ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM AUGUST 14, 2013

# Peering Into Personal Space: Investigating Employee-Owned Mobile Devices

***By Kimberly Peretti and Bruce Sarkisian***

With BYOD ("bring your own device") nearly a foregone conclusion in many organizations, one of the next puzzles to solve will be what happens when data on an employee-owned mobile device, or the mobile device itself, becomes the subject of an investigation. In these circumstances, companies must have the legal right to access both the device and the data it contains, as well as the forensic tools to extract and review the data.

## I. On the Legal Side

### Corporate Data on Mobile Devices Complicates Investigations

Employees of organizations that must comply with legal requirements such as PCI-DSS (Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability and Accountability Act of 1996) may find their devices subject to more scrutiny if the devices are compromised while storing regulated data. Indeed, any organization could find itself in trouble if it can't obtain emails and SMS messages or other data stored on an employee-owned mobile device when the information becomes subject to litigation holds and resulting discovery requests.

The solution might not be as simple as asking the employee for the device and providing a replacement while forensics is conducted. If there is no agreement between the employer and employee regarding the use of personal mobile devices for business purposes (including sending corporate communications and accessing corporate data), the company has lost a way to compel the employee to produce the device. Employee devices will likely have personal information, such as photos, music, contacts, emails, and text messages, that the employee does not want to lose even temporarily or want their employer to see.

### The Stored Communications Act and Personal Devices

The federal Stored Communications Act, 18 U.S.C. §2701 (SCA), and similar state statutes, may affect company access to personal devices. Under the SCA, a pre-condition for violating the statute is access to stored communications "without authorization" or if one "exceeds an authorization." The SCA's "without authorization" language in effect creates a consent exception. An effective user agreement, as described below, should provide the consent required to avoid running afoul of the SCA.

**Keys to Successful User Agreements**

Clear user agreements are essential if employees are going to access company data on personal devices. Successful user agreements should:

- clearly establish that an employee has no expectation of privacy in his mobile device if he accesses corporate data or engages in corporate communications from that device (otherwise, an employee can make a strong case for invasion of privacy if the employer accesses data on an employee-owned device and the employee can prove he had a reasonable expectation of privacy in the device);
- clearly disclose what the employer can do with an employee-owned mobile device if an investigation occurs; such a disclosure should be drafted so that the employer has the legal right to access both the device and the data on the device should potential evidence be stored there;
- inform or remind employees that participating in an employer program that allows use of employee-owned devices to access corporate data or send corporate communications is a privilege—not a right—and that an employee must agree to the program's terms if the employee wishes to participate in the program;
- include the employer's right to completely wipe the device of company data if the device is reported lost or does not connect to the company network after a defined period of time;
- require the employee to activate some security features on the device, such as a PIN code or password; and
- require the employee to produce the device (as well as any PINs or passwords to unlock the device) upon request, in the event of litigation or an investigation, at least for as long as is required to extract the relevant data from the device.

  (Note: Recent developments at the state and federal level regarding the monitoring of social media might be relevant here. Several states, including California, Delaware, Illinois, Maryland, Michigan, New Jersey and Washington, have enacted legislation prohibiting school officials and/or employers from requiring individuals to provide credentials (i.e., user name and password) to their social media accounts (e.g., Twitter or Facebook) in order for the school official or employer to access those accounts.

  At the federal level, lawmakers recently reintroduced a bipartisan proposal, the Social Networking Online Protection Act, which similarly prohibits employers and other third parties from requiring employees and potential employees to disclose their credentials for social media networks.

  While this state and federal legislation is narrowly aimed at privacy concerns related to social media accounts, it could signal a willingness of legislators to take a closer look at drawing firm boundaries with respect to personal data and personal accounts. Any attempt to restrict employers from requesting passwords or PINs to personal devices could present a challenge to conducting investigations.)

Just as important as any terms in the agreement is making sure the agreement is accessible to employees, not just buried in an employee handbook. A clear agreement will do an employer less good if employees could make a colorable claim that they did not know about the user agreement. On mobile devices, this problem could be solved by requiring employees to click a button on the device's screen to indicate their assent to the employer's user agreement before the employees are allowed to install software that will enable access to company data.

Equal Employment Opportunity Commission (EEOC) Chief Information Officer Kimberly Hancher emphasized the importance of clearly communicating terms of use when she was speaking in March 2013 at a Fordham Law School symposium on privacy and employment in the digital age. She indicated that the EEOC's employees were presented with a choice of giving up some privacy in exchange for the ability to carry sensitive data on their personal devices. Some employees chose to opt into the program, while others did not. "The rules of behavior were showstoppers," she said. "They were turnoffs for some, who said they were not going to volunteer to do bring your own device, but for others, they were no problem. Explaining the rules in plain language helped people really understand what the program is, what is involved and if they're OK with it or not."

