Considerations from California: Relevant Themes from a Lawsuit over a Terrorist's iPhone

by Liz Dillon

The long-standing debate over whether private companies must aid governmental efforts to access secured data recently culminated in a short-lived lawsuit between the Federal Government and Apple, Inc. (Apple). The lawsuit centered on whether Apple should assist the FBI in obtaining data from San Bernardino shooter Syed Farook Rizwan's iPhone. Although the lawsuit quickly caught the public's attention, it unfortunately did not resolve the debate, as, on March 28, 2016, the Federal Government moved the Court to vacate its earlier order compelling Apple to assist the FBI, effectively ending the case.

The lawsuit between Apple and the Government centered on the following key issues: (1) the public's (often conflicting) concerns over data security; (2) the future of governmental efforts to compel private companies to aid in accessing data; (3) the potential for legislation to resolve the dispute over data security; and (4) the potential economic effect of the changing legal landscape surrounding these issues. Although the lawsuit has ended, these issues will continue to resurface in the ongoing debate over data security, and should be considered by corporate attorneys.

A Terrible Tragedy in California.

On Dec. 2, 2015, 28-year-old Farook and his 27-year-old wife, Tashfeen Malik, shot and killed 14 people (and seriously injured 22 others) during a holiday party and training session at Inland Regional Center in San Bernardino, CA. Of the 14 dead, 12 were Farook's co-workers at the County Health Department. The incident appears to have been both a mass shooting by a disgruntled employee against his co-workers and a vicious attack motivated by terrorist ideologies. The shooting has been called the deadliest terrorist attack on U.S. soil since Sept.11, 2001.

After the attack, Farook and Malik fled in a rented black Lexus SUV, but fortunately were intercepted by police. During a subsequent shoot-out, Farook and Malik were killed. While searching the getaway car, the police discovered an iPhone issued to Farook by his employer. It is the data on this iPhone that led to the lawsuit between the Government and Apple.

A Short-Lived Lawsuit Over a Terrorist's iPhone.

Despite having obtained a warrant to search Farook's iPhone, the Government initially was unable to access the data on the password-protected phone. The Government was unable to "brute force" its way into Farook's iPhone (i.e. by repeatedly guessing random passwords) due to three Apple-implemented security measures featured on the phone: (1) a requirement that passwords be manually-entered (i.e. not entered by a computer program); (2) the increasing delay, after each incorrect password entry attempt, before another attempt could be made; and (3) an optional feature, which may or may not have been activated on Farook's iPhone, which deletes <u>all</u> data on the phone after ten incorrect password-entry attempts.

The Government moved the Court to compel Apple to develop and load an operating system onto Farook's iPhone to bypass these security measures. While the Court initially granted the motion, the Government was able to obtain the data without Apple's assistance, and the litigation concluded less than two months after it began. Although the lawsuit now is over, its four key themes remain worthy of consideration by corporate lawyers.

Americans Hold Conflicting Concerns Over Data Security.

The first key theme is that Americans hold conflicting concerns about the security of data contained on their smart phones and other devices.

The Government focused largely on the public's concerns about data security, as it relates to terrorism. Specifically, the Government argued that if private companies like Apple did not help bypass security measures like those found on Farook's iPhone, the Government could be unable to access data essential to preventing future terrorist attacks like the one in San Bernardino.

For its part, Apple also focused on the public's concern over data security and terrorism, but reached a wholly different conclusion. While the Government argued that the order compelling Apple to assist the FBI could prevent future terrorist acts, Apple argued the order would actually have the opposite effect. Specifically, Apple argued that the "back door" code into the iPhone contemplated by the order could be stolen and/or exploited by identity thieves, cybercriminals, oppressive foreign governments, and even terrorists. Further, Apple argued that increasing governmental access to data could lead to governmental surveillance of the wealth of personal information that most Americans keep on their smart phones, including information relating to their health, finances, businesses, and families.

The Court did not ultimately determine which of these concerns should take precedence. As the debate surrounding data security continues, lawyers should consider and advise their clients as to these various security concerns.

Lawsuits Between the Government and Private Companies Over Data Security Will Continue.

The second theme worthy of consideration is the ongoing state of litigation regarding data security.

As noted by the parties, the Government has previously requested, and will continue requesting, the assistance of private corporations in accessing data. Where companies like Apple have not complied with such requests, the Government has moved to compel such assistance, and will likely continue doing so.

Corporate attorneys should be aware that their corporate clients who refuse governmental requests for access to secured data may face costly litigation.

The Legislature May Ultimately Resolve the Dispute Over Data Security.

The third theme worthy of consideration is the potential for legislation to resolve the ongoing debate over data security.

Apple argued that any requirement for private corporations to assist the Government in obtaining secured data must come from the Legislature, not the courts. Apple criticized the Government for bringing the lawsuit in what Apple sees as an attempt to bypass the Legislature. The Government agreed that Congress could resolve the debate, but maintains that Courts also have the authority to do so.

Congress, for its part, already has begun taking action. For example, House Homeland Security Committee Chairman Michael McCaul and Senate Intelligence Committee member Mark Warner introduced a bill creating a National Commission on Security and Technology Challenges to advise Congress on Americans' conflicting concerns over data security.

Attorneys representing corporations should be aware of, and advise their clients about legislative efforts to resolve disputes between the Government and private corporations over data security.

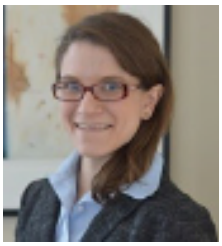
Any Resolution to the Debate over Data Security May Significantly Impact Corporations.

The fourth theme worthy of consideration is the potential economic impact of Governmental requests for assistance in accessing data. As Apple noted, repeated governmental requests for assistance may require companies like Apple to divert key personnel to write and test software code any time the Government requests, or a court orders, such assistance.

It is unclear whether the economic burden on private corporations will be as significant as Apple portends, and Apple never actually had to assist the Government access Farook's data. Corporate attorneys should, however, advise their clients as to the potential economic impact of requests for assistance in obtaining secured data, particularly where requests may be numerous.

Conclusion.

Although the lawsuit between Apple and the Government over Farook's iPhone has concluded, the four key themes on which the lawsuit centered remain relevant for corporate attorneys. Attorneys should pay particular attention to the ongoing debate over data security, potential efforts by courts and the Legislature to resolve this debate, and the potential economic impact on corporations of any such resolution. ■



Elizabeth Dillon is an attorney at Cetrulo LLP. Her practice focuses on employment advice and counseling, as well as employment, business, real estate and probate litigation.