Health Technol. (2017) 7:369–376
DOI 10.1007/s12553-017-0192-4

ORIGINAL PAPER

# Can Apple build a privacy minded iPhone security system so secure that Apple cannot access it?

**Brian L. Owsley** [1]

Received: 1 September 2016 / Accepted: 2 May 2017 / Published online: 7 June 2017


**Abstract** The world has become less secure and less private with the advent of technology. Law enforcement agencies, such as the FBI, have sophisticated technology that would amaze J. Edgar Hoover. In response to this increasing surveillance capabilities, telecommunications providers like Apple are seeking to keep pace with technological advances of their own to protect the personal privacy of their consumers and subscribers. In the background of this factual situation, the article explores the vagaries of security in our technological world in light of the dispute between the FBI and Apple regarding the iPhone at issue is the San Bernadino shooting. The current law poses challenges for both the FBI and telecommunications providers like Apple. Moreover, legislative solutions are also difficult to envision. Ultimately, the government should be cautious about preventing software manufacturers from seeking to create impenetrable operating systems. Indeed, the prevention of development of better software and operating systems comes at the expense of the loss of privacy in financial and health records.

**Keywords** Apple · FBI · iPhone · Password · Privacy security

## 1 Introduction

Last year's legal battle between Apple and the FBI raises many concerns about privacy of the various types of data that are at issue regarding the most intimate aspects of most of our lives. For example, many among us, have access to, or interact with multiple digital devices; and a typical iPhone contains a myriad of personal data, including email, contact information for friends and colleagues, photographs, videos, notes, and many other types of information.

Among the apprehensions related to the well-advertised dispute between Apple and the FBI in association to the San Bernadino terrorist's iPhone case are, the future concerns that it portends. Recall the omnipotence paradox, which is essentially a philosophical principle enunciated by St. Thomas Aquinas among others.[1] In a basic form of the principle, the question is posited, whether it will be possible for God to create a stone so large, which God then cannot lift.[2] While that does present a dilemma for philosophers to grapple, how does this concern affect privacy? Simply put, the paradox can be rephrased to ask whether Apple can build an iPhone security system so secure, and impenetrable, that even Apple could not access.

This article is part of the Topical Collection on *Privacy and Security of Medical Information*

✉ Brian L. Owsley
brian.owsley@untdallas.edu

[1] UNT Dallas College of Law, 1901 Main Street, Dallas, TX 75201, USA

[1] Thomas Aquinas, The Summa Theologica, Book 1, Question 25, art. 3.

[2] Philosopher Rene Descartes addresses this paradox in his work. *See* Rene Descartes, "Mediation V: On the of Material Objects and More on God's Existence," *Meditations on First Philosophy.*

Indeed, this philosophical question has even found a home in American pop culture. *The Simpsons* provide a more modern whimsical version of this question in a discussion between Homer and Ned Flanders:

Homer: Hey, I've got a question for you. Could Jesus microwave a burrito so hot that he himself could not eat it?

Ned: Well sure of course, … he could, … but then again…. Wow, as melon scratchers go, that's a honey doodle.

Homer: Now you know what I've been going through.

https://www.youtube.com/watch?v=JhhXCuUG2pw (The Simpsons, *Weekend at Burnsie's* (Apr. 7, 2002)).

## 2 The ins and outs of the dispute between the FBI and Apple

How did we arrive to this highly contentious fight between Apple, one of the most successful global telecommunications companies, and the U.S. Federal Bureau of Investigations (FBI), the United States' leading domestic law enforcement agency? It began on December 2, 2015, when a married couple Tashfeen Malik and Syed Rizwan Farook decided to embark on a mass killing spree, at Farook's workplace in San Bernadino, California, killing fourteen people and wounding over twenty others. Prior to the attack, Malik declared her allegiance to the Islamic State in Iraq and the Levant (ISIL), also known as ISIS. This pledge - in our age of social media, was most fittingly made via Facebook. During their assault on the workplace, law enforcement officers killed both terrorists. Afterwards, the FBI launched an investigation of the two attackers, in order to ascertain whether there were more individuals involved.

