The University of Cincinnati Intellectual Property and Computer Law Journal

Volume 1 | Issue 1 Article 5

2016

National Security or Consumer Privacy? A Question Even Siri Couldn't Answer

Rebecca Knight

Contributing Member for IPCLJ (2015-2016), University of Cincinnati College of Law, knightra@mail.uc.edu

National Security or Consumer Privacy? A Question Even Siri Couldn't Answer

By: Rebecca Knight

On December 2, 2015, Syed Rizwan Farook and his wife Tashfeen Malik attacked Farook's office holiday party, killing fourteen people and wounding over twenty others, in what officials are investigating as an act of terrorism.[1] In the course of this investigation, the Federal Bureau of Investigation ("FBI") seized an iPhone 5c pursuant to a federal search warrant authorizing the search of a black Lexus IS300.[2] The iPhone was owned and issued to Farook by his employer, the San Bernardino County Department of Public Health ("SBCDPH"), as part of his employment.[3] In addition to the issued work phone, agents also examined two other mobile devices belonging to Farook and Malik that were obtained, destroyed and discarded, from the trash behind the Farook residence.[4] SBCDPH gave consent for the iPhone to be searched, but it was locked and secured by a numeric passcode created by Farook.[5] Despite the phone being locked, FBI agents were able to find evidence in the phone's iCloud account indicating that Farook had communicated with co-workers that would later become victims during the mass shooting.[6] Agents believed that there may be "relevant, critical communications and data" on the phone from around the time of the shooting, but the information would reside solely on the phone itself.[7] However, without the passcode, the information could not be accessed by any means known to the government or Apple because of the powerful passcode system and encryptions[8] embedded in the iPhone's operating system and hardware.[9] Thus, the battle between the FBI and Apple over providing assistance to hack into Farook's iPhone began.

The FBI's Position

On February 16, 2016, the United States of America ("Government") filed an *ex parte* application pursuant to the All Writs Act ("Act") for an order compelling Apple to provide assistance to FBI agents in their search of Farook's iPhone.[10] Originally enacted in 1789, the Act provides that "[t]he Supreme Court

and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[11] The Government claimed that only Apple had the "exclusive technical means" to assist the FBI in completing the search, but Apple declined to provide the assistance voluntarily.[12] Apple manufactured the iPhone and created the operating systems and software, thus it could easily modify the operating system and disable software.[13] On older operating systems, Apple has the ability to obtain unencrypted information from iPhones without the passcode, and has done so before to help law enforcement execute search warrants in accordance with accompanying All Writs Act orders.[14] However, the operating system running on newer iPhones was designed to provide much greater protection to the iPhone's owner so that even Apple could not bypass the system.[15] Regardless, the Government maintained that because Apple built the iPhone it could also hack into Farook's.

The FBI sought Apple's assistance with two objectives: (1) removal of security features such as auto-erase and delays coded into the operating system; and (2) modification of the data encryption embedded into iPhone hardware.[16] With respect to the first objective, the FBI was unable to search the device because it was locked by a secure, user-determined, numeric passcode.[17] The FBI could not make attempts to determine the passcode because Apple had coded an auto-erase function into the iPhone's operating system.[18] After ten erroneous attempts at entering the passcode, the auto-erase function activates and permanently deletes all encrypted information contained on the device.[19] In addition to the auto-erase function, Apple had also created a delay after every erroneous passcode entered, locking the phone for increasing amounts of time before another passcode entry can be attempted.[20] This means that after every failed passcode entry attempt, the user must wait for a set amount of time before another attempt can be made, up to an hour by the ninth attempt.[21] The FBI wanted Apple to disable both security features.

