FTI CONSULTING | TECHNOLOGY

MOBILE DEVICES, DATA COLLECTION AND THE NEXT E-DISCOVERY FRONT

Mobile devices are impacting corporations profoundly in ways both obvious and subtle. As in-house counsel, IT staff and the security department grapple with bring your own device (BYOD) policies, security issues and the massive proliferation of data generated by mobile devices, they may not be focusing as closely on litigation and investigational risks caused by mobile device data. Potentially responsive discovery data—or data that may be necessary for internal and external investigations regarding HR matters, fraud, IP theft and more—that resides on smartphones, tablets and other devices isn't only hard to track, it can be extremely difficult to capture and preserve. As with most risks, playing catch-up once an incident occurs is a prescription for failure. Thinking proactively about these issues, on the other hand, will allow legal departments to take control and avoid trouble later on.

MOBILE DEVICE CHARACTERISTICS

Mobile devices of all types are proliferating. According to Pew Research Center, in 2014, 90% of American adults have a cell phone, 58% of American adults have a smartphone, 32% of American adults own an e-reader and 42% of American adults own a tablet computer.

This means that most employees are now walking around with the equivalent of a 1990s supercomputer in their pockets. The typical mobile device holds all types of important information, such as call logs, email, texts, GPS information, photos, video files, voicemail, Web browsing history, address books, search history and calendars. All of this data can be potentially responsive to an inquiry, whether it is for e-discovery purposes or a company investigation.

Mobile device data can also reside in multiple formats, many of which may be irretrievable from anywhere but the device itself. Compounding this is the fact that when using mobile devices, people are accustomed to being informal. Employees may tap out information, opinions and feelings from their phone that they would never consider writing in a corporate context—with many specifically choosing texting as a platform for sharing things they would not put in an email—as if a text message could never be uncovered and become evidence in an investigation or legal matter.

When combined, these unique characteristics come together to create an extremely volatile and important source of corporate data.

IMPLICATIONS FOR LITIGATION AND INVESTIGATIONS

Just like in the early days of email, vast sources of electronically stored information (ESI) on mobile devices are potentially being overlooked or ignored by litigators and investigators. Part of the reason is that much of the data is available only on the device itself and devices can be difficult to get and difficult to pull data from. Most email accounts and files can be pulled from enterprise servers, preventing much disruption (or sometimes even knowledge) of the worker. This is not true when employees must hand over their phones.

As such, legal teams may look the other way and not ask for their adversary's mobile information in the hopes that the adversary will not ask for theirs either. This is not sustainable, however. There is now abundant case law that makes it clear that mobile data is discoverable, and government agencies now expect mobile data to be produced as part of any investigation. Not to mention the fact that in matters with asymmetrical information, plaintiffs have every incentive to force opponents to go through the trouble of collecting mobile data.

Mobile Device Case Law

Civil courts have begun to notice device data and have begun to issue rulings and even sanctions regarding the duties that companies have to preserve and collect it. In *In Re Pradaxa (Dabigatron Exterilate) Prods. Liab. Litig.*, MDL No. 22385, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), the plaintiffs had specifically requested text messages as part of the e-discovery process. However, the defendants did not stop automatically deleting them once a litigation hold was issued. The defendants were fined nearly $1 million for failure to prevent text deletions on company-issued smart phones, among other things.

In another recent case, *Christou v. Beatport*, LLC, No. 10-CV-02912-RBJ-KMT, 2013 WL 248058 (D. Colo. Jan. 23, 2013), the defendant was ordered through a litigation hold to make a forensic image of his iPhone. He failed to do so, then later lost the phone. In response, the court granted the sanction that plaintiffs be permitted to introduce as evidence defendant's failure to preserve text messages.

If the urgency around the need to preserve mobile device data has been at all unclear, the recent ruling in *Small v. University Medical Center of Southern Nevada* should end any ambiguity. In this 600-plaintiff wage and hour class action, a court-appointed e-discovery Special Master, Daniel B. Garrie, recommended an order of default judgment against the defendant based on its handling of ESI in general and on mobile device data in particular.

While different types of ESI were lost, the Special Master in *Small* found the failure to preserve text messages and data from mobile devices particularly troubling. He identified two areas where the litigation hold was not instituted properly: company-issued BlackBerries and personal smartphones that employees used as part of a BYOD policy. By the time the litigation hold was instituted for the BlackBerries, more than 26,000 messages had been deleted. The defendant never issued a litigation hold for the BYOD smartphones, and more than two years' worth of data was lost.

"The level of intentional destruction of evidence by UMC shocks the conscience," Special Master Garrie wrote in the recommendation.

Mobile Device Investigations

Along with lawsuits, mobile device data can be relevant in internal and external investigations that may happen before or independent of a lawsuit. Ranging from human resources issues to intellectual property theft to fraud to Foreign Corrupt Practices Act matters, the evidence found on mobile devices in these investigations can be pivotal. For example, an employee stealing trade secrets might try to avoid detection by copying files for a competitor using a personal device; however an internal examination of the phone could yield the stolen files or even text messages providing evidence of the employee's intent.