During the course of the FBI's investigation, it was learned that one of the terrorists left behind an Apple iPhone that may have some important data or information still on it. Initially, the FBI sought Apple's assistance in unlocking the cell phone to access the data. Indeed, Apple had provided technical assistance on numerous occasions in the past - for the FBI.

As one may recall, Farook had an iPhone 5c, which was ran the iOS Version 9 Operating System, and was issued to him by his employer, the San Bernadino County Public Health Department, who then authorized the FBI to access his government-issued cell phone. The existing problem stemmed from the fact that Farook had enabled the settings feature requiring a password in order to access the phone. Thus, if the FBI's specialists attempted to randomly generate the correct password for the iPhone, they could cause the phone to delete all data after a set threshold for incorrect password attempts was reached, if Farook had set the iPhone to erase all data automatically when 10 failed password attempts had been made.

In February 2016, the FBI sought Apple's assistance in decrypting Farook's iPhone so that the agency could obtain access to the data onboard the iPhone. When Apple did not cooperate in a manner that the FBI found satisfactory, and given its investigatory needs, the FBI sought and received a federal court order, mandating that Apple assist the FBI in its onboard search of Farook's iPhone.[3]

In addition to the courtroom battle, Apple and the FBI waged a media campaign to convince the public of the value of their respective positions. Apple CEO Tim Cook issued an open letter to Apple's customers decrying the FBI's request as a "dangerous precedent." Cook wrote,

> "*We have great respect for the professionals at the FBI, and we believe their intentions are good. 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 we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.*
>
> *Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.*
>
> *The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.*"[4]

FBI Director James Comey responded a few days later, challenging Apple's account and arguing that its request for assistance is necessary, and justified, stating:

> "*The particular legal issue is actually quite narrow. The relief we seek is limited and its value increasingly obsolete because the technology continues to evolve. We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land. I hope thoughtful people will take the time to understand that. Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't. But we can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead.*
>
> *So I hope folks will remember what terrorists did to innocent Americans at a San Bernardino office*

[3] *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451 M (C.D. Cal. Feb. 16, 2016) (Order Compelling Apple, Inc. to Assist Agents in Search).

[4] Tim Cook letter to Apple customers dated February 16, 2016, *available at* http://www.apple.com/customer-letter/.

*gathering and why the FBI simply must do all we can under the law to investigate that. And in that sober spirit, I also hope all Americans will participate in the long conversation we must have about how to both embrace the technology we love and get the safety we need.*"[5]

Thus, the battle lines were drawn. This fevered pitched raged for a while in the media.

Then, on March 28, 2016, the FBI abruptly informed the district court and Apple that it would not need Apple's assistance as it had "successfully accessed the data stored on Farook's iPhone."[6] This report followed the revelation by the FBI that it had obtained a method by which to circumvent the security system for Farook's iPhone thus obviating the need for any assistance from Apple [2].

In the end, the FBI paid a third-party more than $1.3 million to hack into Farook's iPhone so that Apple's assistance was rendered unnecessary [3]. This figure of $1.3 million, was based on a statement by FBI Director Comey that the agency paid more than the remaining amount he would earn over the course of his term as director [3]. It raises the question, of why, the FBI had to hire a private individual or firm - to engage in this work - instead of handling it internally with its agents. Fortunately, the FBI got value for its investment, as it indicated that the information extracted from Farook's cell phone was useful, even though there was no evidence of any contact with ISIS [4].

Of course, Apple now wanted to know how the FBI succeeded in accessing Farook's cell phone [5]. It would be interesting to know whether the FBI did share how it accessed Farook's cell phone with Apple. Such cooperation by the federal government with private industry would be consistent with the longstanding federal policy to notify companies of specific vulnerabilities.[7] The downside for the government was that Apple would repair the vulnerability thus preventing the government from obtaining access in the future when it encountered a similar problem. In a situation where the government cannot access an Apple iPhone because the vulnerability has been correct, it would again have to pay another hacker or teams of hackers to access the device. If this approach failed, then it would have to pursue the legal wrangling that was short-circuited here by the government's hacking success. Regardless, Apple is no doubt unhappy that the cell phone buying public now views its security as breakable. Still, it could market the new and improved iPhone once it has fixed the vulnerability.

