Smarter Phones, Bigger Risk

White Collar

Smartphones are a universal fact of life in business today, where they help companies increase speed and productivity. But when it comes to potential white collar investigations and litigation, they are raising some difficult questions about preserving and accessing data.

Smartphones have not only proliferated in recent years, they've also become more sophisticated, expanded to encompass a broader range of functions, and added increasingly powerful security, including password protection, biometric access control, and data encryption. And they've become deeply interwoven in people's lives. As a result, "many companies have a 'bring your own device' culture, allowing people to use their own phones for business purposes," says Glen McGorty, a Crowell & Moring partner and a former federal prosecutor in the U.S. Attorney's Office for the Southern District of New York and the Department of Justice in Washington, D.C.

When it comes to accessing data in order to respond to a subpoena, smartphones represent a fundamental change from the past. Decades ago, business records were kept in company file cabinets. Since then, business data has steadily moved to new platforms—mainframes, personal computers, company servers, the cloud. But throughout that evolution, data has still remained under the company's control and been relatively easy for the company to access.

With smartphones, on the other hand, data is often held on the device, not merely on the server to which it has access, and that device, which contains both personal and business information, is not under the company's direct control. "The medium has changed, but the company's obligation to be able to look through and provide data for investigations and litigation has not—even if the phones are not owned by the company," says McGorty. "And the phone can be a much harder 'file cabinet' to search than computers and servers."

For example, McGorty continues, "search warrants cannot compel an owner to provide a password in light of Fifth Amendment protections, and even the government has a hard time collecting material from smart devices." That point was underscored in 2016, when the FBI tried to compel Apple to create software to unlock an iPhone belonging to one of the attackers in the San Bernardino, California, terrorist shootings. Apple refused and the case went to court. However, the day before the trial, the FBI announced that it had found a third party that could unlock the phone without deleting its data.

To avoid such problems—and potential litigation and compliance issues—companies need to have rigorous policies that clearly address the question. "They need to carefully establish how their data will be stored and how it will be accessible," says McGorty. "Make it clear that by consenting to the use of their own personal devices for business, employees can't deny an employer access to the business-related data on that phone if the company needs it. And make sure employees are aware of that and sign off on it." At the same time, he says, companies need to make sure that they have a process in place that lets them easily capture and retrieve data from phones if that becomes necessary. "If you're not doing those things up front and it all comes to a head in an investigation," he says, "the government may well decide that you aren't properly preserving data."

Ephemeral Messages Create Concrete Problems

In addition to managing physical access to smartphones, companies need to think about the growing range of apps running on those devices—in particular, ephemeral messaging apps such as SnapChat, Wicker, and Confide. These typically let

"The medium has changed, but the company's obligation to be able to look through and provide data for investigations and litigation has not." **Glen McGorty**

users send encrypted messages that then self-destruct after they are read. This naturally disrupts the preservation of business-related messages.

The use of ephemeral messaging in business has been increasing over the years. In 2017, the DOJ responded by adjusting its Foreign Corrupt Practices Act enforcement policy to require companies seeking cooperation credit in government FCPA investigations to prohibit their employees from using "software that generates but does not appropriately retain business records or communications."

However, the DOJ changed that policy in March 2019—perhaps in recognition of the widespread use of ephemeral communications in business. Now, instead of prohibiting such apps, the DOJ requires companies to implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

That change provides some flexibility in using ephemeral messaging, but it also introduces new complications. By including the term "personal messaging," the DOJ has made it clear that it is interested in other types of messaging apps, such as WhatsApp, that are not ephemeral in nature. These apps are frequently used outside of company IT systems, and employees often use them on multiple devices, such as tablets and home computers—all of which could make it difficult to track data down. And companies still need to preserve business records from both ephemeral and personal messaging apps. Doing so will not only require costly tools and complex rules, but it will also introduce the possibility of inadvertently accessing employees' personal information.

With that in mind, companies may decide that it's easier to simply prohibit employees from using personal and ephemeral communications. But that can bring challenges in its own right. For example, monitoring usage to enforce the prohibition is likely to be intrusive and could lead to data-privacy issues. A blanket prohibition would also mean that employees are unable to access tools that are increasingly important in business.

Here again, putting the right policies in place will be key. "You need to explicitly spell out how information will be preserved and how you'll govern these types of communications, and absolutely dictate the circumstances where you believe that it's appropriate to permit the use of this sort of communications," says McGorty. "The more specific and articulate you are, the better.

"Under DOJ guidance, you really need to be able to articulate how and why you're using these apps—the real business reasons," he continues. Often, there are good reasons for doing so, such as the immediacy of the communication, an improved ability to do business in industries and regions where these apps are widely used, and, of course, security. "Certainly, the less data that's out there, the less likely you are to have data stolen," he says.

However, by asking businesses to explain their reasons for using these apps, the DOJ guidance is opening the door to more litigation. "Companies will be coming up with arguments rationalizing why they are using these communications for business purposes," McGorty says. "So by removing the absolute prohibition against ephemeral communication, they're creating a window for subjective interpretations—and it's very likely that litigation will be arising from that."

The Growing Reach of RICO

When Congress passed the Racketeer Influenced and Corrupt Organizations Act in 1970, it became a well-known tool for fighting organized crime. "But the law also allowed civil remedies, and a growing number of plaintiffs have been using RICO to move fairly ordinary business disputes into federal courts," says Crowell & Moring's Glen McGorty.

In recent years, companies in the pharmaceutical, social media, automotive, entertainment, medical marijuana, and finance industries have been the focus of private RICO lawsuits. In general, these claim that a company or class has been wronged by the alleged corrupt actions of a company, and that those actions are part of running a criminal enterprise.

RICO cases can be hard for a private plaintiff to win. But many are motivated by the possibility of winning treble damages and attorneys' fees under the law, and they are likely to keep looking for new ways to use the RICO statute. As a result, says McGorty, "general counsel should keep an eye on this trend, factor it into their risk assessments, and consider whether to implement a RICO compliance program."