Ivey | Publishing

W16245

BUILDING A "BACKDOOR" TO THE IPHONE: AN ETHICAL DILEMMA[1]

Tulsi Jayakumar and Surya Tahora 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.

In February 2016, Tim Cook, Apple's chief executive officer (CEO), took a stance on a matter that drew strong public debate. Involving Apple's flagship product, the iPhone, the debate pitted on either side of the fence proponents of two rights.[2] On the one side were Apple and digital rights groups advocating protection of customer digital privacy, while on the other were the U.S. government and the Federal Bureau of Investigation (FBI) seeking support from Apple and from other technology companies in protecting national security.

Specifically, the U.S. government and the FBI sought and demanded Apple's help in unlocking the iPhone of a terrorist involved in a terrorist attack in San Bernardino, California. The phone, which had been recovered from the slain terrorist, was expected to provide vital insights into the motives of the attack, as well as to provide crucial evidence regarding terrorist networks and activities. The FBI demanded that Apple build a "backdoor" to the terrorist's iPhone — essentially, a new version of its iPhone operating system (iOS) software — that could help FBI agents unlock the phone and access the information on it as a one-off case. Cook, however, refused to acquiesce to the government's demand, citing Apple's commitment to customer digital privacy and security.

Was Cook justified in his refusal to heed the U.S. government's demand to build a one-time access to the iPhone retrieved from the terrorist on grounds of protecting customer digital privacy? Was Apple's obligation to protect customer privacy greater than its obligation to contribute to national security? What dilemmas did Cook and the Apple management team face in this decision? How could the dilemmas be resolved?

APPLE'S IPHONE AND IOS

Steve Jobs and Steve Wozniak, both college dropouts, founded Apple Computers, Inc. (Apple) in 1976 with a vision to make small, user-friendly computers to be used in homes and offices. Apple's initial products — Apple I and Apple II — revolutionized the computer industry. The company's sales increased from US$7.8 million[3] in 1978 to $117 million in 1980, the year Apple went public.[4] In 1990, the company posted its highest profits yet; however, the company's market share waned after this peak.

Jobs, who had left the company in 1985, rejoined it in 1997.[5] Apple subsequently launched a host of products, which included personal computers (iMac), portable digital music players (iPod), mobile communication and media devices (iPhone and iPad), various related services and software (iOS, iTunes Store, and iCloud), and ancillary products (Apple TV and Apple Watch).[6] However, the iPhone, accounting for two-thirds of Apple's revenue in 2016, was Apple's flagship brand — the brand that contributed to Apple gaining and maintaining its status as the world's most valuable brand through the period 2011 to January 2016.[7]

The first iPhone was launched on June 29, 2007, in a 4- and 8-gigabyte version. Apple's mobile revolution, however, could be credited to creation of the iOS (previously iPhone OS) — a mobile operating system. Apple initially developed the iOS in 2007 and distributed it for the iPhone and iPod Touch. Apple developed later versions of the iOS to support other devices such as the iPad and Apple TV. By Q3 2015, Apple had sold more than 1.1 billion iOS devices.[8] As of June 2015, Apple's App Store contained more than 1.5 million available iOS-based applications,[9] which had been collectively downloaded more than 100 billion times.[10]

Apple provided major updates to the iOS operating system approximately once a year. The update most recent to the "backdoor issue" was iOS 9, released on September 16, 2015. As of February 8, 2016, 77 per cent of devices were using iOS 9, 17 per cent were using iOS 8, and the remaining 6 per cent were using earlier operating systems.[11]

In the fiscal quarter ending December 2015, Apple experienced a slowdown in its sales. The iPhone, as well as other Apple products, exhibited weak performance. Sales of the iPhone grew by less than 1 per cent year-on-year, compared to a 50 per cent growth in the previous year. Unit sales of the iPad tablet fell 25 per cent from the previous year, and sales of iMac computers fell by 4 per cent.[12] Even so, Apple's faith in its flagship product, the iPhone, remained strong. Cook maintained that the popularity of the iPhone provided the company with a "long-lasting foundation."[13]