## 3 The government argued that Apple's assistance was required pursuant to the *All Writs Act*

Prior to accessing Farook's cell phone with the assistance of its hacker, the FBI argued that the *All Writs Act* provided the basis for the court to order Apple to access the cell phone. A judge may exercise the discretion to grant a request pursuant to the *All Writs Act,* if the statute's requirements are met, but is not obligated to grant any such request.[8] In other words, a federal judge has discretion whether even to exercise the authority provided in the *All Writs Act.*

The *All Writs Act* was enacted in 1789, and allows federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[9] The Supreme Court has characterized this as an extraordinary writ - that should be used only in extraordinary circumstances.[10]

In *United States v. New York Telephone Company*,[11] a pivotal case regarding the dispute between Apple and the FBI, the Supreme Court addressed the use of the *All Writs Act* to compel a telephone company to provide telephone numbers pursuant to a pen register.[12] In addressing whether the use of this statute was appropriate regarding a pen register, the Court concluded that "that the power of federal courts to impose duties upon third parties is not without limits [as] unreasonable burdens may not be imposed."[13]

Consequently, use of the *All Writs Act* regarding applications for court orders authorizing electronic surveillance are impermissible when the order unreasonably burdens the provider. How unreasonable burden is measured or assessed is difficult, but at minimum, Apple would have had a good argument - that the FBI's request for it to create a means to hack into Farook's iPhone (especially if such action would jeopardize the security provided to Apple iPhone users with the same operating software), would be unreasonably burdensome.

[5] FBI Press Release dated February 21, 2016, *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter.

[6] *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451 M (C.D. Cal. Mar. 28, 2016) (Government's Status Report); [1].

[7] *See* "Commercial and Government Information Technology and Industrial Control or System Vulnerabilities Equities Policy and Process," *available at* https://www.eff.org/files/2015/09/04/document_71_-_vep_ocr.pdf; *see also* [6].

[8] *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 149 F. Supp. 2d 341, 350–51 (E.D.N.Y. 2016).

[9] 18 U.S.C. § 1651.

[10] *Platt v. Minnesota Mining & Mfg. Co.*, 376 U.S. 240, 245 (1964) (quoting *Ex parte Fahey*, 332 U.S. 258, 260 (1947)).

[11] 434 U.S. 159 (1977).

[12] *See id.* at 161–64.

[13] *Id.* at 172.

## 4 Congress cannot succeed in enacting legislation to either bar Apple's efforts or protect Apple's efforts

Notwithstanding the fact that Apple will continue to struggle with its ability to create an iPhone so secure that it cannot hack into it, the federal government has begun murmuring about taking measures to prevent Apple (and other technology providers) from creating software or technology that is so secure it is impenetrable. Senator Richard Burr, a Republican from North Carolina, and Senator Diane Feinstein, a Democrat from California, as the leaders of the Senate Intelligence Committee have co-sponsored a bill proposing legislation that would bar technology so impenetrable it cannot be accessed.[14] A few states have also proposed similar legislation, either requiring companies like Apple to be able to decrypt their smartphones for law enforcement, or penalizing providers that cannot decrypt.[15] Like the federal proposal, none of these state bills became law.

