****

**9B18E013**

APPLE V. THE FBI[[1]](#endnote-1)

Chris F. Kemerer and Michael D. Smith wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

This publication may not be transmitted, photocopied, digitized, or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e) cases@ivey.ca; www.iveycases.com.

Copyright © 2018, Ivey Business School Foundation Version: 2018-09-10

WHAT KIND OF WORLD DO YOU WANT TO LIVE IN?

On December 2, 2015, Syed Farook and his wife, Tashfeen Malik, attacked Farook’s co-workers at a Christmas party in San Bernardino, California, killing 14 and wounding 22 others. During the subsequent mass-murder investigation, the U.S. Federal Bureau of Investigation (FBI) was able to recover the Apple iPhone 5c that had been issued to Farook by his employer; the phone was running iOS 9—the ninth version of Apple Inc.’s (Apple’s) mobile operating system (iOS). However, Farook had secured the iPhone with a passcode, and anyone who tried to guess it by entering a random code would risk having the phone auto-delete its data after 10 failed attempts.[[2]](#endnote-2)

With no known method to access Farook’s iPhone, the FBI and the U.S. Attorney’s Office for the Central District of California drafted a court order under the *All Writs Act* (AWA)[[3]](#endnote-3) to compel Apple’s technical assistance.[[4]](#endnote-4) The AWA was a legal instrument dating back to 1789 that allowed courts to compel the assistance of a third party when there was no other means to obtain the necessary assistance. Under U.S. law, the FBI needed the consent of a federal judge to require Apple to comply with its AWA request. The court signed the FBI’s order on February 16, 2016,[[5]](#endnote-5) and Apple immediately contested the order. Although Apple, similar to most technology companies, had a policy of co-operating with court orders, Apple argued that the software the government was requesting was a “master key” that could unlock millions of users’ iPhones through a “backdoor.” Using the software would set a dangerous precedent for user privacy going forward.[[6]](#endnote-6)

Tim Cook, Apple’s chief executive officer (CEO), faced numerous challenges. In terms of the FBI order, no matter who won the legal challenge, the loser would appeal, and therefore senior management would likely remain focused on the incident for several years. Beyond this issue, however, Cook needed to determine Apple’s policies regarding security systems in its products and what Apple’s overall relationship was, or should be, with the U.S. government. How much, after all, did customers care about the security of their smartphone data? Could protecting privacy at all costs have public relations implications? Resisting the order meant that Apple could be branded, at best, as unpatriotic, and, at worst, as complicit in terrorist acts against the United States. Would an agreement reached with the U.S. government set a precedent for Apple’s products in overseas markets? And how would Apple’s stance on this issue influence government attempts to pass legislation that might require Apple’s partnership in criminal investigations? These issues needed to be addressed in the context of rapidly evolving technology, which included alternatives to password protection.

Apple’s Security Environment

Apple had been systematically improving the security of its iOS, which ran on devices such as the iPhone and iPad. Apple had evolved its iOS security to the point where the company could no longer routinely circumvent a device’s security for law enforcement for devices running on iOS 8 or later versions.[[7]](#endnote-7) While Apple had clear, justified interests in developing secure devices for its customers, law enforcement also faced growing difficulties in accessing digital evidence in the interest of criminal investigations, public safety, and national security. The FBI referred to this problem as “Going Dark,” and it had been the subject of FBI testimony before U.S. Congress.[[8]](#endnote-8)

The AWA order requested that Apple develop a piece of software—a modified version of its iOS—that would give the government the ability to test passcodes on Farook’s iPhone 5c to find the correct code without risking destruction of the data on the device. The custom software would achieve three functions: (1) allow electronic testing of passcodes, instead of having to enter the passcodes by hand; (2) eliminate any software-induced time delay between passcode attempts; and (3) disable or bypass the feature in iOS 9 that wiped data from the device after 10 unsuccessful passcode attempts. To make the AWA order more acceptable to Apple, the software was to be written incorporating identifiers unique to Farook’s iPhone, and thus built to function on only that specific device.[[9]](#endnote-9) The writ further stipulated that, if Apple desired, Apple could apply the new software to Farook’s iPhone in an Apple facility rather than Apple providing the software to the government.[[10]](#endnote-10)

DIGITAL DEVICE SECURITY

Encryption

Numerous components were involved in creating and preserving digital device security, including, for example, restricting physical access to the device. In the context of the Apple and FBI case, the fundamental security issue was that of *encryption*. Digital encryption was the process of using a computer code to convert digital data so that it could no longer be seen in its original format without entering the code to digitally decrypt it, or convert it back. The ones and zeros that represented information (e.g., text, images, and videos) were converted into a different series of ones and zeros that appeared to no longer represented the original information.