CUSTOMER PRIVACY AND APPLE

Apple's business model was based on selling products, not harvesting data. This business model was unlike others in the industry, such as Google's, which generated revenue through targeted ads developed with the assistance of harvested data. Cook had long been a champion of customer privacy. Speaking at a technology conference in 2010, Cook made his views on customer privacy clear: "[Apple] has always had a very different view of privacy than some of our colleagues in the [Silicon] Valley." Thus, after building a feature into the iPhone that showed where the phone and its user were located, the company, citing customer privacy, left the choice of whether to use this feature entirely to users, who could control whether apps were able to use the phone's location data.[14]

The increasing use of iPhones as a store of personal information, and consumer sensitivity regarding the potential use and abuse of personal information, prompted Cook to take a hard stance on customer privacy. The matter came to a head in June 2013 following revelations of massive U.S. government surveillance, exposed by Edward Snowden, a former Central Intelligence Agency (CIA) employee and U.S. government contractor. Called Prism, the surveillance system — essentially a counter-terrorism data collection effort launched in 2007 — "allowed the U.S. National Security Agency (NSA) to receive emails, video clips, photos, voice and video calls, social networking details, logins, and other data held by a range of U.S. Internet firms,"[15] which included Apple.[16]

More specifically, Snowden's disclosures included revelations that questioned the ability of Apple products to withstand tampering and ensure customer privacy. It appeared that the CIA had, for more than a decade, tampered with Apple products, embedding spy tools in the hardware and modifying Apple software updates in order to collect data about app developers and carry out systematic surveillance of their customers. Irate Apple customers wrote to Cook, expressing concerns regarding Apple's commitment and ability to ensure users' privacy.[17]

Meanwhile, the Internet and social media were being increasingly used to plan and coordinate international terror attacks and to "spread propaganda, incite violence, and attract new recruits."[18] The use of secret, private chat rooms and encrypted Internet message boards prompted the advent of surveillance programs like Prism. In a world faced with growing threats of terrorism, Apple and other technology companies faced increased pressure from law-enforcement agencies to share information about their customers and devices. Justifying Prism, President Obama stated, "You can't have 100 per cent security and also then have 100 per cent privacy and zero inconvenience."[19] Technology companies, especially Apple, viewed information-sharing requests as compromising customer security and privacy.

One of the ways technology companies like Microsoft, Yahoo, Facebook, and Apple handled the conflicting dimensions of the government requests was to share with the public (to the extent allowed under the law) the details and scope of the government's periodic requests.[20] For instance, Apple disclosed that, in the first six months of 2015, it had received between 750 and 999 national security-related requests from the U.S. government, affecting 0.00673 per cent of Apple's customers.[21]

Nonetheless, customers remained concerned, and in response, Apple implemented increasingly stringent encryption measures.[22] Until iOS 6, only resident Apple apps were encrypted by default; developers of third party applications had to opt in to encryption. By 2013, however, Apple had taken measures to ensure that third party application data was also protected. With iOS 7, Apple began "encrypting all third party data stored on customers' phones by default, until [customers] first unlocked [the phone] after rebooting."[23] When the company designed iOS 8, it ensured that even its own engineers would be unable to extract data from the mobile phones and tablets.[24]

In an open letter to Apple customers in September 2014, Cook reiterated Apple's concern regarding privacy: "Security and privacy are fundamental to the design of all our hardware, software, and services, including iCloud and new services like Apple Pay."[25]

He added:

> Our business model is very straightforward: We sell great products. We don't build a profile based on your email content or web browsing habits to sell to advertisers. We don't "monetize" the information you store on your iPhone or in iCloud. And we don't read your email or your messages to get information to market to you. Our software and services are designed to make our devices better. Plain and simple.[26]

Addressing the issue of trust, Cook stated, "Our commitment to protecting your privacy comes from a deep respect for our customers. We know that your trust doesn't come easy. That's why we have and always will work as hard as we can to earn and keep it."[27]

THE SAN BERNARDINO BOMBING AND APPLE

On December 2, 2015, a married couple, Syed Rizwan Farook, 28, and Tashfeen Malik, 29, shot at and killed 14 people and injured 22 at the Inland Regional Center in San Bernardino, California. The victims were employees of the San Bernardino health department who had gathered for a holiday party in a conference room at the centre, which provided services to disabled people. The FBI stated it had evidence that the attack was based on "extensive planning" and that it was investigating the attack as an act of terrorism.[28] Farook was an inspector with the county health department and had left the party in progress, returning with his wife to shoot at his co-workers. The couple were later killed in a gun battle with the police. The terror group Islamic State of Iraq and the Levant (ISIS or ISIL) claimed that the two slain suspects were supporters of the group.