This phenomenon of passing laws to enable access to encrypted devices has also reached Europe. The European Union law makers are considering legislation that would enable governmental authorities to "access data stored in the cloud by encrypted apps" [8]. Vera Jourova, the European Union Justice Commissioner explained that European officials needed better more reliable ways to obtain such information from providers.[16] In March 2017, the German government proposed a law requiring companies to remove with 24 h any content that was obviously criminal in nature or face at 50 million euro fine.[17]

Interestingly, just a few years earlier, American federal legislators proposed protections for providers like Apple, seeking to ensure that they could create impenetrable technologies. In 2014, members of Congress introduced a bill entitled "Secure Data Act of 2014," proposing "[t]o prohibit Federal agencies from mandating the deployment of vulnerabilities in data security technologies."[18] However, this bill failed. More recently, some members of Congress have introduced legislation to prevent law enforcement officers from search cell phones at the border without a warrant.[19] Relying on a Supreme Court decision mandating a warrant for a search of a cell phone, *Riley v. California*,[20] Senators Ron Wyden and Rand Paul have introduced a bill.[21] Members of the House of Representatives have introduced a similar bill.[22] As Senator Paul explained, "innovation does not render the Fourth Amendment obsolete."[23]

The fact that Congress has been unsuccessful in both barring federal agencies from mandating decryption in support of law enforcement, or requiring that providers refrain from creating unbreakable encryption software, does not mean that there have not been adverse consequences for providers. For example, Lavabit was an encrypted email service created and operated by its owner Ladar Levison in 2004 to provided secure email for paying subscribers, including his most infamous client, Edward Snowden.[24] Based on a federal investigation regarding a target who was a Lavabit customer, the federal government sought court orders requiring Lavabit to provide information pursuant to the Pen Register Statute and the Stored Communications Act.[25] Lavabit employed a sophisticated encryption system that was designed to protect a subscriber's emails while they were being stored as well as during transmission.[26] This encryption system was dependent on keys that were created by Lavabit and that the federal government sought in order to access the data that Lavabit had regarding the criminal investigation target. Essentially, Levison refused to comply with the court orders to provide the keys because he maintained that his other 400,000 subscribers' emails would be compromised.[27]

In response to an adverse rulings by the federal courts requiring Levison to produce the encryption keys, he had closed down Lavabit instead, thus avoiding to have complied with the request [10]. Levison explained his decision on Lavabit's website: "I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit."[28] The federal government's approach mirrors many of those it took with Apple in the San Bernadino case. Of course, there are large differences between Lavabit and Apple, the latter being one of the most successful companies today and Lavabit at its height had 410,000 subscribers [11].

It would be highly unlikely for Apple to close, or be shut down by the federal government. Apple is a top Fortune 500 company that is only behind WalMart and Exxon Mobil in the rankings with revenue of $233.7 billion.[29] There are well over one billion Apple devices being used worldwide [12]. Indeed,

[14] https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf; see also [7].
[15] *See* Assem. Bill 1681, 2015–2016 Reg. Sess. (Cal. 2016); House Bill 1040, 2016 Reg. Sess. (La. 2016); Assem. Bill A8093, 2015–16 Leg. Sess. (N.Y. 2015).
[16] *Id.*
[17] *Id.*
[18] H.R. 5800, 113th Cong. (2d Sess. 2014); *see also* S. 2981, 113th Cong. (2d Sess. 2014).
[19] Morgan Chalfant, "Lawmakers introduce bill to end warrantless phone searches at border," The Hill, www.thehill.com/policy/cybersecurity/3277246-bipartisan-bill-would-end-warrantless-searches-of-digital-devices-at.
[20] 573 U.S. _, 134 S. Ct. 2473 (2014).
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *See In re Under Seal*, 749 F.3d 276, 279 (4th Cir. 2014); [9].
[25] *See In re Under Seal*, 749 F.3d at 279.
[26] *See id.*
[27] *See id.* at 280.
[28] https://lavabit.com/; *see also* Ackerman, *supra* note _.
[29] fortune.com/fortune500/apple-3.

Apple has sold over one billion iPhones around the world, including about 100 million in the United States [13, 14].

Arguably, the closing of Lavabit was an extreme response and was not compelled directly by the government's actions. However, the ultimate concern is that the government could use its power in cases similar to Apple's against companies like Lavabit that result in either the complete capitulation by the company, or the complete destruction of it, by the government. It seems unlikely that Apple was willing to cooperate with the government unless ordered to do so by a court of law. In the case involving the San Bernandino shooting, it is unlikely that a court would have ordered Apple to decrypt the cell phone if Apple could demonstrate that it was truly burdensome. If the decryption would have jeopardize Apple's overall security of its iPhones, then decryption likely was truly burdensome.