Encryption was done on a computer by inputting the original data into an algorithm that transformed the original input (i.e., “plaintext”) into the converted output (i.e., “ciphertext”).[[11]](#endnote-11) Of course, encryption was sensible only when the algorithm was reversible—that is, when the ciphertext could be decrypted back to its original form. Such an algorithm had value as a security measure only when access to the decryption step could be limited to the owner of the data. Such algorithms required the use of an input (i.e., “a key”) known only to the owner of the data, plus anyone with whom the owner wished to share the key.

Good encryption systems made discovery of the key nearly impossible through the use of so-called “brute force methods”—methods that simply repeatedly made guesses at the key until stumbling upon the one that worked. In a password system such as that on the iPhone, the actual encryption key was generated by a key derivation function—an algorithm that built a complex encryption key from a simpler, user-supplied password.[[12]](#endnote-12) The weakest link in the overall system was users who chose passwords that were too easy to guess.

Modern encryption was done with the use of computers, and cryptographic science had evolved such that very good encryption could be done on easy-to-acquire consumer devices, such as personal computers and smartphones. For example, a cryptosystem developed in 1978 relied on a one-way algorithm involving the product of two very large prime numbers. Such an algorithm was mathematically highly resistant to brute force attempts to decrypt the data.[[13]](#endnote-13) The widespread availability of powerful encryption technology created a dilemma for law enforcement because criminals could use these tools to encrypt their digital data, and law enforcement, without knowing the key, was effectively prevented from reading the data.

Apple iPhone Security[[14]](#endnote-14)

The phone the FBI wanted to access with its AWA order was an iPhone 5c running iOS 9. The phone was owned by the San Bernardino County Department of Public Health, which had provided the phone to Farook, the suspect, to use for work. Farook created a password to lock his iPhone, which posed three barriers for law enforcement: (1) the passcode needed to be entered by hand on the phone itself; (2) the iOS forced a delay after each passcode attempt; and (3) the iOS allowed users to enable an extra security measure that completely deleted the user’s data on the device after 10 incorrect passcode attempts.[[15]](#endnote-15)

Similar to many modern security systems, the Apple operating system combined two pieces of data to prevent unauthorized access. The first was a unique 256-bit advanced encryption standard (AES) secret key that was embedded in the phone when it was manufactured.[[16]](#endnote-16) The second piece of data was a user-chosen password. Since passwords were typically short, Apple protected the device against random guesses by including an optional feature that limited the number of attempts to enter the password. When this limit was exceeded, the correct passcode key was erased, which made the data on the phone permanently inaccessible.

As a part of the process of limiting the number of guesses for a password, the device required approximately 80 milliseconds to process each password attempt. Although this delay would not be noticeable for humans, it effectively prevented computer-generated guessing. Computer security expert Dan Guido noted that, “In terms of cracking passwords, you usually want to crack or attempt to crack hundreds or thousands of them per second. And with 80 milliseconds, you really can only crack eight or nine per second. That’s incredibly slow.”[[17]](#endnote-17) A four-digit passcode (i.e., from 0000–9999) had a maximum of 10,000 unique passwords; random attempts to guess the code would require trying about half of those possibilities. Increasing the passcode to six digits would lead to *1 million* combinations. The number of possible combinations could be greatly increased by including letters in addition to digits. Apple estimated that, without safeguards in place, an all-numeric passcode could be defeated in a few days, whereas a password that accommodated letters could take more than five years. The operating system in the San Bernardino iPhones was set to default to a six-digit passcode, although a user could change this default to an easier to remember (but less secure) four-digit passcode, or to a more secure six-character password.

THE FBI’S REQUEST[[18]](#endnote-18)

The FBI’s request, provided as a signed court order, required that Apple “assist” by providing the FBI with a signed, loadable iPhone software image file. The software, required to work on only the single specific iPhone in question, needed to bypass or disable the auto-erase function, allow the FBI to submit passcodes electronically, and remove the delay between passcode entries.

