HARVARD | BUSINESS | SCHOOL

9-316-069

REV: NOVEMBER 29, 2017

HENRY MCGEE

NIEN-HÊ HSIEH

SARAH MCARA

Apple: Privacy vs. Safety (A)

We believe that people have a fundamental right to privacy. The American people demand it, the constitution demands it, morality demands it.[1]

— Tim Cook, Apple CEO

Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families.[2]

— Cyrus Vance, Manhattan district attorney

On September 9, 2015, Tim Cook, CEO of technology behemoth Apple, took to the stage in front of 7,000 people at San Francisco's Bill Graham Civic Auditorium to kick off the debut of the company's highly anticipated new product range. The lineup included the iPhone 6S, successor to the iPhone 6, the world's best-selling smartphone.[3] Introduced the year before to rave reviews,[4] the iPhone 6 had a key feature that enflamed a debate between privacy advocates and law enforcement officials around the globe. The phone's operating system (OS), iOS 8, employed a default encryption system that prevented Apple, as well as law enforcement authorities, from accessing customer data on the device without permission.

Apple's enhanced data security measures came against a backdrop of heightened debate about privacy following the 2013 revelation of clandestine U.S. surveillance programs. National Security Agency (NSA) contractor Edward Snowden had revealed that the NSA was collecting private data stored by telecommunications (telecom) and Internet companies. Many citizens were shocked by the operation's scale, and several foreign leaders were outraged to discover the NSA had tapped their cellphones to monitor private and official conversations. However, numerous law enforcement officials defended the surveillance as a key weapon in the fight against crime and international terrorism.

Many praised Apple's decision to employ stronger encryption in iOS 8. "It's heartening," one industry observer commented, "to see a major American company conclude that it's a business advantage to protect its users' privacy and security."[5] But law enforcement officials were deeply critical. James Comey, Director of the Federal Bureau of Investigation (FBI), observed, "Encryption isn't just a technical feature; it's a marketing pitch. . . . Sophisticated criminals will come to count on these

Senior Lecturer Henry McGee, Professor Nien-hê Hsieh, and Associate Case Researcher Sarah McAra (Case Research & Writing Group) prepared this case with the assistance of Associate Director Kerry Herman (Case Research & Writing Group). This case was developed from published sources. Funding for the development of this case was provided by Harvard Business School and not by the company. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?"[6] Comey and officials worldwide called for an encryption key that would allow law enforcement to bypass security measures, known as a backdoor.

Despite these demands, in 2015, Apple introduced additional security enhancements. The company's new operating system, iOS 9, included two-factor authentication[a] and boosted the length of the passcode users had to enter to access their devices from four digits to six. Immediately, industry publication *Computerworld* observed that "the move to longer passcodes is not likely to please U.S. authorities, who have expressed fears that stronger security measures, including encryption, may make it more difficult to obtain information for time-sensitive investigations, such as terrorism."[7]

The increasingly heated debate raised a number of issues for Cook. Was there a way that Apple could meet both the privacy needs of customers and the access demands of law enforcement? If Apple provided limited access for U.S. authorities, how should the company respond to requests from other governments, especially those with records of human rights violations? And if Apple worked with law enforcement, would the company lose consumer trust and market share?

Apple

Apple designed, manufactured, and sold consumer electronics hardware, software, and services. Established in 1976 as a manufacturer of personal computers, by 2001, Apple's portfolio had grown significantly. In 2015, its primary products were Apple TV, Apple Watch, the iPad, iPhone, and iPod, and a range of desktop computers and laptops. Software included the operating systems iOS (mobile devices) and OS X (computers and laptops). The iTunes store, Apple Music, iCloud storage, and mobile payment tool Apple Pay rounded out its offerings. In 2014, Apple sold a record 243 million iOS devices, including 169 million iPhones, and posted a profit of $39.5 billion on net sales of $182 billion. The iPhone accounted for 56% of net sales.[8] (See **Exhibits 1** and **2**.) In 2015, Apple manufactured 15% of smartphones shipped globally, but accounted for 92% of the industry profit.[9] (See **Exhibit 3**.)