Even if Congress could reasonably put forward some type of legislation toward the goal of requiring providers to enable access encrypted devices, the response by providers would no doubt be quick and firm against it. It appears unlikely that in this era of legislation the American legislators would be willing to stand up to such political pressures.

## 5 Congress should be wary of thwarting the development of impenetrable operating systems and software

The federal government may want to be cautious about banning the use of impenetrable encryption. Such a ban would disincentivize companies from developing this capability and reduce greatly the likelihood that it will be created; when the federal government quite likely would benefit from such encryption.

Indeed, a congressional committee report indicates that the Chinese government hacked into computers and servers at the Federal Deposit Insurance Corporation between 2011 and 2013, including the computer of its Chairwoman Sheila Bair [15]. Moreover, American federal officials have accused the Chinese government of hacking into an Office of Personnel database compromising sensitive personal information of about 21 million current and former federal employees [16, 17]. Additionally, the federal government has indicted five individuals employed by the Chinese military to hack into private American companies seeking trade secrets.[30]

Similarly, Iranian hackers sponsored and supported by their government have targeted American State Department officials who worked on Iranian matters and hacked into their email and other social media accounts [19]. Other Iranian hackers have targeted a four-star admiral, through online contacts with the person's family and friends [20].

Finally, Russian governmental officials are hacking into American computers in a new form of espionage. Russian hackers working on behalf of the Russian government allegedly hacked into the computers at the United States Department of State, which in turn enabled them to hack into the White House computer system [21]. The Obama Administration took the significant step of publically accusing the Russian government of being behind the hacking of the Democratic National Committee's computers, which in turn led to a large release of sensitive emails, potentially in an attempt to influence the 2016 presidential election in favor of Donald Trump [22]. The Russian interference has led to a large number of sensitive emails, including those from the hacked account of Clinton's campaign chairman John Podesta, being released by WikiLeaks [23].

Even if this Russian attack on the DNC computers and the Clinton presidential campaign was not perpetrated against a governmental entity, they demonstrate the national security interest in our elections. With the move from paper ballots and hanging chads, many polling sites in the United States have switched to electronic voting machines. Unfortunately, these machines are quite vulnerable to cyberattacks around the country [24]. Indeed, then-Secretary of Homeland Security Jeh Johnson indicated that the federal government is concerned about such attacks by a foreign government or even terrorist organizations that could be designed to compromise American elections [25]. Malcolm Nance who previously served in the United State Navy as an intelligence officer, characterized these Russians attacks as "a deliberate strategy behind the timing of release of the hacked email" designed to release false information with actual, stolen emails.[31]

The notion that the American government can legislate its way to safety is foolhardy. First, it is unlikely to make us much safer. Apple marketed the iPhone used by Farook in San Bernadino as having the latest innovations in software security. In the end, those innovations were insufficient to prevent the FBI from accessing Farook's cell phone from being hacked by Cellebrite [26]. In other words, the ability to prevent providers from developing flawless security is only as possible as the next hacker. It is like an arms race. Apple and other providers will keep working on improving the security of their phones and operating software. Simultaneously, the best individual hackers as well as companies like Cellebrite will be working on cracking the code.

Second, the American public is unlikely to accept much legislation restricting their privacy in such a draconian manner. The reason that companies like Apple create sophisticated security

[30] *United States v. Wang*, Criminal No. 14–118 (W.D. Pa. May 1, 2014) (Indictment); *see also* [18]

[31] Wheelwright, supra note _.

systems is, in part, because consumers demand it. In this age of identity theft, there is a strong need. No doubt, Apple took the position it did with the FBI over the iPhone used by the San Bernadino shooter because they received significant media attention and publicity. Indeed, Apple has previously assisted law enforcement in criminal investigations that involved accessing cell phones with passwords. Apple is not appearing to be concerned about consumer privacy for its own, but because it is in its best corporate interest if future cell phone purchasers view their products as state of the art. Conversely, members of state and federal legislatures should tread lightly when proposing to limit such technological innovation.