With respect to the second objective, Apple had designed the iOS 9 operating system for iPhones to encrypt the data files found on the devices using two components: (1) the user-determined passcode; and (2) a unique 256-bit Advanced Encryption Standard ("AES") key that is embedded into the phone itself during manufacturing.[22] Both components must be satisfied in order for the operating system to decrypt the phone's data.[23] When the user inputs a passcode, the phone conducts a complex calculation through Apple's software.[24] This complex calculation combined with the AES unlocks and decrypts the data on the phone.[25] This encryption process is the root of the Government's problem. The Government believes that because Apple designed, implements, and updates the iOS operating system, it also has the technical capabilities to modify the system to enable the FBI to hack into Farook's phone.[26] As such, the Government requested that Apple be ordered to provide the FBI with a custom software file with a unique identifier that can be loaded onto the device.[27] Once loaded, the custom software would have three primary functions: (1) bypass or disable the auto-erase function; (2) enable the FBI to submit passcodes to the iPhone electronically for testing; and (3) eliminate any additional delays between failed passcode attempts beyond what is incurred by the hardware on the device.[28] The software would be installed on Farook's iPhone at either a government facility, or alternatively, at an Apple facility, but any passcode attempts would be made by the Government. The Government also requested that the order permit Apple to satisfy the three functions by the software requested or by an alternative technical manner, but the alternative means must be mutually agreeable.[29]

The Government argued that the order to compel Apple's assistance was permitted by the All Writs Act, which allows a court, in its "sound judgment" to issue orders necessary "to achieve the rational ends of law" and "the ends of justice entrusted to it."[30] The Government further contended that the Court has the authority "in aid of a valid warrant, to order a third party to provide *nonburdensome* technical assistance to law enforcement officers" to facilitate the execution of the search warrant.[31] This contention relied heavily on *United States v. New York Telephone Co.*, a 1977 Supreme Court decision, which upheld

an order directing a phone company to help the government execute a pen register search warrant issued under Rule 41.[32]

New York Telephone Co. established three factors to determine whether an All Writs Act order to the phone company is appropriate.[33] The factors are: (1) whether the third-party is not "so far removed from the underlying controversy that its assistance could not be permissibly compelled;" (2) whether the order is likely to place any unreasonable burden on the third-party; and (3) whether the assistance of the third-party is necessary to effectuate the warrant.[34] The Government argued that each factor supported the issuance of the order directed to Apple.[35]

First, the Government contended that Apple is not far removed from the matter because it designed, manufactured, and sold the iPhone; in addition, Apple wrote and owns the software that is preventing the Government from executing the warrant.[36] IPhones can only run software cryptographically signed by Apple.[37] Access to the code that creates that software is restricted to Apple. Thus, no other party, except for Apple, has the ability to assist the Government in manipulating the software.[38]

Second, the Government contended that the order would not place any unreasonable burden on Apple because compliance would require little effort for Apple, and reasonable reimbursement for that effort would be available.[39] The order would require Apple to write software code, but, the Government alleged, that is not an unreasonable burden on a company that writes software code in its regular course of business.[40]

Third, the Government argued that Apple's assistance was necessary to fully execute the search warrant.[41] Full execution of the warrant is necessary because Farook is believed to have caused "the mass murder of a large number of his coworkers" and "built bombs and hoarded weapons for this purpose."[42] Evidence from the phone's iCloud account demonstrated that Farook communicated with victims of the

shooting, as well as Malik, and the most recent backup was done in October 19, 2015 (a month and a half before the shooting).[43] The last backup indicated to the FBI that Farook may have disabled the automatic iCloud backup function to hide evidence, such as accomplices or plans for other attacks, which can now be found only on the device itself.[44] For all of these reasons, the Government requested that the court order Apple to assist the FBI in the searching the iPhone in accordance with its proposed order.