Apple had over 400 retail locations in 16 countries, and 62% of net sales were international.[10] The company was headquartered in Cupertino, California, and had locations throughout Europe, China, Singapore, and Japan. Its data centers were housed in the U.S., and as of 2014, it owned a manufacturing facility in Cork, Ireland. The majority of Apple's hardware was manufactured by Asian outsourcing partners; as Apple inscribed on its hardware, "Designed by Apple in California. Assembled in China."

Apple fiercely competed with Google in many markets. Founded in 1998, Google, a California-based Internet company, offered products and services in nearly every country. In addition to its popular search engine, which was available in over 100 languages, Google's products and services included a web browser, e-mail service, cloud storage, mobile payment system, and an autonomous car. Google partnered with hardware manufacturers to develop the Google Nexus smartphone line, and Google's Android OS, launched in 2008, dominated the market: in 2014, 81% of total global smartphone shipments and 52% of tablet shipments ran on Android.[11] In 2014, 89% of Google's $66 billion in revenue came from advertisers, and 57% of total revenue was earned overseas.[12]

[a] Two-factor authentication allowed a user to combine two components to verify her identity. On iOS 9, the components were the user's passcode and a unique verification code automatically sent to another device the user had registered with Apple.

Tim Cook

In 1998, Apple co-founder and then-interim CEO Steve Jobs convinced Cook to join Apple to improve the company's manufacturing system. At the time, Apple was recovering from record losses and undertaking a major product restructuring. Originally from a small town in Alabama, Cook had an undergraduate degree in Industrial Engineering from Auburn University, an MBA from Duke University, and years of experience working at IBM and Compaq Computer.[13] Cook's practical work style complemented Jobs's more idealistic outlook.[14] Cook became chief operating officer (COO) in 2005, and in 2011, Jobs named Cook his successor as CEO. Under Cook, Apple introduced new products and achieved a record-breaking $700 billion market capitalization in 2015.[15] (See **Exhibit 4**.)

Cook also pushed Apple into the public arena, and the company took strong stances on issues ranging from data privacy to lesbian, gay, bisexual, and transgender (LGBT) nondiscrimination. "We believe that a company that has values and acts on them can really change the world," Cook said. "There is an opportunity to do work that's infused with moral purpose."[16] At an annual shareholder meeting in 2014, Cook told Apple shareholders that if they cared only about return on investment and disagreed with Apple's focus on multiple stakeholders, they "should get out of the stock."[17]

Edward Snowden

In June 2013, news broke of extensive U.S. government clandestine surveillance operations. Snowden released documents to the press revealing that the NSA was collecting records of phone calls and data transmissions within the U.S. and between the U.S. and other countries from telecom providers, such as AT&T and Verizon. Documents also exposed NSA programs, called PRISM, that allowed intelligence agencies to collect data from Internet companies, such as Google and Facebook, using a variety of technical means. PRISM gave the government front-door access to consumer data by legally compelling nine Internet companies to disclose specific content and metadata[b] for national security purposes upon request. Some companies challenged PRISM, including Yahoo!, which took the issue to court.[18] MUSCULAR, jointly operated by the U.K.'s intelligence service, allowed the NSA to collect content and metadata from network connections at a company's private data centers without the company's knowledge. While most Internet exchanges occurred over encrypted data transmission protocols—primarily Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS)—data exchanges on companies' private servers often were not encrypted.[19] The government had access to a plethora of data, including searches, chat messages, real-time e-mail and chat events (e.g., logging in), e-mails, social media posts, video conferences, and file transfers.[20]

Snowden, who watched the news unfold from Hong Kong, was admonished as a traitor by some and hailed as a hero by others. Days after the leaks, U.S. prosecutors filed criminal charges against him, one for theft of government property and two under the Espionage Act.[21] In August 2013, after many failed attempts to seek asylum around the world, he was granted temporary asylum by Russia.[22]