**Potential Pitfalls When Accessing Personal Accounts on Personal Devices**

Because of the potentially intimate and sensitive nature of an employee's own data (e.g., text messages, photos, personal email), access to this data creates a somewhat heightened level of scrutiny even where policies and agreements attempt to abolish any privacy expectations. Indeed, case law has addressed whether employees have a heightened expectation of privacy in personal accounts such that monitoring or access could constitute tortious conduct, such as invasion of privacy or intrusion on seclusion. For example, in *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 928 (W.D.Wis. 2002), the court denied summary judgment in an invasion of privacy claim where an employee's personal Hotmail account was accessed, holding that "it is disputed whether accessing plaintiff's email account is highly offensive to a reasonable person and whether plaintiff's email account is a place that a reasonable person would consider private." Companies also should consider the effect that monitoring or accessing any personal email account or personal data on employee-owned devices may have on employee relations, even if such practices may be legally defensible.

One key to avoiding legal and employee-relation problems when investigating employee-owned mobile devices is to limit the scope of the investigation to what is absolutely necessary to satisfy legal requirements. The investigation should stop when the company has what it needs to answer discovery, produce the necessary files, or determine whether regulated data was accessed. The original cause of the investigation may not justify tearing the device apart and accessing the employee's own data.

## II. On the Forensics Side

**Current Limits of Mobile Device Forensics**

Even with the legal right to access the employee-owned device, companies still need to have capabilities that allow them to extract and review the data on the device. Unfortunately, mobile device forensics are not as developed as forensics for traditional enterprise computing tools.

For an investigation involving evidence stored on an employee-owned mobile device to hold up under legal scrutiny, the investigator must obtain an accurate, complete, and forensically sound image from a mobile device. It is estimated that less than 40 percent of the smartphone models on the market can be imaged. In fact, on Apple iOS, the security is proving so effective that bypassing the PIN or password may be a challenge for investigators. Thus, unless the employee can be compelled to provide the PIN or password, as discussed above, obtaining valuable or critical evidence from the device may be difficult. Android devices present their own forensics issues, because the software that performs the forensics must be programmed to work across an entire spectrum of Android device versions.

In litigation, when responding to ediscovery, it may be difficult to physically extract data involving files on a mobile device, such as deleted SMS messages and actual files and folders.

One way to ease the difficulty with forensics may be to limit the type of employee-owned mobile devices that are allowed to be used for corporate purposes. That way, only devices from which data may be reasonably extracted in the event of a forensic investigation will be allowed.

**Put Company Data in a "Container"**

Once a company has the capabilities necessary to access the data on employee-owned devices, the company must ensure that it does not access too much data—especially personal data—for the reasons outlined above. Many mobile device management (MDM) programs on the market today can separate company data on a mobile device from personal data on the device by putting the corporate data in a "container." This feature has several advantages:

- If the device is lost or stolen, the company can wipe its data from the device while leaving the employee's own data intact in case the device is ever recovered.
- The company can put an additional layer of security on its data while not affecting the employee's data on the device.
- The container should be designed to ensure that the company can see and affect only its own data on the employee's device, while the employee's data remains untouched. (The "containerized" structure could help shield the company from claims that the company improperly "accessed" an employee's personal accounts in violation of the SCA. For example, in *Shefts v. Petrakis* 1:10-cv-01104-JBM-BGC # 249 (order on issue of defendant's authority to access plaintiff's company email), the court found that the defendant could not be held to have "accessed" text messages that it never saw, even though it had the ability to see such messages. Thus, a company using the container structure could reasonably argue that it only "accessed" the company data in the container, and was not interested in the employee's data outside of the container, though it might have had the ability to see the employee's data as well.)

## Conclusion

While the law has yet to be fully formed in the area of access to and investigation of employee-owned devices, a set of basic ground rules can help companies navigate the law as it develops. Companies can minimize legal missteps and tension in relationships with employees by: (1) setting clear expectations regarding the access to a device that an employee must allow in exchange for the ability and convenience of viewing company data on that device, (2) separating company data from the employee's own data where possible, and (3) setting limits on how far an investigation can go.

*This article was originally published in the Summer 2013 Edition of* The SciTech Lawyer.

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Bruce Sarkisian| 404.881.4935 | bruce.sarkisian@alston.com