently released Internet Security Census, an October 2013 survey of 3,200 employees between the ages of 21 to 32 in 20 countries, 51 percent of respondents said they would ignore any policy banning the use of personal devices for work. 89 percent responded that they have their own personal cloud storage accounts, with 70 percent using the accounts for work. 36 percent said they would break any rules intended to stop them. And 48 percent would also ignore company policies to curb their use of other emerging mobile technologies, such as Google Glass and smart watches.

Do companies have a duty to preserve and collect data from employee-owned, as opposed to company-owned, devices? Federal Rule of Civil Procedure 34 provides that a party must produce documents and electronically stored information in its "possession, custody or control." But it does not define those terms.

An inconsistent and conflicting body of case law has developed regarding what constitutes "control." Generally, two approaches have emerged. First, under the "practical ability" approach, a party is deemed to have control where it has the "right, authority, or practical ability" to obtain the documents from a nonparty. Second, under the "legal right" approach, a party is not deemed to have control unless it has actual possession of or a legal right to obtain the information. In some federal circuits, the party may also have a duty to notify the requesting party about relevant documents in the possession of third parties. These approaches have not been applied consistently even within the circuits in which they have been adopted. In more than a few cases, the decisions have lacked a careful analysis of "control."

Judicial decisions involving mobile devices have been few, but that is likely to change. ESI on personal devices has been held to be within companies' control under the practical ability approach. Under the legal right approach, even without a BYOD agreement allowing company access, a court may hold that the company has control of work-related documents under the rationale that employees created them in furtherance of their employment and have a duty to maintain them for the company's benefit.

Mobile devices therefore increasingly present a potential source of documents that should, in many circumstances, be considered for preservation and collection. Does this mean that you need to reflexively extract all data from employees' mobile devices? No. The employee must be connected to the issues and the data must be relevant or responsive. Although employees may use mobile devices, they may not have used them for relevant or responsive communications and documents. In the emerging distributed and decentralized workforce, those on the front lines are often the ones using mobile devices, and they may not be involved in the matters in dispute. Similarly, those in other roles may not be using these devices for relevant documents and communications. At least, not yet.

In sum, although considered in the past to be "outlier" sources of ESI, mobile devices are likely to become significantly more mainstream if current trends continue.

Gareth Evans

About the Author

Gareth Evans is a partner at Gibson Dunn. His practice focuses on complex litigation, including information technology, data privacy and e-discovery.