Industry Fallout and Response

American technology (tech) companies were caught in the tumultuous wake of the Snowden revelations. Cisco Systems saw a drop in customers, especially outside the U.S., in part because the revelations "caused a number of customers to pause and reevaluate" working with an American

[b] *Metadata* was data about data; it was the information generated from using technology, such as the date and time a user made a call or his location when he connected to Wi-Fi. Content was the data sent over the technology, such as the text of a message.

company.[23] In China, Qualcomm and Hewlett-Packard reported a decline in late 2013 sales,[24] and state media accused Apple of giving Chinese users' data to U.S. intelligence agencies.[25] Brazil switched from Microsoft Outlook for e-mail to a domestic company with local data centers,[26] while its lawmakers proposed responsive legislation. One estimate placed the three-year cost to the American cloud computing industry at $35 billion as customers switched to other providers.[27] A number of non-U.S. companies stepped in to attract concerned customers; some marketed their services as NSA-resistant and insisted they would not share user data with other companies or governments.[28]

Following the NSA revelations, surveys found that the majority of Americans did not feel "very secure" using many forms of communication, including landlines, cellphones, and e-mail.[29] In 2015, 25% of survey respondents reported having changed their use of technology as a result of the revelations, and 74% believed they should not have to give up privacy and freedom in exchange for safety (up from 60% in 2004).[30] Only 55% of users were satisfied with their phones' security features.[31]

People around the world had willingly disclosed data to companies in exchange for convenience or financial savings but were increasingly wary of how businesses—and the government—used their data.[32] One study found that consumers in India, the Middle East, and China and Hong Kong were most willing to trade data for improved services, while German and Canadian consumers were least willing.[33] Beyond written and voice communications, users relied on phones for important tasks such as accessing information about health conditions, making purchases, or banking online.[34] In Europe, consumers trusted hospitals, banks, and the government to protect their data more than social media sites, retailers, and tech companies.[35] (See **Exhibits 5a** and **5b** for consumer attitudes.) Over 50% of respondents to a global survey had experienced a data breach,[36] yet many people expected companies and governments to secure their data and did not actively protect their own data: 62% did not change passwords regularly and 39% did not use a password to protect their mobile devices.[37] Attitudes toward government use of online data and surveillance varied by country (see **Exhibits 6a** and **6b**).

American tech companies, determined to protect their reputations and improve their privacy policies, denied allegations of giving the government direct access to their servers. In December 2013, senior executives from major tech and telecom companies, including AT&T, Yahoo!, Apple, Twitter, Google, and Facebook, met with U.S. President Barack Obama to discuss the consequences of the NSA programs for the industry.[38] Companies started to invest in greater privacy controls and a range of improved security measures. Google accelerated plans to encrypt traffic between its data centers.[39] In 2014, IBM announced a plan to invest over $1 billion to build a data center outside the U.S. to assure non-U.S. customers that the U.S. government could not access their data.[40] Apple planned a $1.9 billion investment to build two data centers in Europe, which some speculated were for similar reasons.[41]

In addition, a number of companies increased the reporting of data requests they received from governments around the world.[42] Initially, the FBI limited the scope of information about data requests companies could release, but in early 2014 the companies reached an agreement with the U.S. Department of Justice to expand the disclosures of requests.[43] (See **Exhibits 7a** and **7b**.) Some companies took the additional step of informing customers when their data was disclosed due to a request.

U.S. Legal Landscape

Many national laws and international treaties, such as the Universal Declaration of Human Rights, guaranteed people a level of privacy. (See **Exhibit 8**.) In the U.S., the Fourth Amendment of the Constitution gave a reasonable expectation of privacy regarding Americans' "persons, houses, papers,

and effects."[44] Law enforcement officials were required to persuade a judge of probable cause of criminal activity to conduct search and seizures for evidence.