There was no requirement that the software or iPhone needed to leave Apple’s facilities, and Apple was to advise the government of the reasonable cost of performing these actions.

Early reports created some confusion, which led to the public believing that the court had ordered Apple to unlock the phone.[[19]](#endnote-19) Instead, the FBI wanted to try guessing the password without the risk that the operating system would make the data unreadable, and to be able to do so in a reasonable amount of time. In other words, the FBI wanted to be able to bypass the touch screen so that the password guesses could be generated and entered electronically. To enable this functionality, Apple would need to create a so-called “crippled” version of its operating system that would be less secure, and then install this special software on Farook’s iPhone.[[20]](#endnote-20)

Apple, as a software vendor, required the ability to update software on user phones by delivering a download of new copies of the software when improved versions became available.[[21]](#endnote-21) To prevent malicious parties from installing malware on their customers’ phones, Apple signed its software with a combination of the device’s unique device identifier (UDID) and Apple’s secret, private key, which the phone used to recognize a legitimate upgrade.[[22]](#endnote-22) If a malicious party were to attempt to modify Apple’s software, the key signing procedure would fail without Apple’s private key to sign the software update, and the software would not install on the iPhone. From the FBI’s perspective, the secret key-signing feature of Apple’s software updates, combined with Apple’s ability to code the UDID from Farook’s phone into the modified version of the iOS, would ensure that the crippled version of Apple’s operating system could not be modified to function on any device other than Farook’s phone without Apple’s explicit co-operation.

The FBI also believed that the software it was requesting did not represent a simple “backdoor” into the system because even if Apple did everything asked of them, the FBI’s attempts to randomly guess the password might not work. In particular, if Farook had not accepted the default, four-digit passcode, and instead had protected the phone with the optional six-digit passcode, or, more securely, a password containing both letters and numbers, the FBI would likely be unable to access the data in any reasonable amount of time, even with Apple’s accommodations.

APPLE’S RESPONSE[[23]](#endnote-23)

Apple’s corporate policy, which was typical for technology companies, was to comply with all legal orders to provide information. However, in response to the AWA order, Cook published a “Message to Our Customers,” which started by establishing Apple customers’ need for encryption:

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going. . . .

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

Cook then described the government’s request as mandated hacking:

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers—including tens of millions of American citizens—from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

Cook concluded by describing the government’s approach as “a dangerous precedent”:

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by “brute force,” trying thousands or millions of combinations with the speed of a modern computer.

The implications of the government’s demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone’s device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone’s microphone or camera without your knowledge.

LEGAL ISSUES[[24]](#endnote-24)

In a rare display of unity among otherwise competing technology firms, a brief to Judge Pym in support of Apple’s position was jointly authored by Amazon, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo.[[25]](#endnote-25) The brief made three main arguments: (1) The U.S. federal government was inappropriately overreliant on the AWA and did not have the legal authority to make the requests it had presented to Apple; (2) The request was to defeat security safeguards and was far beyond “non-burdensome technical assistance;” and (3) Construction of software code was enforced speech, which was prohibited by the First Amendment to the U.S. Constitution.[[26]](#endnote-26)

The brief also elaborated a set of dangers for a firm such as Apple if it complied with the court order. In addition to the immediate dangers of lost sales to customers who believed the resulting product was inferior in terms of its security features, if the backdoor key were to fall into the wrong hands, the firm could experience fallout in the future from possible lawsuits, lost customers, and damaged reputation. The firms signing the brief tended to have business models based on the collection of large amounts of customer data. Therefore, they found themselves on the same side as Apple—normally a competitor—given concerns over any growth in government access to their customers’ data.

Statutory Arguments

The AWA stated, “The 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.” As such, the AWA applied only to situations that Congress had not specifically addressed. Apple argued that Congress had passed the specific *Communications Assistance for Law Enforcement Act* (CALEA),[[27]](#endnote-27) whose purpose was to ensure that telecommunications firms could intercept communications when presented with a lawful order to do so. But the CALEA also stated that the government could not mandate the design of telecommunications systems and could not require telecommunications companies to decrypt user data.[[28]](#endnote-28)

A relevant case cited by both parties was a 1977 Supreme Court case involving New York Telephone Co.[[29]](#endnote-29) The court found that the telephone company could be compelled by the government to install a “pen register” to record the phone numbers that were called from a particular phone. Three factors were central to this decision: (1) The government could not compel a third party far removed from the underlying controversy; (2) The company could not be unduly burdened to provide the assistance; and (3) The government must have a necessity to obtain the assistance.