A key focus of the investigation involved checking the couple's phone, travel, computer, and other records to ascertain the motive behind the attack and to determine the reasons for the makeshift bomb lab found in the couple's rented home.[29] The shooters had tried to destroy any evidence that could track their digital footprints. Their computer's hard drive was missing, and the authorities found two relatively new cellphones lying smashed in a garbage can near the shooting scene.[30] However, an iPhone, provided to Farook by his employer, was found in the vehicle in which the couple had been killed in the aftermath of the attack.[31]

The iPhone was not Farook's property but that of his employer, San Bernardino County, which consented to a search of the phone,[32] but the investigators feared that the data stored on the iPhone would be completely and permanently erased in their attempts to unlock the phone. The FBI sought Apple's assistance in the days following the attack, and Apple "provided data that was in [its] possession, complied with valid subpoenas and search warrants . . . made Apple engineers available to the FBI to advise them, and offered [its] best ideas on a number of investigative options at their disposal."[33] However, the FBI wanted Apple to go a step further. It sought Apple's assistance in unlocking the encrypted iPhone used by Farook. The FBI wanted Apple to build what became known as "a backdoor" to the iPhone. Talks between lawyers of the Obama administration and Apple went on for two months,[34] but in the end, Apple refused to acquiesce to the FBI's demand.

THE GOVERNMENT'S STANCE

A dispute had been building between the U.S. government and technology companies for more than a decade regarding the latter's encryption practices. In 2010, the Obama administration proposed draft legislation that would have forced technology companies like Google and Apple to provide unencrypted data to the government. The draft legislation was similar to the legislation forced on phone companies during the Clinton administration, which made it mandatory for such companies to build digital networks that government agents could tap. If the new draft legislation was accepted as law, it would have been a blow to customer privacy activists. However, the Snowden disclosures in 2013 led to a large-scale criticism of the U.S. government, and the Obama administration decided not to move on the proposed legislation.[35]

The San Bernardino case proved to be a flashpoint in the dispute. The U.S. government stated that it would "attempt to exhaust every investigative lead in the case," since it owed resolution to the victims and their families. Consequently, when the talks between the government lawyers and Apple failed, the U.S. Justice Department filed an application in the Federal District Court for the District of Central California to "learn everything possible about the attack in San Bernardino."[36]

Federal prosecutors, in their initial filing, stated:

> The government requires Apple's assistance to access the . . . device to determine, among other things, who Farook and Malik may have communicated with to plan and carry out the IRC shootings, where Farook and Malik may have travelled to and from before and after the incident, and other pertinent information that would provide more information about their and others' involvement in the deadly shooting.[37]

Prosecutors further claimed that Farook's device could be encrypted to the point that its content would be "permanently inaccessible" and that "Apple has the exclusive technical means which would assist the government in completing its search."[38]

Based on this request, a U.S. Federal Court judge passed an order directing Apple to provide "reasonable technical assistance" to the FBI. Such assistance was to be in the form of software that could disable the security features that erased data from the iPhone after 10 unsuccessful attempts to unlock the phone.[39] If the security feature was disabled, the investigators could attempt as many combinations as necessary to unlock the phone.

APPLE'S STANCE

Apple's position on customer privacy was largely driven by its chief executive officer, Tim Cook. Cook, who joined Apple as a senior executive in 1998 and worked largely as a behind-the-scenes executive, had evolved to become one of the most outspoken corporate executives in recent times.

Tim Cook

Cook took charge as Apple's CEO in October 2011. Since then, he had spoken out on various issues pertaining to human rights and corporate responsibility toward the environment, society, and employees, even if some of the initiatives adversely affected the corporate bottom line. This approach to leadership was in keeping with Cook's values and personal principles, which could be discerned from his commencement address to the graduating class of George Washington University in May 2015. Cook's speech referred to justice and injustice, outlining his opinion that personal values did not exist independently of the workplace: "It's about finding your values, and committing to them. It's about finding your North Star. It's about making choices. Some are easy. Some are hard. And some will make you question everything."[40]

Cook also referred to his choice to keep his values out of his work sphere until he joined Apple. It was at that point, Cook claimed, that he realized the practice of treating work as work and keeping values out of it left him "feeling adrift and rudderless, like Apple [before Steve Jobs rejoined Apple]."[41]