In the late twentieth century, U.S. legislation sought to translate the right to privacy to evolving technologies and the growing volume of private digital data. (See **Exhibit 9** for a description of the laws.) One set of laws governed criminal investigations (i.e., the Wiretap Act and the Electronic Communications Privacy Act [ECPA]) and delineated a telecom provider's role in enabling surveillance (i.e., the Communications Assistance for Law Enforcement Act [CALEA]). Another governed national security investigations and foreign communications (i.e., the Foreign Intelligence Surveillance Act [FISA]) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [USA PATRIOT Act]). At the same time, heightened cybersecurity threats pressed legislators and corporations to find ways to protect consumers', companies', and governments' data and information systems.

Criminal Investigations

Critics charged that surveillance laws for criminal activity were outdated, pointing to conflicting court rulings on law enforcement's right to access digital data.[45] Some ruled that data voluntarily shared with a third-party provider was no longer private (e.g., a number dialed on a phone was shared with the phone company), while others ruled that e-mails stored on a third-party provider's server should have privacy protections and thus require a search warrant.[46] In June 2014, the Supreme Court ruled that law enforcement officials must obtain a warrant to search a suspect's cellphone.[47] Chief Justice John Roberts wrote in the court's opinion, "The fact that technology now allows an individual to carry such [private] information in his hand does not make the information any less worthy of the protection for which the Founders fought."[48] He continued, "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. . . . Privacy comes at a cost."[49]

National Security

Power to collect communication content for national security investigations was greatly expanded under the USA PATRIOT Act, enacted shortly following the terrorist attacks in the U.S. on September 11, 2001, and extended by subsequent legislation. Section 215 of the act was the legal authority used for the bulk collection of domestic phone metadata. It allowed the FBI to issue National Security Letters (NSLs)—extraordinary search orders that did not require judicial review—to compel companies to disclose their business records pertaining to a user and forbade companies from revealing a request had been made.[c] Section 702 of the FISA Amendments Act of 2008 made the PRISM program possible by empowering the Foreign Intelligence Surveillance Court to issue broad authorization for the collection of vast quantities of Internet traffic from major Internet companies. The government strongly maintained the necessity of the procedures. "[M]y assessment and my team's assessment was that they help us prevent terrorist attacks," President Obama explained shortly after the Snowden leaks. "You can't have 100% security and also 100% privacy and zero inconvenience."[50]

Cybersecurity

Government officials and companies also grappled with the increasing threat of cyberattacks, both from state and non-state actors. Experts estimated the global cost of cybercrime to be over $400 billion.[51]

[c] Apple was one of the first major companies to use a "warrant canary" for NSLs. The company's 2013 transparency report stated that Apple had never received an order under Section 215. The statement did not appear in the following years' reports, presumably indicating that the company had since received such a request but was prohibited from saying so.

In 2014, cybercriminals stole the personal information of an estimated 40 million people in the U.S., 54 million in Turkey, 20 million in China, and millions more worldwide. (See **Exhibit 10** for major cyberattacks.) In 2015, cyber-economic espionage—hacking into companies to access trade secrets—was also on the rise in the U.S.[52] Tech experts nearly universally recommended strong encryption as a necessary tool to prevent cyberattacks. Given the lack of comprehensive legislation for cybersecurity (the last act was passed in 2002), in July 2014, legislators proposed a new cybersecurity act, but critics feared it would compromise citizens' privacy protections.[53] (Refer to **Exhibit 9**.)

Consumer Protection

With few laws in place, the Federal Trade Commission (FTC), which was responsible for consumer protection in the U.S., had "been the *de facto* privacy and security regulator in the U.S."[54] Though the FTC did not regulate digital security, it did offer recommendations for protecting data.[55] Between 2002 and 2014, the FTC cited 47 companies for poor data security measures.[56]

Encryption

Strong encryption was considered a crucial tool for securing data. By converting data into an unreadable form that only the intended recipient could read, encryption both protected data in transit and at rest, and allowed a recipient to verify the identity of a sender. Many Internet companies relied on public key encryption, a tool based on a system of public and private keys,[d] to protect consumer data. (See **Exhibit 11** for an explanation of public key encryption.) Public key encryption was the cryptography behind SSL/TLS sites; service providers generated and held the keys.

