1919 SOCIALLY RESPONSIVE INVESTING INVESTMENT COUNSEL

SOCIAL RESEARCH REPORTER

Commentary from our Social Research Analysts

ISSUE 3, 2016

Digital Privacy: Where Do We Draw the Line?

The high-profile legal battle between Apple and the FBI seems to be over, at least for now. The case, in which Apple was resisting a judge's order to help the FBI unlock the iPhone used by Syed Farook, one of the shooters in the San Bernardino terror attack, raised a number of important questions about privacy and security. In the end, the FBI dropped its case against Apple, after a third party came forward and helped it access the data on the iPhone. Unfortunately, this has only raised more questions and has left many of them unanswered. However, as companies like Apple continue to bolster the security of their products, questions about the roles that companies play in protecting individual privacy and how that is balanced with the needs of law enforcement will persist.

Apple has consistently increased the security of its products through the use of encryption and other features and touts that as an advantage to its customers. In a world in which smartphones have become an important part of our everyday lives, strong security is a must. We store an enormous amount of personal information on these devices and we rely on companies like Apple to protect it. However, problems arise when law enforcement wants to access the data on a device as part of a criminal or terrorist investigation, but cannot because of the security protections. This is what happened in the San Bernardino case. The data on Farook's iPhone was encrypted and there was no way for anybody to access it, not even Apple. The FBI obtained a court order requiring Apple to create a unique version of its iPhone operating system that would disable the security features.

Apple objected. Tim Cook, the company's CEO, published an open letter explaining the company's position on its website. In it he wrote "Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have and something that we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."[1]

The FBI's request in this case had broad implications and would have set a legal precedent. Not only did it have the potential to impact the privacy and security of all of Apple's customers worldwide, but it also would have opened the door for similar requests aimed at other technology providers and connected devices. If Apple had conceded, how would it or any other company refuse these requests in the future? Other state and local authorities indicated that if the government prevailed, they would ask to open hundreds of other seized devices in cases having nothing to do with terrorism. Multinational companies such as Apple are subject to the laws of other countries. A ruling in the U.S. government's favor might have encouraged other countries to make similar, perhaps even more extensive demands for access.

Further, if the courts can compel a company to create a new product to assist a government investigation, what's next? Could the government order a company to build and release a software update that includes surveillance capabilities? Where would we draw the line? What would it mean for digital privacy going forward?

The emotional nature of this case and its potential impacts has invoked many strong and differing opinions. The FBI's request seems simple and reasonable: the iPhone is evidence in a domestic terrorism investigation and it could contain information that would be helpful. The FBI request was limited to this one iPhone and Apple could unlock the iPhone in its own facilities and not provide any information on how it was done to the FBI. Doesn't a company have a legal obligation to do everything possible? What if there is information on that iPhone related to other terror plots? Shouldn't the FBI have that information in order to protect Americans and thwart another attack?

This case is an example of the ongoing dispute between law enforcement and technology companies and the challenges they face. The operating system that Apple was asked to create is a tool that would defeat its encryption. Once created, anyone with knowledge of this tool could use it to hack into millions of other Apple devices. While any company would do its best to guard this tool, it could fall into the wrong hands. Its existence would weaken the security protections that Apple has in place and make all of its customers more vulnerable to invasions of privacy from governments, hackers, and thieves. If a company could be forced to alter its products at the direction of law enforcement, it would erode public trust in new technologies and connected devices and the companies that provide them. Many companies, including Apple, have policies in place to address government requests for customer information in a criminal or terrorist investigation. Apple states that it complies with valid subpoenas and search warrants, as it did in this case, but argued that this order went beyond the authority of the All Writs Act, the law that the government was relying on to compel the company's cooperation. The All Writs Act, passed more than 200 years ago and 50 years before the

telegraph was invented, gives federal judges the power to enforce existing laws. Its successful use in this case would have given federal courts new authority.

IS THE FBI "GOING DARK"?

The FBI has a "going dark" problem. "Going dark" refers to law enforcement's inability to obtain the evidence needed to prosecute crime and prevent terrorism, even with lawful authority, due to the widespread availability of advanced encryption and other security technologies in everyday consumer products. With the use of encryption it is not technologically possible to create a secure way to give law enforcement special access to those communications without compromising the protection that encryption provides.

U.S. technology companies are regularly boosting their encryption and expanding it to new areas of customer communication. For example, WhatsApp, which uses end-to-end encryption in its mobile messaging service and has one billion users worldwide, recently announced it would offer users encrypted voice calls and group messages.