Exhorting the young graduates not to remain silent and passive observers, Cook said, "The sidelines are not where you want to live your life. The world needs you in the arena. There are problems that need to be solved. Injustices that need to be ended. People that are still being persecuted."[42]

Cook believed in the maxim "To whom much is given, much is required." He was aware of his own responsibility to give back, especially since, by his own admission, he had "been given a lot."[43]

In 2014, Cook revealed that he was gay, acknowledging that his desire for personal privacy had held him back from disclosing until then.[44] Apple's annual report on suppliers and working conditions for its factory workers, published under Cook's leadership, was a first-of-its-kind initiative, signifying the new culture of openness at Apple. Further, under Cook, Apple undertook non-business initiatives, including some environmental initiatives, which were criticized by investors.[45] Cook defended these initiatives in a shareholder meeting, saying that Apple should do things because "they're just and right."[46] He believed he was merely representing Apple's long-standing culture of caring for these issues, even if these issues had not previously been openly discussed. Cook proclaimed, "You want to be the pebble in the pond that creates the ripple for change."[47]

As a CEO, Cook laid great importance on cultural fit, going so far as firing a senior team member who did not fit with Apple's culture. Additionally, the culture itself was being changed, slowly and subtly. Cook, unlike Jobs, believed in sharing the limelight with his senior leaders. Again, unlike Jobs, who dismissed corporate philanthropy, Cook advocated it and encouraged employee giving. The company was becoming more open and transparent under Cook than it had been under the publicity-seeking Jobs.[48]

Despite criticism that Cook would be unable to replicate Job's magic, Apple continued to innovate. Under Cook's direction as CEO, the Apple Watch was launched in March 2015, and the company's financials remained "fundamentally sound,"[49] with its split-adjusted stock price increasing from $54 in August 2011, when Jobs died, to $126 in March 2015.[50] Its market capitalization was above $700 billion — double that of companies like Exxon Mobil and Microsoft. Apple was the first company to cross that level. Its cash management record under Cook was also enviable. Thus, despite distributing $92.6 billion in dividends and buybacks under Cook, Apple's cash reserves, at more than $150 billion, were still triple the level of 2010.[51] However, since July 2015, its stock prices had been going down, dropping from $126 in March 2015 to $96.76 on February 25, 2016.[52] In fact, in February 2016, share prices of Alphabet — Google's parent company — rose by 3 per cent. The resultant higher market capitalization led Alphabet to displace Apple as the world's "most valuable public company," a title it had held since 2011.[53]

Was there a contradiction between Cook's various commitments — to himself, his shareholders, his employees (as a company leader), and to the larger society beyond Apple's boundaries?

Cook's Customer Letter

Apple responded to the federal court order with a 1,100-word open letter written by Cook to Apple customers, outlining why Apple refused to acquiesce to the government's demands.[54] Cook's letter warned of the "chilling" breach of privacy posed by the government's demands, "undermining the very freedoms and liberty our government is meant to protect." Cook described the government's demands as a case of "overreach by the U.S. government."[55] The key points, which expressed Apple's stance, included the following:[56]

- The U.S. government asked Apple to create something (i.e., a backdoor to the iPhone) the company "simply [did] not have" and "something [it] considered too dangerous to create."
- The software (a version of the iOS) that the FBI wanted Apple to create for one iPhone (the Bernardino terrorist's phone) — software did not exist as of that day — "would have the potential to unlock any iPhone in anyone's physical possession."
- There was no guarantee that the use of the backdoor would be limited to the given case. "Once created, the technique could be used over and over again, on any number of devices." Apple referred

to the backdoor as the equivalent of a master key in the physical world, "capable of opening hundreds of millions of locks."
- The building of a backdoor would defeat the very purpose of encryption. "Once the information for unlocking the encrypted data [was] known, or a way to bypass the code was revealed, the encryption could be defeated by anyone with that knowledge."
- Apple had worked hard to put customer data out of "even . . . our own reach, because we believe that the contents of your iPhone are none of our business."
- Apple faced an ethical dilemma in that "the government was asking it to hack its own users and undermine decades of security advancements that protected its customers from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect Apple users would, ironically, be ordered to weaken those protections and make [its] users less safe."