Third, cell phone users have a right to privacy. Indeed, the United States Supreme has determined that police officers must obtain a warrant before search a cell phone because they hold so much personal data.[32] The government should tread lightly when enacting legislation mandating the creation of a backdoor that will enable it to readily invade the privacy of so many people.

## 6 The loss of privacy in financial and health records

The vulnerabilities exposed by the Russian hackers seeking to influence, or to manipulate the 2016 presidential election as well as the federal government's hacking of Farook's cell phone, just reiterate the vulnerabilities that we face in our daily lives. North Korea's hack of Sony Pictures - made for front page news, but its hacks of foreign banks are less well known [27]. The Chinese government was behind a series of hacks of the Federal Deposit Insurance Corporation, which maintains "extremely sensitive internal information at 4,500 banks and savings institutions" [28]. Chinese spies also hacked into the database of the Office of Personnel Management compromising the personal information of about four million former and current federal workers [29]. Even though the United States has signed an agreement to forgo hacking of each other's companies, Chinese spies are still actively targeting American technology and pharmaceutical companies [30].

Hackers are not just threatening trade secrets of large companies, but jeopardize privacy of American consumers. Target, Home Depot, Nordstrom, Michael's, and Nieman Marcus have all been hacked in recent years [31–33]. These hacks not only expose the companies to liability to their customers, but also result in the loss of these customers' personal information [34, 35].

It is not just our personal information and financial records that are vulnerable to hackers. Our health records are also being attacked. In response to the barring from competition of numerous Russian Olympic athletes, hackers released the medical records of American athletes [36, 37]. It is not just Olympic athletes that have cause for concern regarding the security of their personal medical records. Indeed, one hacker was selling over 650,000 patient records containing names, dates of birth, social security numbers, addresses, etc. [38]. Health care insurance providers have been hacked, including over 78 million people with insurance from Anthem and 10 million subscribers to Blue Cross Blue Shield [39, 40]. This type of crime has become more profitable for hackers than credit card information from retailer. In some cases, the insurance information is used by people to obtain surgical procedures that are billed to the actual insured [41].

All of these hacks as well as a myriad of other small measures chip away at individual privacy. The security of our medical records and financial data is in jeopardy, which in turn prevents easy access to capital, or medical care. These are industries - that are continually seeking to acquire highly secured systems for data control and management; secured systems that are so strong, that no one can hack them.

We live in an age in which privacy is diminishing. Some of that is our own doing. For example, the ardent consumers among us will gladly trade personal information in exchange for a couple entitling the holder to a free latte. Nonetheless, we express outrage at revelations of spying by the NSA, but often remain oblivious to the threats that other government surveillance, such as the use of cell site simulators, pose.

## 7 Conclusion

This background and discussion brings us back to the question of whether Apple can create an iPhone so secure that Apple cannot access. Apple is in the business of advancing their technology platforms and associated products. Apple's product security features and its corporate position regarding the dispute over the San Bernadino case are designed to market their iPhones to consumers. In other words, it behooves Apple's marketing department to be able to advertise that not even Apple can access the security of its cell phones - once the owner has configured the security features. This ability appeals - to both savvy criminal professionals, as well as people paranoid of Big Brother's reach, and everyone in between.

It is unclear whether Apple can actually build an impenetrable software and operating system. If you had asked Tim Cook at the end of 2015 whether someone could hack into Farook's cell phone, he likely would have responded, no. He optimistically would have presented that iPhone and operating software as impenetrable, in part because such a feat of hacking would have been extremely difficult for just about anyone and because it was in Apple's best interest from a market perspective to depict its phones and software as impenetrable. Of course, such optimism on his part was overblown as evidenced by the FBI's success in finding someone,

[32] *See Riley*, 134 S. Ct. at 2489–90.

or a group of individuals, who could hack into an iPhone, for a large amount of money.