The Order

On the same day the *ex parte* application was filed by the Government, Magistrate Judge Sheri Pym granted the order compelling Apple to assist the FBI in searching the iPhone.[45] It was ordered that: (1) Apple should assist in enabling the search of Farook's iPhone 5c by providing reasonable assistance to law enforcement to obtain access to the data on the phone; (2) the assistance should accomplish the three primary functions previously mentioned; (3) Apple's reasonable assistance may include providing the FBI with the software described above to be loaded onto the device; (4) if Apple determines that it can achieve the three primary functions using an alternative technological means, then Apple could comply with the Order that way, as long as the Government approves; and (5) Apple should advise the Government of the reasonable costs of providing its assistance.[46] This was the first time a judge issued such an order for an iPhone running Apple's iOS 9 operating system.[47]

Apple's Position

In true Apple fashion, CEO Tim Cook took the battle to the people first, and to the courts second.[48] In a message addressed to Apple customers, Cook wrote that: "[t]he United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand."[49] Cook went on to explain that Apple has no sympathy for terrorists and provided the FBI with all of the data requested that was in its possession.[50] Apple complied with all subpoenas and search warrants, made engineers available to

advise the FBI, and offered ideas on investigative options at its disposal.[51] But then the Government asked for something that Apple did not have, and something that it considers "too dangerous" to create, and that is a "backdoor to the iPhone."[52] Cook proclaimed that a backdoor would be a "master key" that could be used to unlock any iPhone which would undermine decades of technological advancements to protect iPhone users from hackers and cybercriminals.[53] Apple believed that the FBI's intentions were good, but that it would be wrong for the government to force it to weaken its Apple products, especially when there is no way to guarantee that the technique would be limited to just Farook's phone. Cook concluded that Apple fears the Order would "undermine the very freedoms and liberty our government is meant to protect." These sentiments are reflected in Apple's Motion to Vacate filed on February 25, 2016.[54]

Apple's position was simple. The Order was not about one iPhone; it was about the privacy interests of millions of iPhone users around the globe.[55] Apple's motion began with an emphasis on the necessity for increased security in a modern world dependent on technology.[56] Apple claimed that since the beginning of the computer age, there have been people dedicated to breaching the security of technology and stealing the personal information stored therein.[57] Apple highlighted that even the Government has fallen victim to hackers, cybercriminals, and foreign agents on a regular basis, including a breach that affected 22 million federal workers and their family members.[58] Knowing that the stakes are high, Apple claimed that it has dedicated itself to enhancing the security of its devices, so that customers are confident that their private information – financial records, credit card information, health information, physical location, calendars, family photographs, personal messages – are all protected.[59] In order to protect its customers and their private information, Apple uses encryption and improves security with every software release, because breaches are becoming more frequent and highly sophisticated.[60] Apple believes that encryption provides the strongest means to ensure the safety and privacy of its customers, and the Government now seeks to undermine that protection through the Order.[61] To that end, Apple argued that:

> Rather than pursue new legislation, the government backed away from Congress and turned to the courts, a forum ill-suited to address the myriad [of] competing interests, potential ramifications, and unintended consequences presented by the government's unprecedented demand. And more importantly, by invoking 'terrorism' and moving ex parte behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis.[62]

Essentially, Apple's argument was that Congress, not the courts, should determine when a third-party must be compelled to assist in investigations conducted by the government. Additionally, Apple contended that if the technology that the Government wants were to be created, millions of people would be at risk of having their personal data hacked at no fault of their own but rather as a consequence of Farook's act of terrorism.[63]

Legally, Apple argued that the Order had no statutory basis and violated the Constitution. Vehemently opposing the Government's use of the All Writs Act to secure the Order, Apple contended that the Act is intended to enable the federal courts to fill in gaps in the law, not provide the courts with unlimited and unrestrained power.[64] More specifically, Apple maintained that the Act does not grant authority to compel assistance when Congress has considered but decided not to permit such authority.[65] In the Communications Assistance of Law Enforcement Act ("CALEA")[66], Congress decided not to require electronic communication service providers to facilitate the government's decryption of devices.[67] Apple claimed that it is an electronic communication service provider because it makes mobile phones and provides customers with messaging services through iPhones.[68] As such, Apple argued, the Government may not use the All Writs Act to do what Congress refused to allow in the CALEA.[69] Thus, according to Apple, the court's Order expanded the obligations under the CALEA, and violated the separation-of-powers by performing a legislative function when it repurposed the statute to meet the Government's request.[70]