Constitutional Arguments

Apple and the other technology firms that had submitted the brief to Judge Pym then invoked their First Amendment protection to not write the software required to comply with the court order. It had previously been established that being compelled to speak violated the First Amendment’s protection of the freedom of speech; thus, for example, school students could not be required to recite the U.S. Pledge of Allegiance. Other cases had established that computer code (i.e., software) was considered to have the same protections as speech.

OPTIONS AVAILABLE TO APPLE AND OTHER TECHNOLOGY FIRMS

Apple had a variety of technical options available to it going forward. Newer versions of the iPhone (e.g., post-Farook’s 5c model) had a separate computer inside the phone enclosure, called the “secure enclave,” which managed security (see Appendix). Security expert Guido described the options to *Wired* magazine:

There are changes that Apple can make to the secure enclave to further secure their phones. . . . For instance, they may be able to require some kind of user confirmation, before that firmware gets updated, by entering their PIN code . . . or they could burn the secure enclave into the chip as read-only memory and lose the ability to update it [entirely]. . . .

There’s a couple of different options that they have; I think all of them, though, are going to require either a new major version of iOS or new chips on the actual phones. . . . But for the moment, what you have to fall back on is that it takes 80 milliseconds to try every single password guess. And if you have a complex enough password, then you’re safe.[[30]](#endnote-30)

The technical world had already changed to accommodate non-password security technologies.[[31]](#endnote-31) And, ironically, smartphones themselves were now being used as the second factor in two-factor authentication log-in schemes.[[32]](#endnote-32) Thus, smartphones had become even more important, securing not just the data that was on the mobile device itself but also data stored with other Internet-based services. Increasingly, biometrics, such as Apple’s Touch ID fingerprint reader and its Face ID facial recognition system—primarily used to unlock the phone—were being used to access applications (apps) or make point-of-sale payments. If a mobile device were limited to biometric access, then no password entry scheme would be feasible, whether brute force or not.

Apple and other technology firms also needed to consider their relationships with foreign governments, not just with the United States. For example, Apple generated approximately 20 per cent of its sales in China, where its App Store brought in more revenue than its U.S. store.[[33]](#endnote-33) Given the importance of this market, Apple had removed virtual private network (VPN)[[34]](#endnote-34) software from its App Store in China at the request of the Chinese government. Apple also agreed to store its keys for the Chinese version of its iCloud software in China, which, critics argued, would make it easier for the Chinese government to access data stored there.[[35]](#endnote-35) Other technology firms chose a different route abroad from the route that Apple took when confronted with the FBI’s court order in the United States. For example, BlackBerry Limited (formerly Research in Motion Limited, or RIM) provided the Government of India with BlackBerry’s encryptions keys when ordered to do so. BlackBerry chose to comply with the request, despite the report that “Super-secure corporate emails, called BlackBerry Enterprise Services, had traditionally been RIM’s main attraction for companies and corporate executives.”[[36]](#endnote-36)

FUTURE OPTIONS AVAILABLE TO THE GOVERNMENT

Given the increasing importance of digital devices, it was not surprising that forensic evidence, such as that obtained from cellphones, tablets, and other personal electronics, had been increasingly used by law enforcement at all levels, not just in high-profile national cases such as those prosecuted by the FBI (see Exhibit 1). Law enforcement agencies had labs to examine the contents of phones to discover, for example, where the owners were, what they were doing, and whom they were calling or texting immediately before they were the victims or perpetrators of a crime.[[37]](#endnote-37)

But, as security on devices and the use of that security for illegal purposes increased, law enforcement found it increasingly difficult to access data. Further, data access issues were not limited to encrypted personal devices. For example, Microsoft refused to provide the contents of email messages that were located outside of the United States, on a server in Ireland. A New York court upheld Microsoft’s right to not provide the contents—a decision that the Justice Department appealed.[[38]](#endnote-38)