CHALLENGES FOR LEGAL, IT AND SECURITY

BYOD and COPE

Company-issued devices that do not allow mixed professional and personal use are becoming increasingly rare, and more companies are implicitly or explicitly letting workers use their own smartphones and tablets for work. Gartner Inc. predicts that half of employers will require employees to supply their own device for work purposes by 2017.

For organizations, the drive towards BYOD is understandable, and in many cases, inevitable. Rather than imposing technology that employees don't want, a BYOD approach allows workers to use the device of their choice. BYOD also cuts costs and allows workers more flexibility in their work habits, including working remotely. Additionally many organizations mix BYOD with Company-Owned, Personally-Enabled (COPE) devices and policies, which can bring similar benefits.

However, BYOD and COPE policies also increase challenges. When workers use their personal devices for work purposes or work devices for personal purposes, companies should pay close attention to concerns around privacy, as well as issues co-mingling of personal and corporate data.

As the data on personal mobile devices can also be much more difficult to access during investigations and lawsuits, it is critical to have a policy in place that forces the employee to surrender—and allows the company to fully access—devices used for company business when necessary. Organizations should also think about what happens to enterprise data when employees leave and take their devices with them and any policy must include provision to allow that information to remain in the company's "possession, custody, or control," as described by Federal Rule of Civil Procedure 34. This is a crucial practice because when employees use their devices for business purpose, courts have generally been more willing to expect companies to preserve and produce information.

Challenges with Preservation and Collection

Whether BYOD or company-issued, mobile devices present challenges for data preservation and collection. For example, legal departments, working with outside counsel and other experts, must consider how to impose, enforce and document legal holds for mobile devices. In order to effectively implement holds, companies need to know who is using mobile devices, what devices they are using and how. It is also critical to communicate to employees when the data on their mobile devices is subject to a litigation hold and to suspend any regular deletion of text messages and mobile data (as evidenced in the *Pradaxa* case discussed above).

Collection of mobile device data represents another challenge. There are no solutions for enterprise-wide multi-device data collection at the present time. While Mobile Device Management (MDM) solutions allow enterprises to monitor and wipe devices, they are not able collect data for e-discovery or even investigatory purposes. (For example data from many texting and email apps is inaccessible.) To conduct a true collection requires the discovery team to put hands on the physical device every time. Collection is further complicated by the fact that BYOD users employ a wide range of devices that change and upgrade constantly. Devices can also use strikingly different operating systems and file types that store data in a variety of local and remote locations. With some of the newest devices, the technology doesn't even exist to "jail break" or open them to remove the data.

Cross-border investigations and lawsuits further complicate the matter. Physical distances can represent problems, as well as international privacy laws that restrict the type of information that companies can move outside jurisdictions, not to mention the question of where exactly data "resides" if it is on a mobile device.

STEPS TO PROACTIVELY MANAGE MOBILE DEVICE DATA

If companies haven't yet had to produce mobile device data in a lawsuit or investigation, they will, and probably soon. Rather than working defensively, organizations can prepare thoroughly enough to be ready—and perhaps even utilize the fact that they can handle mobile device data requests as a way to put pressure on adversaries. This involves having a strategy in place before it's necessary. The plan should explicitly address e-discovery collection strategies, as well as preservation and deletion plans in the event of a litigation hold. At minimum, the company should have a policy that allows it to gain access to employees' mobile devices and one that clarifies how to manage legal holds.

Organizations should also find trusted partners that have the sophistication, experience and knowledge to manage data on mobile devices, ideally before a lawsuit or investigation. Projects involving preservation and collection of data from mobile devices often provide little notice—it is best to have relationships in place before they are necessary

Companies should also consider how issues with internal and external investigations can differ from litigation. A small-scale internal investigation of finance people at headquarters might be easy to handle, with the targets expecting the legal team to access their device. On the other hand, a wide-ranging investigation—perhaps an (FCPA) investigation that involves the entire overseas sales force—can be much more complicated.

Policies around mobile device usage, particularly around BYOD, should be airtight. Employees need to understand their employer's expectations around usage and data on devices, particularly the question of access, remote wiping and the company's rights to demand the surrender of the device if necessary. Most employees have a heightened expectation of privacy for what they do on their mobile devices; it is critical to disavow them of the notion that work they do on their own device—or anything they do on a company-issued device—is private.

CONCLUSION

For many in-house counsel, IT and security professionals, the issues involved with mobile device data can seem overwhelming and hopelessly complex. However, ignoring mobile devices as a required source of e-discovery and investigative data is extremely risky, and waiting to react to the problem until after it happens could be costly. Instead, a proactive mobile device e-discovery and investigative strategy incorporating experienced partners inside and outside the company is crucial for organizations wishing to both protect themselves and gain insight into their own data sources.

ABOUT FTI TECHNOLOGY

FTI Technology helps clients manage the risk and complexity of e-discovery. We collaborate with clients to develop and implement defensible e-discovery strategies with keen focus on the productivity of document review. Our complete range of offerings, from forensic data collection to managed document review services, provides unprecedented flexibility to address and discovery challenge with confidence. Clients rely on our software, services and expertise to address matters ranging from internal investigations to large-scale litigation with global e-discovery requirements. For more information, please visit: **www.ftitechnology.com**.