Next, Apple argued that the factors established by *New York Telephone Co.* were not met, so the court was not permitted to order the "unprecedented and unreasonably burdensome" assistance

requested by the Government.[71] First, Apple contended that its connection to the underlying case was too far removed to compel assistance.[72] Specifically, Apple claimed that it is a private company that does not own or possess the phone at issue, has no connection to the data sought from the phone, and is not related in any way to the mass shooting that gave rise to the investigation.[73] Apple merely placed a good into the stream of commerce, and cannot be linked to an alleged terrorist because it did.[74]

Second, Apple argued that, if carried out, the Order would impose an "unprecedented and oppressive" burden on Apple because it would require Apple to develop software and a system that does not exist.[75] Experienced Apple engineers would have to design, create, test, and validate the requested system within a hyper-secure isolated room, then deploy and supervise the operation of the system by the FBI.[76] According to Apple, the technical assistance sought would be much more vast and complicated than simply pushing a few buttons, as the Government seemed to believe.[77]

Third, Apple argued that the Government did not demonstrate that Apple's assistance was necessary to effectuate the warrant.[78] The Government did not exhaust all avenues for recovering the information, and ignored the fact that the FBI foreclosed an avenue when it changed the iCloud password associated with Farook's iPhone, and prevented the phone from performing an automatic iCloud backup of the information contained on the phone.[79] Moreover, the Government made no showing of whether or not it sought or received technical assistance from other federal agencies with expertise in digital forensics, which could negate the need for Apple to create a backdoor into the iPhone.[80] Thus, in Apple's opinion, the Order should not have been granted because the Government did not satisfy the factors under *New York Telephone Co.*

Finally, Apple argued that compliance with the Order would violate the First Amendment and the Fifth Amendment's Due Process Clause.[81] Specifically, the Government asked the court to compel Apple to write software that would eliminate safety features built into the iPhone in response to consumer

privacy concerns.[82] Apple contended that the Order amounted to compelled speech and viewpoint discrimination.[83] Under established law, computer code is treated like speech within the meaning of the First Amendment.[84] Thus, whenever the Government seeks to compel speech, the First Amendment is triggered.[85] Compelled speech can only be upheld if it is narrowly tailored to obtain a compelling state interest.[86] Apple contended that in this instance, the Government could not meet this high standard.[87] In particular, Apple argued that, although investigating terrorists is a legitimate interest, the government only produced speculative evidence that Farook's iPhone might contain relevant information.[88] Moreover, terrorists and other criminals use highly sophisticated encryption techniques and readily available applications (apps).[89] As such, any information that could be on the phone could be protected behind several layers of non-Apple encryption.[90] More importantly, the FBI foreclosed the option of backing up the data into the iCloud by changing the password, which certainly would have been a more narrowly tailored option.[91] Thus, Apple believed that it could not be compelled to speak (write code) pursuant to the Order.

Apple also argued that the Order discriminated on the basis of Apple's viewpoint.[92] When Apple designed the iOS 9 software, it wrote code that announced the value it placed on data security and the privacy of its consumers by leaving out a backdoor for anyone, including Apple, to use.[93] Thus, Apple argued that being compelled to write new software in accordance with the Government's contrary view that national security trumps data security and consumer privacy violated its First Amendment rights and provided additional grounds to vacate the Order.

In addition to the First Amendment, Apple argued that the Fifth Amendment's Due Process Clause prohibited the Government from compelling Apple to create the code.[94] By conscripting Apple, a private party, with an attenuated connection to the crime to do the Government's bidding, the Order violated Apple's right to be free from "arbitrary deprivation of [its] liberty."[95] The touchstone of due process is

protection of the individual from arbitrary action by the government.[96] However, the Order was clearly compelling Apple to do something it did not want to do, without any definitive showing that doing so would lead to any worthwhile information. Therefore, Apple argued that the action was arbitrary and Apple should be protected from having to do the Government's bidding.[97]

