4-9-2016

Terrorism Versus the Right to Privacy: Apple Takes on the DOJ

Anastasia Dolph
Cardozo Arts & Entertainment Law Journal

Terrorism Versus the Right to Privacy: Apple Takes on the DOJ

By ANASTASIA DOLPH / ON APRIL 9, 2016

The long-simmering struggle between two essential American interests came to a dramatic head this week when Apple indicated its intent to appeal a court order directing the company to unlock an iPhone used by Syed Rizwan Farook, one of the San Bernardino terrorists. The case brought to light the enduring and intense battle between privacy rights and national security. For over a decade, Americans have grappled with how to prevent acts of terrorism on American soil without contravening our highly valued right to privacy.

Post-9/11, the Patriot Act triggered the erosion of Americans' civil liberties in the name of protecting our country from terrorism.[1] For a detailed look at the history of the Patriot Act see the New York Times summary. While there was certainly some uproar from civil liberties groups, for the most part, the Patriot Act operated quietly in the background. It wasn't until 2013, when NSA whistleblower Edward Snowden released classified documents revealing the extent of U.S. governmental surveillance, that the struggle between privacy and national security was propelled into the forefront of the American consciousness.[2]

The struggle between keeping America safe from terrorism and safeguarding our civil liberties is inescapably complex and has garnered a wide range of reactions. The current dispute between U.S. law enforcement and Apple is an embodiment of this dichotomy, and due to the brutality of the attack, is perhaps the perfect test case for the American government to advance their position.

This is not the first time that Apple and the U.S. government have disagreed about the proper balance between security and privacy. The issue made headlines last year when the Obama administration and Apple clashed over providing Americans with access to encryption technology for their devices.[3],[4] Coverage of that skirmish died down, however, because the debate was largely theoretical.

What differentiates the current case is twofold. First, rather than weighing a hypothetical threat against a hypothetical invasion of privacy, the San Bernardino case replaces that hypothetical threat with a real, brutal attack on the homeland. After the San Bernardino attack, American citizens are no longer contemplating remote probabilities. Second, an actual legal proceeding has been commenced in federal court, meaning that at its conclusion a binding decision will be rendered. That decision will undoubtedly have significant legal ramifications going forward.

Following the San Bernardino attack, which left fourteen people dead and twenty-two seriously injured, investigators discovered an iPhone 5c that had been used by Syed Rizwan Farook.[5] The FBI obtained a warrant to search the phone, which is owned by Farook's former employer, the San Bernardino County Department of Public Health.[6]The problem, according to the FBI, is that they have been unable to unlock the phone. An optional security feature on iPhones, if activated by the user, permanently deletes all data after ten failed attempts to enter the passcode.[7] Farook had activated this security feature. When Apple refused to assist investigators in unlocking the phone, the DOJ filed for a court order to compel Apple's assistance. The DOJ maintains that the iPhone may provide critical information about the attackers' motives and whom they communicated with in the months leading up to the attack.

Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California issued an order compelling Apple to provide "reasonable technical assistance" to the FBI.[8] Judge Pym specified that Apple should provide the requisite assistance to allow the FBI to "bypass or erase the auto-erase function."[9] Both sides have made compelling arguments in response.

Apple CEO Tim Cook issued a statement vowing to appeal the order, adding that the government's request constituted a "chilling" breach of privacy that would create a dangerous precedent.[10] According to Cook, the government is compelling Apple to "hack [their] own users and undermine decades of security advancements that protect [their] customers."[11] Apple contends that it does not currently have the technical ability to bypass the security feature, and therefore, the only way Apple can comply with the order and assist the FBI is by creating an entirely new version of iOS. According to Cook, doing so would effectively create a backdoor and allow any iPhone in someone's physical possession to be unlocked.[12] In his statement, Cook emphasized that customers store sensitive private data on their iPhones, including financial information and details about their health.[13] He also highlighted the serious privacy threat to iPhone users if this backdoor ends up in the hands of criminals and hackers.[14] Cook contests the FBI's claim that the technology would only be used in this case, arguing that there is no real way to control the technology once it is created.[15] While Cook acknowledged the importance of national security and said Apple has been cooperative by providing the FBI with information in its possession, he refused to create a backdoor to iPhones that doesn't already exist.[16]