Regardless of whether Apple can achieve such a feat, why would we want to stop them? In an insecure world, we are probably all better off in having providers that at least attempt to safeguard our secrets. However, we all have an obligation to be better informed about the privacy security risks that we face both from the private sector and the public sector and act accordingly in a responsible manner.

Indeed, the limiting of companies like Apple from developing the best software security just limits individuals' ability to protect their own privacy. It shifts power from the people to the government, which is not the appropriate place for it in the context of who is better suited and more interested in preserving individual privacy concerns.

**Compliance with ethical standards**

**Conflict of interest** I, Brian Owsley, declare that I have no conflict of interest regarding this article.

**Funding** There is no funding source for this article beyond my salary at my institution.

**Ethical approval** This article does not contain any studies with human participants or animals performed by the author.

## References

1. Rubin J, Queally J, Dave P. FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now. Los Angeles Times. 2016. Available at http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.
2. Benner K, Lichtblau E. U.S. says it has unlocked iPhone without apple. N.Y. Times. 2016. Available at http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0.
3. Edwards J. FBI paid more than $1.3 million to break into San Bernardino iPhone. Reuters. 2016. Available at http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.
4. Reisinger D. FBI got useful information off San Bernardino iPhone. Fortune 2016. Available at http://fortune.com/2016/04/20/fbi-san-bernardino-iphone/.
5. Dave P. Apple wants the FBI to reveal how it hacked the San Bernardino killer's iPhone. Los Angeles Times 2016. Available at http://www.latimes.com/business/technology/la-fi-tn-apple-next-steps-20160330-story.html.
6. Schwartz A, Knake R. Government's role in vulnerability disclosure. Harvard Kennedy School. 2016. Available at http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.
7. Welna D. The next encryption battleground: congress. NPR 2016. Available at http://www.npr.org/sections/alltechconsidered/2016/04/14/474113249/the-next-encryption-battleground-congress?utm_campaign=storyshare&utm_source=twitter.com&utm_medium=social.
8. McCarthy K. Europe to push new laws to access encrypted apps data. The Register 2017. www.theregister.co.uk/2017/03/30/ec_push_encryption_backdoors/.
9. Holpuch A. Lavabit loses contempt of court appeal over Edward Snowden encryption keys. The Guardian. 2014. Available at https://www.theguardian.com/technology/2014/apr/16/lavabit-court-ruling-edward-snowden-encryption.
10. Ackerman S. Lavabit email service abruptly shut down citing government interference. The Guardian. 2013. Available at https://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden.
11. Rosenblatt S. Lavabit chief predicts 'long fight' with feds (Q&A). CNET. 2013. Available at https://www.cnet.com/news/lavabit-chief-predicts-long-fight-with-feds-q-a/.
12. Statt N. 1 billion Apple devices are in active use around the world. The Verge 2016. Available at www.theverge.com/2016/1/26/10835748/apple-devices-active-1-billion-iphone-ipad-ios.
13. Costello S. How many iPhones have been sold worldwide? Lifewire. 2017. Available at www.lifewire.com/how-many-iphones-have-been-sold-1999500.
14. Reisinger D. iPhones in use in the US rise to 94M, new study suggests. CNET. 2015. Available at www.cnet.com/news/nearly-100m-iphones-in-use-in-the-us-new-study-shows.
15. Associated Press. Chinese government suspected of hacking into FDIC computers. NBC News 2016. Available at http://www.nbcnews.com/tech/security/chinese-government-suspected-hacking-fdic-computers-n609206.
16. Nakashima E. Chinese hack of federal personal files included security-clearance database. The Washington Post 2015. Available at https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html.
17. Davis JH. Hacking of government computers exposed 21.5 million people. The New York Times. 2015. Available at http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.
18. Press Release, Department of Justice. U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. 2014. Available at https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
19. Sanger DE, Perlroth N. Iranian hackers attack state dept. via social media accounts. The New York Times. 2015. Available at http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.
20. Gorman S. Iran-based cyberspies targeting U.S. officials, report alleges. The Wall Street Journal. 2014. Available at http://www.wsj.com/articles/iran-based-cyberspies-targeting-u-s-officials-report-alleges-1401335072.
21. Perez E, Prokupecz S. How the U.S. thinks Russians hacked the White House. CNN. 2015. Available at http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html.
22. Sanger DE, Schmitt E. Spy agency consensus grows that Russia hacked D.N.C. The New York Times. 2016. Available at http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.
23. Wheelwright G. Entire US political system 'under attack' by Russian hacking, experts warn. The Guardian 2016. Available at https://www.theguardian.com/technology/2016/oct/14/hillary-clinton-email-hack-russia-cybersecurity.
24. Wofford B. How to hack an election in 7 minutes. Politico 2016. Available at http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

