Published on *The National Law Review* https://natlawreview.com

Can the Government Unlock my Cell Phone? Companies' Heightened Security Features to Protect Customer Privacy Affects DOJ Investigations

Article By:

David A. Frazee

Kathleen L. Matsoukas

As the numbers of highly publicized data breaches have become more prevalent, companies continue to find new ways to secure private customer information. However, as companies become more successful at protecting their customers and reducing their own liability, the government's ability to extract information on targets of criminal investigations has become more difficult. This tension between personal privacy and the federal government's desire and ability to access private data during investigations through search warrants has now reached the federal courts.

During the execution of a search warrant on Jun Feng's (Feng) residence, the government seized a password-locked Apple iPhone 5. *See In re Order requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* Cause No. 1:15-mc-01902-JO, Dkt # 1 & 15 (EDNY, Oct. 8, 2015). However, as the government recognized, compelling the target of a federal investigation to disclose the passcode "raises significant Fifth Amendment issues[.]" Even if Feng knew the passcode, it could be considered testimonial evidence that could incriminate Feng, potentially in violation of his Fifth Amendment protections. *See, e.g.*, *Virginia v. Baust*, 2014 WL 6709960, at *3 (Va. Cir. Ct. 2014) ("[C]ompelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected[.]")

Unable to bypass the locked screen without damaging the data, the government sought to compel Apple, Inc.'s assistance under the All Writs Act, 28 U.S.C. § 1651. In its response, Apple challenged the request in part as "substantially burdensome" because, "[i]n most cases now and in the future[,] . . . it would be impossible" for Apple to access the data on a password-locked device. *In re Order requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* Cause No. 1:15-mc-01902-JO, Dkt. #11 (EDNY, Oct. 19, 2015). Apple noted that it has implemented a security feature on its iOS 8 and higher operating systems that "prevents *anyone* without the device's passcode[, including Apple,] from accessing the encrypted data." (Emphasis added). The security feature implemented by Apple "helps protect users from attackers if Apple's servers are compromised or if the user no longer has physical possession of his or her device."

Arguments largely centered on whether the All Writs Act provided the government sufficient authority

to compel Apple to extract encrypted data from a locked iPhone. *In re Order requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* Cause No. 1:15-mc-01902-JO, Dkt. #16 EDNY, Oct. 23, 2015). The All Writs Act is a gap-filler. However, it is not a "catchall" intended to fill gaps Congress intentionally left open. *Id.* Apple argued that Congress carved out an exception for "information services" providers, which includes Apple, from providing such assistance under the Communications Assistance for Law Enforcement Act (CALEA). However, the government argued that the CALEA did not "specifically address" its request. *In re Order requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by this Court,* Cause No. 1:15-mc-01902-JO, Dkt. #15 EDNY, Oct. 22, 2015). According to the government, the CALEA applies to court orders for "real-time interceptions and call-identifying information," not "data already stored on a cell phone." *Id.* Therefore, the exception Apple claimed was not applicable to this case. *Id.*

Before the court could decide whether Apple was required to assist the government, Feng pled guilty. Therefore, no definitive answer on the issue was provided. With technology constantly evolving and data breaches still occurring, this tension between privacy and security is not likely to disappear.

It is brief, Apple had also argued that forcing it to extract data, "absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand." *Id.* In 2015, in response to these types of issues, Congress attempted to address tech companies' concerns in the highly debated Cybersecurity Information Sharing Act (CISA). Other companies, such as Google, Yahoo, Facebook, T-Mobile, and the Computer and Communications Industry Association (CCIA), which is a trade group that represents major tech firms, came out against the CISA in October 2015, at the same time Apple was debating the matter in court. However, on Dec. 20, 2015, CISA was passed and signed into law as part of the budget bill.

The cybersecurity section of the bill seeks in part to absolve companies from liability when they share customer data with the government. But establishing legal authority to share with the government is only half the battle.

In order to access the information the government desires, companies may need to leave a "back door" into its devices. However, "[i]t's impossible to build a back-door for just the good guys[,]" Representative Jason Chaffetz, chairman of the Government Oversight and Reform Committee, said and the Washington Post reported. Indeed, Apple's CEO Tim Cook has stated that creating a back door is not an option. "No one should have to decide between privacy or security. We should be smart enough to do both[,]" Cook said.

Intentionally not taking the necessary steps to fully protect customer data is a slippery slope that could still leave companies vulnerable to lawsuits. How this will play out under the new cybersecurity law is unknown, but we will closely monitor further developments in this area.

National Law Review, Volume VI, Number 32