Industry observers criticized U.S. government efforts to pass new legislation that would enhance government access to encrypted data.[[39]](#endnote-39) For example, the proposed *Compliance with Court Orders Act of 2016* would have required any data encrypted by private companies to be decrypted upon request. Experts argued that this requirement would make end-to-end encryption impossible and would weaken the security of America’s technology infrastructure, including how data were transmitted over the Internet. In addition, some noted that the government had the option to acquire data before it was encrypted or could collect metadata, which had been shown to be useful. Finally, some argued that the larger problem might be that law enforcement had not demonstrated that it knew what to do with the data they had previously acquired.[[40]](#endnote-40)

The CALEA was enacted in 1994, and technology had changed significantly in the meantime.[[41]](#endnote-41)Previous FBI director James Comey stated as early as October 2014, that Apple’s new operating system default meant that “the companies themselves won’t be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.”[[42]](#endnote-42)

The government’s position had largely remained the same since the FBI had sought its court order against Apple. The U.S. Justice Department’s deputy attorney general, Rod Rosenstein, gave a speech in October 2017, reiterating the position taken by the previous administration: Companies seemed to have no reason to create encryption that could be breached for a search warrant, and the public bore the consequences. Rosenstein contrasted the companies’ stance on encryption with their other behaviours, including collecting detailed data on their customers and acceding to the requests of foreign governments to remove protections that shielded the data of their citizens from those governments.[[43]](#endnote-43)

COOK’S CHALLENGES

Apple and similar technology firms faced a public relations dilemma: It could be said that if you were not against terrorists and child molesters, then you must be for them.[[44]](#endnote-44) And law enforcement was aware of the power of these arguments. *Wired* magazine reported:

Robert S. Litt, general counsel in the Office of the Director of National Intelligence, predicted as much in an email sent to colleagues three months ago [circa August 2015]. In that missive obtained by the *Washington Post*, Litt argued that although “the legislative environment [for passing a law that forces decryption and backdoors] is very hostile today, it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement. In the story about that email, another U.S. official explained to the *Post* that the government had not yet succeeded in persuading the public that encryption is a problem because “[w]e do not have the perfect example where you have the dead child or a terrorist act to point to, and that’s what people seem to claim you have to have.”[[45]](#endnote-45)

Even without an event as dramatic as the shooting in San Bernardino, Apple faced numerous practical issues at the confluence of technology and public policy. Co-operating with the government would allow Apple both to manage the public relations issues and to be perceived as being on the right side of helping to defend the country against terrorism. However, compliance could set a precedent for future FBI requests, many or most of which could be expected to be less dramatic and might even entangle Apple in disputes between competing government political factions, such as the FBI’s involvement with the 2016 U.S. presidential election. In addition, Apple’s co-operation with the U.S. government could have a chilling effect on worldwide iPhone sales, especially if Apple’s main competitor, Google with its Android phones, was seen as less susceptible to such requests. However, thinking longer term, co-operating in this specific case could forestall momentum for new legislation that would require technology companies to design their systems in such a way as to be able to provide the government with whatever data they requested. Such legislation would likely constrain the design space for future devices and, therefore, potentially limit innovation and future sales. Weighing all these factors made Cook’s choice of the next steps difficult and certain to be criticized.

APPENDIX: Security through Cryptography

Cryptography, or literally, “hidden writing,” was a practice going back hundreds of years whose purpose was to represent information in a way that only selected readers could read.1 It was typically described as “scrambling” ordinary text (also referred to as plaintext or cleartext) into ciphertext. This scrambling was referred to as *encryption*, and the process of converting it back into ordinary text was *decryption*.

Although cryptography existed long before the invention of the computer, the addition of computing resources made the tasks of both encryption and decryption easier and more powerful. In addition, with computers themselves becoming a standard storehouse of information, the desire to limit access to this information led to the creation of barriers by using cryptography. Access to computer systems was commonly limited by passwords that were known only to the owner of the data, and potentially to system administrators.

The design of such systems inevitably involved trade-offs among characteristics such as ease of use versus vulnerability to unintended access. For example, passwords that were shorter or easier to remember also tended to be easier for others to observe or to guess. Changing passwords on a frequent basis could improve their security, but made legitimate access more difficult. In addition, systems could be designed to allow other trusted parties to access the system even when they were not the owner of the data.