While the use of encryption presents a challenge for law enforcement, some groups argue that it is not as detrimental as portrayed. Banning or weakening encryption could actually hurt good, law-abiding citizens more than criminals or terrorists, who would simply switch to encrypted applications written outside of the U.S. and thus beyond the reach of the government. Below are a few reasons why the FBI's "going dark" claims may be overstated.

- End-to-end encryption is not going to be universally adopted by companies because many businesses that provide communication services rely on access to user data to generate revenues and provide functionality.
- Metadata – information about communications, such as who is calling whom, how often and when – is not encrypted and the vast majority is likely to remain that way because it is necessary for the systems to operate. This information provides an enormous amount of surveillance data that was not available before these systems became widespread.
- Networked sensors and the Internet of Things are growing substantially and could offer new opportunities for surveillance.

Apple does not stand alone; there has been an outpouring of support for the company and its position from a number of different groups including other companies in the technology industry, civil society organizations, academics, and security experts. Jack Dorsey, CEO of Twitter, tweeted "We stand with @tim_cook and Apple (and thank him for his leadership)!"[2] Google CEO Sunday Pichai tweeted, "Important post by @tim_cook. Forcing companies to enable hacking could compromise users' safety."[3] Many of these groups filed legal briefs in support of Apple. In one filed by Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest Labs, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo, the companies acknowledge that while they are often fierce competitors, they "are also united in their view that the government's order to Apple exceeds the bounds of existing law and when applied more broadly will harm Americans' security in the long run."[4] Microsoft wrote in a blog post that "the issues raised by the Apple case are too important to rely on a narrow statute from a different technological era to fill the Government's perceived gap in current law."[5] In its own blog post, the American Civil Liberties Union (ACLU) wrote that "the power the government aims to establish here would set a troubling and dangerous precedent that would undermine everyone's digital privacy and security."[6] Privacy International and Human Rights Watch filed a brief in which they draw attention to the human rights implications of this case, stating that in societies governed by repressive regimes, "secure technologies protect all members of society but especially vulnerable ones – such as journalists, human rights defenders, and political activists – by giving them a safe space to communicate, research, and organize."[7] The U.N. High Commissioner for Human Rights, Zeid Ra'ad Al Hussein, spoke out in Apple's defense saying, "It is potentially a gift to authoritarian regimes, as well as to criminal hackers. Encryption and anonymity are needed as enablers of both freedom of expression and opinion, and the right to privacy. Without encryption tools, lives may be endangered."[8]

It is easy to see why this case has been controversial and why, as citizens, we should care about it. As investors, we also need to be concerned about these issues. While Apple maintained that whatever the court decided, it would comply, a ruling in favor of the government could have done serious damage to the security of Apple's products thereby harming the company's worldwide reputation and costing it large amounts of revenue. That doesn't even consider the impacts to the company if the tool were to fall into the wrong hands. The lawsuit may be over, but the questions it raised about individual privacy and data security and how that can be balanced with law enforcement's goals to protect national security and the American people have not been resolved. Perhaps we need to take this opportunity to engage in a public discussion about the implications of technology for law enforcement, national security, and privacy and to push for legislation that outlines clear boundaries for both the government and the private sector.

[1] Cook, Tim. "A Message to Our Customers." Letter. 16 Feb. 2016. Apple Inc, 16 Feb. 2016. Web. 25 Feb. 2016.
[2] Dorsey, Jack (jack). "We stand with @tim_cook and Apple (and thank him for his leadership)! apple.com/customer-letter." 18 Feb. 2016, 3:09 PM. Tweet.
[3] Pichai, Sundar (sundarpichai). "1/5 Important post by @tim_cook. Forcing companies to enable hacking could compromise users' privacy." 17 Feb. 2016, 6:47 PM. Tweet.
[4] Maddigan, Michael and Neal Kumar Katyal. "Brief of Amici Curiae Amazon.com, et. al." Hogan Lovells US LLP. 2 Mar. 2016. Web. 4 Apr. 2016. PDF.
[5] Smith, Brad. "Our legal brief in support of Apple." Web blog post. *Microsoft On the Issues.* Microsoft, 3 Mar. 2016. Web. 24 Mar. 2016.
[6] Sweren-Becker, Eliza. "Why We're Defending Apple." Web blog post. *Speak Freely.* American Civil Liberties Union, 2 Mar. 2016. Web. 4 Apr. 2016.
[7] Scarlet, Kim and Caroline Wilson Palow. "Brief of Amici Curiae Privacy International and Human Rights Watch." 3 Mar. 2016. Web. 4 Apr. 2016. PDF.
[8] "UN Human Rights Chief Backs Apple in FBI Encryption Row." BBC, 4 Mar. 2016. Web. 7 Mar. 2016.