New York District Court Sides with Apple

While the battle between the FBI and Apple raged in California, the Government was trying to start another one in New York. In the Eastern District of New York, the Government sought an All Writs Act order requiring Apple to bypass the passcode security on an iPhone belonging to a confessed drug dealer.[98] On February 29, 2016, Magistrate Judge Orenstein denied the order in a lengthy opinion that could be adequately described as a judicial spanking.[99] The court recognized that there were significant competing interests at play, such as the commercial interest in conducting a lawful, private business as owners deem most productive, free from harmful governmental intrusion; individual safety and privacy; and national security.[100] Siding with Apple, the court reasoned that these competing interests must be balanced and debated by legislators who are equipped to consider the technological and cultural realities of a modern world unconceived by their predecessors.[101] Judge Orenstein concluded that "it would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789."[102] Two days after the New York ruling, Apple filed a notice of supplemental authority with the Central District of California to "bring to the court's attention" the scathing opinion.[103]

An Anticlimactic Ending

Apple's Motion to Vacate was scheduled for a March 22, 2016 hearing before Judge Pym.[104] On March 21, Judge Pym stayed the Order requiring Apple to help the Government hack the iPhone, and cancelled the scheduled hearing.[105] The hearing was cancelled until the FBI could determine whether an

unidentified third party could access the data on the iPhone, as it had promised.[106] And it did. On March 28, the Government filed a Status Report announcing that it had successfully accessed Farook's phone and the data stored on it and no longer required Apple's assistance.[107] However, no details were provided about how or who helped the FBI gain access. As a result of this newfound access, the Government requested that the Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016 be vacated.[108] On March 29, 2016, the Order was vacated for good cause, and Apple's Motion to Vacate was denied as moot.[109] A statement issued by U.S. Attorney Eileen M. Decker on March 28 stated that the Government's decision to request that the order be vacated "was based solely on the fact that, with the recent assistance of a third party, we are now able to unlock that iPhone without compromising any information."[110] Thus, the Government did not back off its position that the courts should and can compel a private party to assist in a Government investigation under the All Writs Act, even if it means creating technology that never existed before, and weakening a private company's product.

The Status Report and the vacating of the Order may have brought the hotly contested battle between the FBI and Apple to an abrupt and somewhat mutually agreeable end, but the differing opinions of Judge Pym and Judge Orenstein leave more questions than answers. The most important questions: (1) whether national security trumps consumer privacy; (2) how far the government and courts can go in forcing private companies to help in investigations under the All Writs Act; and (3) who should decide, the courts or Congress, remain unsettled. But a clear answer is needed, and with the increasing reliance on technology as a necessary component of modern life, it is needed sooner rather than later.

---

[1] *See*, *e.g.,* Greg Botelho and Ralph Ellis, *San Bernardino Shooting Investigated as "Act of Terrorism,"* CNN (December 5, 2015), http://www.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html.
[2] Gov't. *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search filed February 16, 2016.
[3] Decl. of Christopher Pluhar filed February 16, 2016.
[4] *Id*. at 4.
[5] *Id*. at 3.
[6] *Id*.
[7] *Id*.