Modern encryption systems were based on what were referred to as “public key” systems. Earlier systems used what were termed symmetrical keys, meaning that the secret input to encrypt the information was the same secret input required to decrypt it. This functionality created a security problem: how to ensure parties who legitimately required the key had access to it, while at the same time keeping the key out of the hands of those not entitled to have it.

With public key systems, the key to encrypt the data differed from the key to decrypt it. Therefore, the owner of the information could distribute the encryption key widely (the “public key”) so long as the decryption key was kept “private.” The mathematics behind these systems was based on prime numbers, whereby owners choose two large prime numbers as their private keys, multiplied them together, and published only the product of multiplying the two numbers as their public key. Even with modern computing power, the process of attempting to discover the multiplicand and the multiplier of a very large product of two prime numbers (e.g., a number on the order of 10308) was not solvable in a practical time period.2

Systems such as the iPhone had trade-offs. Users primarily wanted to restrict access to their phones, so they protected their phones with an access method known or possessed only by the user, such as a password. But users also had an interest in allowing Apple to access their individual phones to, for example, update the phone’s software or operating system with new releases. For this access to work, Apple needed to possess a key that would allow it access to all iPhones without needing to know anyone’s individual password.

Apple described the security steps it took to provide software updates to its users’ phones using this key:

Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware. When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM [read-only memory]. This immutable code, known as the hardware root of trust, is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA [certification authority] public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel. This secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices.3

Appendix (continued)

Ongoing technological advances have continued to advance the nature of securing data on a mobile device. Newer iPhones, sold after Farook’s model 5c, were equipped with what was called a “secure enclave,” a feature described as “a separate computer inside the iPhone that broker[ed] access to encryption keys,” and thus improved the security of the keys.4 The feature created longer delays between password guesses and increased those delays after each failed attempt. The delay before the last guess was one hour. The FBI included this information in its application to the court; however, Farook’s phone was an earlier model that did not have the secure enclave software delay.5

Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (New York, NY: Random House Anchor Books, 1999).

2Ibid.

3 Apple Inc., *iOS Security: iOS 9.3 or Later*, May 2016, accessed August 1, 2018, www.apple.com/ca/business/docs/iOS\_

Security\_Guide.pdf.

4 Ibid.

5 Kim Zetter, “Apple’s FBI Battle Is Complicated. Here’s What’s Really Going On,” *Wired*, February 18, 2016, accessed June 27, 2018, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on.

Source: Created by authors.

Exhibit 1: New York County District Attorney’s Office—Evidence gathered from Apple Smartphones, October 2014–January 2016

|  |  |
| --- | --- |
| **Top criminal charge** | **Percentage** |
| Larceny, forgery, cybercrime, and identity theft | 36.4 |
| Drugs and narcotics | 18.1 |
| Sex crimes | 16.0 |
| Assault, robbery, and burglary | 13.9 |
| Homicide and attempted murder | 7.0 |
| Weapons charge | 4.6 |
| Other | 4.0 |
| TOTAL | 100 |

Source: New York County District Attorney’s Office, “Smartphone Encryption and the Impact on Crime Victims,” (presentation, April 18, 2016), slide 6, accessed June 27. 2018, www.manhattanda.org/wp-content/themes/dany/files/

4.18.16%20Victim%20Organizations%20Presentation.pdf.

Endnotes

1. This case has been written on the basis of published sources only. Consequently, the interpretation and perspectives presented in this case are not necessarily those of Apple Inc. or any of its employees. [↑](#endnote-ref-1)
2. Kim Zetter, “Apple’s FBI Battle Is Complicated. Here’s What’s Really Going On,” *Wired*, February 18, 2016, accessed June 27, 2018, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on. [↑](#endnote-ref-2)
3. *All Writs Act*, 28 U.S.C. §1651 (1789). [↑](#endnote-ref-3)
4. Zetter, op. cit. [↑](#endnote-ref-4)
5. Order Compelling Apple, Inc. to Assist Agents in Search, *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 35KGD20*, U.S. District Court for the Central District of California, ED 15-0451M, February 16, 2016, accessed June 27, 2018, www.justice.gov/usao-cdca/file/825001/download. [↑](#endnote-ref-5)
6. Apple Inc., “A Message to Our Customers,” February 16, 2016, accessed June 27, 2018, www.apple.com/customer-letter. [↑](#endnote-ref-6)
7. New York County District Attorney’s Office, “Smartphone Encryption and the Impact on Law Enforcement,” February 2016, accessed August 1, 2018, http://ndaa.org/pdf/Smartphone\_Encryption\_and\_the\_Impact\_on\_Law\_Enforcement8-4-15.pdf; Apple Inc., “We Believe Security Shouldn’t Come at the Expense of Privacy, accessed August 1, 2018, www.apple.com/