Ultimately, Apple's refusal to "comply with the court orders, despite the technical feasibility of doing so," was viewed as "based on its concerns for its business model and public brand marketing strategy."[57]

THE DIRTY-HANDS PROBLEM

The dilemma faced by Cook and by Apple's management team — people with power and complex responsibilities — could be characterized as "the dirty-hands problem." The expression was used by Badaracco, an ethics professor at Harvard University, to refer to the hard, moral choices involving the "right-versus-right" dilemmas faced by management.[58] As stated by Badaracco, "The moral dilemmas of management are, at bottom, clashes among different, conflicting moralities, among very different spheres of responsibility."[59]

The Four Spheres of Managers' Commitment

The Commitments of Private Life: At an individual level, in the sphere of their private lives, managers were committed to abstract, universal principles, such as telling the truth and avoiding injuries to others. The morality of private life differed from person to person, shaped by factors varying from "religious beliefs [to] philosophy, literature, the lives of people they admired, or the convictions born of their own lives and reflections."[60]

The Commitments of Economic Agents: A second sphere of managers' moral claims, in their role as economic agents, was to serve the interests of shareholders and maximize their wealth.

The Commitments as Company Leaders: Another sphere of responsibility existed because managers, as company leaders, shaped the lives and welfare of human beings employed within those companies.[61]

Responsibilities Beyond the Firm's Boundaries: Managers also had responsibilities toward people and organizations outside their own firm's boundaries, since "companies had complex relationships with government agencies, labour unions, or — through strategic alliances — with customers, suppliers, and even competitors."[62]

As a framework for assessing resolution of right-versus-right dilemmas, Badaracco recommended four questions:

- Which course of action will do the most good and the least harm?

- Which alternative best serves others' rights, including shareholders' rights?
- What plan can I live with, which is consistent with the basic values and commitments of my company?
- Which course of action is feasible in the world as it is? [63]

The first question had to do with consequences. Attributed to John Stuart Mill, the moral decision was one that resulted in the greatest good to the greatest number of people, with the least cost, risk, and harm.

The second question focused on rights. For Americans, this question, which was attributed to Thomas Jefferson's draft of the Declaration of Independence, was one of human rights to life, liberty, and the pursuit of happiness. Thus, when business executives considered various ways of resolving a dilemma, they were required to consider the various rights at stake.

The third question, with its roots in Aristotle's philosophy and in several religions, had to do with the interplay of conscience and values. Business executives, faced with "wrenching situations," would ask themselves "what course of action they could live with, as individuals and leaders of a particular company."[64]

The fourth question was attributed to the father of modern political theory, Niccolo Machiavelli, and was pragmatic in its approach. In his own writing on the subject, Badaracco stated:

> In any situation, there may be several options that could, in theory, reconcile the competing claims. The crucial question then becomes: What is actually feasible — in view of a manager's actual power in an organization; a company's competitive, financial, and political strength; the likely costs and risks of various plans of action; and the time available for action?[65]

Apple was given five days to respond to the federal court order. What were the moral dilemmas facing Cook, and how would he choose to address them? Which was right: favouring customer privacy or favouring national security and the right to live in a world increasingly threatened by international terrorism that operated across the seamless borders afforded by digital technology? How should Cook handle this "right-versus-right" problem? Would his decision to safeguard his clients' digital privacy become a defining moment for Cook, the chief executive officer of the world's hitherto most valuable company?