25. Davis, JH. U.S. seeks to protect voting system from cyberattacks. The New York Times. 2016. Available at http://www.nytimes.com/2016/08/04/us/politics/us-seeks-to-protect-voting-system-against-cyberattacks.html.
26. Pagliery J. Cellebrite is the FBI's go-to hacker. CNN. 2016. Available at http://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/index.html.
27. Risen T. North Korea linked with hacks stealing from banks. US News & World Report 2016. Available at http://www.usnews.com/news/articles/2016-05-27/north-korea-linked-with-hacks-stealing-from-banks.
28. Pagliery J. China hacked the FDIC – and US officials covered it up, report says. CNN 2016. Available at http://money.cnn.com/2016/07/13/technology/china-fdic-hack/
29. Nakashima E. Chinese breach data of 4 million federal workers. Washington Post 2015. Available at https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.
30. Kharpal A. Is China still hacking US? This cyber firm says yes. CNBC. 2015. Available at http://www.cnbc.com/2015/10/19/china-hacking-us-companies-for-secrets-despite-cyber-pact-.html.
31. Bertrand N. Here's what happened to your target data that was hacked. Business Insider 2014. Available at http://www.businessinsider.com/heres-what-happened-to-your-target-data-that-was-hacked-2014-10.
32. Banjo S. Home depot hackers exposed 53 million email addresses. The Wall Street Journal 2014. Available at http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282.
33. Brenner R. The new front on fraud? Your credit card. CBS News. 2014. Available at http://www.cbsnews.com/news/the-new-front-on-fraud-your-credit-card/.
34. Riley C, Pagliery J. Target will pay hack victims $10 million. CNN. 2015. Available at http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/.
35. Musil S. Home depot offers $19M to settle customers' hacking lawsuit. CNET 2016. Available at https://www.cnet.com/news/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/.
36. Ross B, Ferran L. Cyber 'smear': hackers publish olympians' medical records. ABC News 2016. Available at http://abcnews.go.com/International/anti-doping-agency-russian-hackers-published-athletes-medical/story?id=42063565.
37. Phippen JW. The hack on U.S. olympians' medical records. The Atlantic. 2016. Available at http://www.theatlantic.com/news/archive/2016/09/fancy-bears-russian-olympic-hack/499829/.
38. Storm D. Hacker selling 655,000 patient records from 3 hacked healthcare organizations. Computerworld 2016. Available at http://www.computerworld.com/article/3088907/security/hacker-selling-655-000-patient-records-from-3-hacked-healthcare-organizations.html.
39. Mathews AW. Anthem: hacked database included 78.8 million people. The Wall Street Journal. 2015. Available at http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.
40. Groden C. This big U.S. health insurer just got hacked. Fortune. 2015. Available at http://fortune.com/2015/09/10/hack-health-insurer-bluecross/.
41. Stone J. One in three americans had their health records breached in 2015, as hackers follow the money from retail to medical data. International Business Times 2016. Available at http://www.ibtimes.com/one-three-americans-had-their-health-records-breached-2015-hackers-follow-money-2281011.