   privacy/government-information-requests/. [↑](#endnote-ref-7)
8. James Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” (remarks prepared for delivery at the Brookings Institution, Washington, DC, October 16, 2014), accessed June 27, 2018, www.brookings.edu/wp-content/uploads/2014/10/10-16-14-Directors-Remarks-for-Brookings-Institution-AS-GIVEN.pdf. [↑](#endnote-ref-8)
9. Each iPhone contained a unique 64-bit electronic chip identification (ECID) assigned in hardware, which Apple could incorporate into the modified version of the iOS to ensure that the software functioned only on Farook’s device. [↑](#endnote-ref-9)
10. Order Compelling Apple, Inc. to Assist Agents in Search, op. cit. [↑](#endnote-ref-10)
11. Orin S. Kerr and Bruce Schneier, “Encryption Workarounds,” *Georgetown Law Journal* 106, no. 4 (2018): 989–1019. [↑](#endnote-ref-11)
12. Matthew Green, “Why Can’t Apple Decrypt Your iPhone?,” *A Few Thoughts on Cryptographic Engineering* (blog), October 4, 2014, accessed June 27, 2018, https://blog.cryptographyengineering.com/2014/10/04/why-cant-apple-decrypt-your-iphone. [↑](#endnote-ref-12)
13. Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (New York, NY: Random House Anchor Books, 1999). [↑](#endnote-ref-13)
14. Zetter, op. cit. [↑](#endnote-ref-14)
15. “Apple Can Comply with the FBI Court Order,” *Trail of Bits Blog*, February 17, 2016, accessed January 22, 2018, https://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order. [↑](#endnote-ref-15)
16. Green, op. cit. [↑](#endnote-ref-16)
17. Zetter, op. cit. [↑](#endnote-ref-17)
18. Order Compelling Apple, Inc. to Assist Agents in Search, op. cit. [↑](#endnote-ref-18)
19. Zetter, op. cit. [↑](#endnote-ref-19)
20. In an attempt to keep the phone forensically sound without altered data, the FBI wanted Apple to design this special operating system and install it into the phone’s memory rather than upload the data onto a disk. [↑](#endnote-ref-20)
21. Apple Inc., *iOS Security: iOS 9.3 or Later*, May 2016, accessed August 1, 2018, www.apple.com/ca/business/docs/iOS\_Security\_Guide.pdf. [↑](#endnote-ref-21)
22. See the Appendix for a description of public and private keys in cryptography. [↑](#endnote-ref-22)
23. Apple Inc., “A Message to Our Customers,” op. cit. [↑](#endnote-ref-23)
24. Felix Wu, “No Easy Answers in the Fight over iPhone Decryption,” *Communications of the ACM* 59, no. 9 (2016): 20–22. [↑](#endnote-ref-24)
25. Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp and Yahoo in support of Apple, Inc., *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 35KGD20*, U.S. District Court, Central District of California, ED No. CM 16-10 (SP), March 22, 2016, accessed June 27, 2018, www.documentcloud.org/documents/2746916-Amazon-Cisco-Dropbox-Evernote-Facebook-Google.html. [↑](#endnote-ref-25)
26. First Amendment to the U.S. Constitution, Legal Information Institute, accessed June 28, 2018, www.law.cornell.edu/constitution/