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 or any of its employees.
[2] Joseph L. Badaracco, Jr., "Business Ethics: Four Spheres of Executive Responsibility," *California Management Review* 34, no. 3 (Spring 1992): 64–79. The word "right" has been used in its sense of "morally good, justified or acceptable." According to Badaracco, management decisions often involve conflicts of "right versus right, of responsibility versus responsibility" and not issues of right versus wrong. Throughout the case, "right" is used in this sense.
[3] All currency amounts are in U.S. dollars unless otherwise specified.
[4] Angelique Richardson and Ellen Terrell, "Apple Computer, Inc.," Library of Congress Business Reference Services, April 2008, accessed February 19, 2016, www.loc.gov/rr/business/businesshistory/April/apple.html.
[4] Richardson and Terrell, op. cit.
[6] To understand how the company introduced a range of innovative products after 1976, see The Apple Timeline, www.theappletimeline.com, accessed February 21, 2016.
[7] "The World's Most Valuable Brands," *Forbes*, accessed April 6, 2015, www.forbes.com/powerful-brands/list. On February 2, 2016, Google's Alphabet, with a market cap of $547.1 billion, overtook Apple, with a market cap of $529.3 billion, to become the world's most valuable public company; Ari Levy, "Google Parent Alphabet Passes Apple Market Cap at the Open," CNBC.com, February 2, 2016, accessed February 19, 2016, www.cnbc.com/2016/02/01/google-passes-apple-as-most-valuable-company.html.
[8] Evan Niu, "How Many iOS Devices Has Apple Sold?" Motley Fool, November 16, 2015, accessed February 21, 2016, www.fool.com/investing/general/2015/11/16/ios-devices-sold.aspx.
[9] Sam Costello, "How Many Apps Are in the App Store?" About Tech*,* September 10, 2015, accessed February 21, 2016, http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm.
[10] "Cumulative Number of Apps Downloaded from the Apple App Store from July 2008 to June 2015 (in Billions)," Statista, accessed February 21, 2016, www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store.
[11] Developer App Store, Apple, accessed February 21, 2016, https://developer.apple.com/support/app-store.
[12] Brett Howse, "Apple Reports Q1 FY2016 Results: Record Revenue Despite Flat iPhone Sales," AnandTech*,* January 26, 2016, accessed February 17, 2016, www.anandtech.com/show/9991/apple-reports-q1-fy-2016-results-record-revenue-despite-flat-iphone-sales.
[13] Katie Benner, "Apple Says Sales of iPhones Have Slowed, "*New York Times*, January 26, 2016, accessed February 17, 2016, www.nytimes.com/2016/01/27/technology/apple-earnings-iphone-sales.html. During this quarter, however, revenue from Apple services grew by 26 per cent, and that from a category known as "other products" — which included the Apple Watch — increased by 62 per cent.
[14] Katie Benner and Nicole Perlroth, "How Tim Cook, in iPhone Battle, Became a Bulwark for Digital Privacy," *New York Times*, February 18, 2016, accessed April 5, 2016, www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html.
[15] Leo Kelion, "Q & A: NSA's Prism Internet Surveillance Scheme," BBC.com, June 25, 2013, accessed February 21, 2016, www.bbc.com/news/technology-23027764.
[16] Other firms involved in this surveillance scheme included Microsoft and its Skype division, Google and its YouTube division, Yahoo, Facebook, AOL, and PalTalk (a lesser-known chat service owned by AVM Software).
[17] Benner and Perlroth, op. cit.
[18] See Adam Goldman and Lara Jakes, "Online Forums Provide Key Havens for Terror Plots," *Times of Israel*, August 15, 2013, accessed April 5, 2016, www.timesofisrael.com/online-forums-provide-key-havens-for-terror-plots; Dan Rivers, "How Terror Can Breed Through Social Media," CNN.com, April 28, 2013, accessed February 19, 2015, http://edition.cnn.com/2013/04/27/world/rivers-social-media-terror.
[19] Kelion, op. cit.
[20] Ibid.
[21] "We Believe Security Shouldn't Come at the Expense of Individual Privacy," Apple, accessed February 21, 2016, www.apple.com/in/privacy/government-information-requests.
[22] Encryption referred to encoding information so that only people with the key to un-encode the information could read it. Encrypted phones could be unlocked with the passcode used to unlock the phone on its home screen. Some phones, including newer iPhones, also included a secure computer chip that carried a key-in hardware. Apple was the first major smartphone producer to make encryption an option, beginning with the iPhone 3. Encryption became the default as of the release of the iPhone 5. Elizabeth Weise, "What Does It Mean that a Phone is Encrypted?" *USA Today*, February 20, 2016, accessed February 21, 2016, www.usatoday.com/story/tech/news/2016/02/20/phone-encryption-iphone-apple-qa/80623208.
[23] Henry Hoggard, "Privacy, Enterprise, and Security Changes in iOS 7," MWR Infosecurity, November 23, 2013, accessed February 20, 2016, www.mwrinfosecurity.com/our-thinking/privacy-enterprise-and-security-changes-in-ios-7.
[24] Benner and Perlroth, op. cit.
[25] Mikey Campbell, "Tim Cook Touts New Apple Privacy Policies in Open Letter to Customers," Apple Insider, September 17, 2014, accessed February 21, 2016, http://appleinsider.com/articles/14/09/17/tim-cook-touts-new-apple-privacy-policies-in-open-letter-to-customers.
[26] Campbell, op. cit.
[27] Ibid.