[8] *See* Daniel Garrie, Yoav Griver, and Elad Yoran, *Privacy vs. Accessibility: Can They Coexist in Cyberspace?*, Law360 (February 26, 2016), http://www.law360.com/articles/763727 (Encryption "is the conversion of data [from plaintext] into another unintelligible form, called cipher text, which cannot be understood by anyone (or by computers) until it is decrypted back to its original form. The process of encryption and decryption is based on complex mathematics implemented thr[o]u[gh] algorithms and the use of long strings of prime numbers [called] keys.").
[9] *Id*. at 3-4.
[10] Gov't. *Ex Parte* Application at Lines 21-25.
[11] 28 U.S.C. § 1651(a).
[12] Gov't. *Ex Parte* Application at 1.
[13] *Id*. at 3.
[14] *Id*. at 4.
[15] *Id*.
[16] *Id*. at 4-5.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*. at 4.
[21] *Id*. at 7.
[22] *Id*. at 5.
[23] *Id*.
[24] *Id*. at 6.
[25] *Id*.
[26] Gov't. *Ex Parte* Application at 7.
[27] *Id*. at 7-8.
[28] *Id*. at 8.
[29] *Id*. at 8-9.
[30] *Id*. at 9 (internal citation omitted) (emphasis added).
[31] *Id*.
[32] *Id*. at 10 (internal citation omitted).
[33] *Id*. at 12 (internal citation omitted).
[34] *Id*. at 12-13 (internal citation omitted).
[35] *Id*. at 13.
[36] *Id*.
[37] *Id*.
[38] *Id*.
[39] *Id*. at 14.
[40] *Id*. at 15.
[41] *Id*. at 16.
[42] *Id*.
[43] *Id*. at 17.
[44] *Id*.
[45] Order Compelling Apple, Inc. to Assist Agents in Search entered February 16, 2016, 2016 U.S. Dist. LEXIS 20543.
[46] *Id*. at *1-*4.
[47] Y. Peter Kang, *Apple Ordered to Help Hack San Bernardino Shooter's Phone*, Law360 (February 16, 2016), http://www.law360.com/articles/759947.
[48] Tim Cook, *A Message to Our Customers*, Apple (February 16, 2016), http;//www.apple.com/customer-letter/.
[49] *Id*. at 1.
[50] *Id*.
[51] *Id*.
[52] *Id*. at 2.
[53] *Id*.

[54] Apple Inc.'s Mot. to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance entered February 25, 2016, Case No. 5:16-cm-00010-SP.
[55] *Id*. at 1.
[56] *Id*.
[57] *Id*.
[58] *Id*.
[59] *Id*. at 2.
[60] *Id*.
[61] *Id*. at 2 and 5.
[62] *Id.*
[63] *Id*. at 4.
[64] *Id*. at 14
[65] *Id*. at 15.
[66] 47 U.S.C. §§ 1001-1010.
[67] *Id*. at 16.
[68] *Id*. at 16-17.
[69] *Id*. at 17.
[70] *Id*. at 18.
[71] *Id*. at 20.
[72] *Id*.
[73] *Id*. at 21.
[74] *Id*. at 22.
[75] *Id*. at 23.
[76] *Id*.
[77] *Id*. at 28.
[78] *Id*. at 29.
[79] *Id*. at 29-30.
[80] *Id*. at 30.
[81] *Id*. at 32.
[82] *Id*.
[83] *Id*.
[84] *Id*. (internal citations omitted).
[85] *Id*.
[86] *Id*.
[87] *Id*. at 33.
[88] *Id*.
[89] *Id*.
[90] *Id*.
[91] *Id*. at 34.
[92] *Id*. at 33.
[93] *Id*.
[94] *Id*. at 34.
[95] *Id*. (internal citations omitted).
[96] *Id*. (internal citations omitted).
[97] *Id*.
[98] In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issues by This Court, 2016 U.S. Dist. LEXIS 25555 (2016).
[99] *Id*. at *2.
[100] *Id*. at *96.
[101] *Id*. at *97.
[102] *Id*.
[103] Allison Grande, *Apple Puts NY Order Into Play in Calif. Phone Unlock Fight*, Law360 (March 2, 2016), http://www.law360/articles/766423.

[104] *Id*. Cover Page at Line 25.
[105] Y. Peter Kang, *DOJ Hacks Shooter's iPhone, Drops Apple Suit*, Law360 (March 28, 2016), http://www.law360.com/articles/777150.
[106] *Id*. at 1.
[107] Gov't. Status Report filed March 28, 2016.
[108] *Id*. at 2.
[109] Order Vacating February 16, 2016 Order entered March 29, 2016, Case No. 5-16-cm-00010-SP.
[110] Y. Peter Kang, *DOJ Hacks Shooter's iPhone, Drops Apple Suit* at 1.