    first\_amendment. [↑](#endnote-ref-26)
27. *Communications Assistance for Law Enforcement Act*, 47 U.S.C. §1001-1010 (1994). [↑](#endnote-ref-27)
28. Comey, op. cit. [↑](#endnote-ref-28)
29. *United States v. New York Telephone Co*., 434 U.S. 159 (1977). [↑](#endnote-ref-29)
30. Zetter, op. cit. [↑](#endnote-ref-30)
31. Robert McMillan, “Tech Firms Push toward a Future without Passwords,” *Wall Street Journal*, February 8, 2016, accessed January 22, 2018, www.wsj.com/articles/tech-firms-push-toward-a-future-without-passwords-1454977631. [↑](#endnote-ref-31)
32. Two-factor authentication was an extra layer of security that required not only the typical password and username required by most systems but also a second factor that only the user possessed. This second factor could be a piece of information that only the user should know (e.g., the answer to a security question, such as “What is the first name of your best friend?”) or a physical token. A common physical token was the user’s smartphone. [↑](#endnote-ref-32)
33. Li Yuan, “‘Shame on Apple’: Consumers Want Apple to Stand Up to China’s Censors,” *Wall Street Journal*, August 3, 2017, accessed January 23, 2018, www.wsj.com/articles/as-apples-services-grow-in-china-so-does-its-censorship-risk-1501752605 . [↑](#endnote-ref-33)
34. VPNs created a virtual network (not a separate physical network) that could protect online data by keeping access to it private to the other members of the virtual network. VPNs could be used by dissidents or others to prevent government access to their communications. [↑](#endnote-ref-34)
35. Robert McMillan and Tripp Mickle, “Apple to Start Putting Sensitive Encryption Keys in China,” *Wall Street Journal*, February 24, 2018, accessed March 6, 2018, www.wsj.com/articles/apple-to-start-putting-sensitive-encryption-keys-in-china-1519497574. [↑](#endnote-ref-35)
36. Joji Thomas Philip, “BlackBerry Maker Research in Motion Agrees to Hand Over Its Encryption Keys to India,” *Times of India*, August 2, 2012, accessed January 22, 2018, https://timesofindia.indiatimes.com/business/india-business/BlackBerry-maker-Research-in-Motion-agrees-to-hand-over-its-encryption-keys-to-India/articleshow/15323093.cms. [↑](#endnote-ref-36)
37. Shannon Prather, “Minnesota Detectives Crack the Case with Digital Forensics,” *Minneapolis Star Tribune*, October 6, 2014, accessed January 25, 2018, www.startribune.com/when-teens-went-missing-digital-forensicscracked-case/278132541. [↑](#endnote-ref-37)
38. Brent Kendall, “Supreme Court to Consider Search Warrant Power in Microsoft Email Case,” *Wall Street Journal*, October 16, 2017, accessed January 23, 2018, www.wsj.com/articles/supreme-court-to-consider-search-warrant-power-in-microsoft-email-case-1508167554. [↑](#endnote-ref-38)
39. Juli Clover, “Senate Draft Encryption Billed Called ‘Absurd,’ ‘Dangerous,’ and ‘Technically Inept,’” MacRumors, April 8, 2016, accessed January 23, 2018, www.macrumors.com/2016/04/08/senate-draft-encryption-bill-dangerous. [↑](#endnote-ref-39)
40. Kim Zetter, “After Paris Attacks, Here’s What the CIA Director Gets Wrong about Encryption,” *Wired*, November 16, 2015, accessed January 22, 2018, www.wired.com/2015/11/paris-attacks-cia-director-john-brennan-what-he-gets-wrong-about-encryption-backdoors. [↑](#endnote-ref-40)
41. Comey, op. cit. [↑](#endnote-ref-41)
42. Ibid. [↑](#endnote-ref-42)
43. Del Quentin Wilber, “Justice Department to Be More Aggressive in Seeking Encrypted Data,” *Wall Street Journal*, October 19, 2017, accessed January 23, 2018, www.wsj.com/articles/justice-department-to-be-more-aggressive-in-seeking-encrypted-data-1507651438; Josh Chin, “Apple Removes Apps That Allowed China Users to Get around Filters,” *Wall Street Journal*, July 29, 2017, accessed January 23, 2018, www.wsj.com/articles/apple-removes-apps-that-allowed-china-users-to-get-around-filters-1501341653. [↑](#endnote-ref-43)
44. Comey, op. cit. [↑](#endnote-ref-44)
45. Zetter, “After Paris Attacks, Here’s What the CIA Director Gets Wrong About Encryption,” op. cit. [↑](#endnote-ref-45)