[28] "What Investigators Know About the San Bernardino Shooting," *New York Times*, December 10, 2015, accessed February 21, 2016, www.nytimes.com/interactive/2015/12/02/us/california-mass-shooting-san-bernardino.html.
[29] Faith Karimi, Jason Hanna, and Yousuf Basil, "San Bernardino Shooters 'Supporters' of ISIS, Terror Group Says," CNN.com, December 6, 2015, accessed February 18, 2016, http://edition.cnn.com/2015/12/05/us/san-bernardino-shooting.
[30] Karimi, Hanna, and Basil, op. cit.
[31] Kevin Johnson and Jessica Guynn, "Apple Ordered to Break into San Bernardino Shooter's iPhone," *USA Today,* February 17, 2016, accessed February 21, 2016, www.usatoday.com/story/tech/news/2016/02/16/apple-san-bernardino-iphone-magistrate-order/80478844.
[32] Johnson and Guynn, op. cit.
[33] Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, accessed February 17, 2016, www.apple.com/customer-letter.
[34] Eric Lichtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone," *New York Times*, February 17, 2016, accessed February 18, 2016, www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.
[35] Lichtblau and Benner, op. cit.
[36] Johnson and Guynn, op. cit.
[37] Mike Levine, Jack Date, and Jack Cloherty, "DOJ Escalates Battle with Apple Over San Bernardino Shooter's Phone," ABC News.com, February 19, 2016, accessed February 21, 2016, http://abcnews.go.com/US/doj-escalates-battle-apple-san-bernardino-shooters-phone/story?id=37056775.
[38] Levine et al., op. cit. Apple phone systems had a function that automatically erased the access key and rendered the phone permanently inaccessible after 10 failed attempts.
[39] Kim Zetter, "Apple's FBI Battle is Complicated: Here's What's Really Going On," *Wired*, February 18, 2016, accessed February 24, 2016, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on.
[40] Dylan Tweney, "Apple CEO Tim Cook Tells Graduates: Values and Justice Belong to the Workplace," Venture Beat, May 17, 2015, accessed February 24, 2016, http://venturebeat.com/2015/05/17/apple-ceo-tim-cook-tells-graduates-values-and-justice-belong-in-the-workplace.
[41] Tweney, op. cit.
[42] Ibid.
[43] Adam Lashinsky, "Apple's Tim Cook Leads Different," *Fortune*, March 26, 2015, accessed February 24, 2016, http://fortune.com/2015/03/26/tim-cook.
[44] Timothy Donald Cook, "Tim Cook Speaks Up," *Bloomberg,* October 31, 2014, accessed February 19, 2016, www.bloomberg.com/news/articles/2014-10-30/tim-cook-speaks-up.
[45] Benner and Perlroth, op. cit.
[46] Ibid.
[47] Lashinsky, op. cit.
[48] Ibid.
[49] Ibid.
[50] Split-adjusted stock prices referred to the share prices after adjusting for stock splits over the company's lifetime. This process facilitated an accurate comparison between the historical and current stock prices. Each time a stock was split, the cost of a single share went down. Hence, share prices had to be adjusted appropriately to reflect true performance.
[51] Lashinsky, op. cit.
[52] "Apple Inc. (AAPL)," Yahoo! Finance, accessed February 26, 2016, https://in.finance.yahoo.com/echarts?s=AAPL#symbol=AAPL;range=.
[53] Ari Levy, "Google Parent Alphabet Passes Apple Market Cap at the Open," CNBC.com, February 2, 2016, accessed February 19, 2016, www.cnbc.com/2016/02/01/google-passes-apple-as-most-valuable-company.html.
[54] Cook, op. cit.
[55] Ibid.
[56] Ibid.
[57] This was the view expressed by the government in its filing to the federal court. Levine et al., op. cit.
[58] Badaracco, op. cit.
[59] Badaracco, op. cit., 66.
[60] Badaracco, op. cit., 66–67.
[61] Badaracco, op. cit., 70.
[62] Badaracco, op. cit., 72.
[63] Badaracco, op. cit., 75.
[64] Badaracco, op. cit., 76.
[65] Badaracco, op. cit., 76.