Following Cook's response, the DOJ filed another motion in the U.S. District Court for the Central District of California.[17] The most recent motion lays out the Justice Department's reasons for compelling Apple's assistance and refutes some of the claims Cook made in his open letter to customers. The DOJ maintains that Apple does in fact have the "technical ability" to assist the government's investigation, as ordered by Magistrate Judge Pym.[18] The motion goes on to suggest that Apple's purported motive for resisting the order is disingenuous, claiming that its real motivation is "concern for its business model and public brand marketing strategy."[19] Further, according to the motion, the government has reason

to believe that Farook used the iPhone to communicate with victims prior to the attack–information that is crucial to the FBI's investigation.

So what are the possible outcomes? Apple could appeal the court order all the way up to the Supreme Court. However, whether Apple complies with the judge's order or continues to appeal, in the end, a legally binding decision will be rendered. That decision will shape interactions between technology companies and law enforcement going forward. If the DOJ is successful, the legal reasoning employed to compel Apple's cooperation will be applicable to other technology companies in the future. Another potential outcome is that Congress will step in and pass a law that seeks to strike a balance between the two seemingly irreconcilable interests. This law could contain criteria stipulating when a company can be forced to cooperate with law enforcement. Factors that could be considered are the imminence of a threat, severity of the crime perpetrated by the device's user and the likelihood that the device contains actionable evidence. Either way, Cook is correct in his assertion that the outcome will set a significant precedent.

For now, a hearing on the current case has been scheduled for 4:00 PM on March 22, 2106, in the U.S. District Court for the Central District of California.

**UPDATE: The hearing has since been canceled by the FBI, as they were able to hack into the iPhone without Apple's help on March 28, 2016. However, the FBI now has issues with a newer iPhone 5s which they are unable to hack into. The iPhone belongs to Jun Feng, a dealer in a New York drug case. This time around, a magistrate judge ruled that Apple did not have to provide assistance—the FBI appealed the ruling. A hearing is scheduled with Judge Margo Brodie.[20]

Anastasia Dolph is a second-year student at Benjamin N. Cardozo School of Law and a Staff Editor of the Cardozo Arts & Entertainment Law Journal. She is interested in criminal justice and hopes to pursue a career in public service.

[1] Adam Liptak, *Civil Liberties Today*, New York Times (Sept. 7, 2011), http://www.nytimes.com/2011/09/07/us/sept-11-reckoning/civil.html?_r=0.

[2] Matt Sledge, *The Snowden Effect: 8 Things That Happened Only Because of the NSA Leaks*, Huffington Post (June 5, 2014), http://www.huffingtonpost.com/2014/06/05/edward-snowden-nsa-effect_n_5447431.html.

[3] Matthew Panzarino, *Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy*, TechCrunch (June 2, 2015), http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/.

[4] Alex Wilhelm, *U.S. Secretary of Homeland Security Warns About the Dangers of Pervasive Encryption*, TechCrunch (Apr. 21, 2015), http://techcrunch.com/2015/04/21/just-let-us-encrypt-our-fucking-phones-bc-the-nsa-can-probably-read-our-messages-anyways/#.adrkgr:Bm2g.

[5] Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, New York Times (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] Tim Cook, *A Message to Our Customers*, Apple (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[xvii] Alina Selyukh, *DOJ Lays Out Its Legal Case For Why Apple Should Help Crack An iPhone*, NRP (Feb. 19, 2016), http://www.npr.org/sections/thetwo-way/2016/02/19/467385553/doj-lays-out-its-legal-case-for-why-apple-should-help-crack-an-iphone?utm_source=npr_newsletter&utm_medium=email&utm_content=20160220&utm_campaign=news&utm_term=nprnews.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Susie Ochs, *The Government Still Needs Apple's Help to Crack a Locked iPhone 5s in New York*, Macworld (Apr. 8, 2016, 10:56 AM), http://www.macworld.com/article/3053962/ios/the-government-still-needs-apples-help-to-crack-a-locked-iphone-5s-in-new-york.html.