Apple was one of the few large companies that developed both encrypted hardware and encrypted messaging services.[57] Beginning with iOS 3 and the iPhone 3GS released in 2009, all iPhones used a form of full-disk encryption (i.e., all data on a disk drive). However, these early encryption tools were easily breakable if Apple (or adversaries) had access to the physical device. In 2011, Apple enhanced security measures with default end-to-end encryption, a type of public key encryption, for its iMessage service. These keys were generated and held by the devices on both ends of the exchange, not with the service provider; only the sender and recipient had the keys to access the content of the messages.

Apple's decision to make full-disk encryption the default on iOS 8, which was compatible with iPhone 4S models or later, was the culmination of improved encryption measures over the years. Apple no longer retained a "master key" to the devices. When a user created a passcode (or setup Touch ID to unlock a device with a fingerprint), the passcode was combined with a unique key stored on the device's memory to create a new encryption key. Apple could not access this data without the passcode. A hacker could attempt to find a bug in the encryption algorithm or guess the passcode, but the process could take a long time and might never be fruitful.[58] Without the ability to access consumer content or communications, Apple officials reasoned, the company would not have to fight off subpoenas or other attempts by the government to access data. "If law enforcement wants something, they should go to the user and get it," explained Cook. "It's not for me to do that."[59]

The company declared, "For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted [including photos, messages (including attachments), and e-mail] are protected by an encryption key

[d] A public key was shared with everyone; it was only used to encrypt, not decrypt, data, so that nothing was compromised if it was intercepted. A private key was unique to one user; it was needed to decrypt messages and was never sent to anyone else.

that is tied to the user's passcode, which Apple does not possess."[60] (See **Exhibit 12** for the data Apple could access.) By September 2015, 41% of Apple devices used iOS 8 and 52% used iOS 9.[61]

Apple's rival Google had been among the first tech companies to add default encryption to some services. In 2010, the company made encryption a default setting on Gmail, its e-mail service; in 2011, on searches; and in 2013, on Cloud Storage. On September 18, 2014—the day after Apple's introduction of iOS 8—Google announced that the next generation of Android devices (Android Lollipop) would have default full-disk encryption. (Encryption measures for communication protocols were determined by each application.) However, in March 2015, the company revised its decision: "due to performance issues," Google now required hardware manufacturers to build devices that supported encryption, which the user could choose to enable, but did not mandate encryption as the default.[62]

As Google's position on encryption underscored, consumer desires and cryptographic best practices did not always coincide. End-to-end encryption programs had been available for many years, but they were not widely used by the general public.[63] One observer wrote that encryption was "intrinsically complex,"[64] and early options typically required user setup. Non-tech-savvy consumers often did not know encryption tools were available. Security features could also compromise performance; full-disk encryption, for instance, slowed every computer process to some extent. For many modern, fast technologies, the effect was negligible, but encryption measures noticeably reduced performance on low-cost commodity devices, as demonstrated by Google's Android phones.[65]

Company Locks and Government Keys

The broad implementation of end-to-end and full-disk encryption by Apple and Google ignited concerns among investigators. FBI Director Comey, along with many government officials around the world, argued that companies should grant law enforcement access to encrypted devices and communications through a backdoor, a technology embedded in a product that allowed them to bypass encryption to access data with encryption keys held in escrow until needed. (See **Exhibit 13** for encryption techniques.) Comey cited the precedent set in other laws that required companies to give government officials technical assistance in the surveillance of communications.[66] However, one such law stated a service provider was not responsible for decrypting certain data. (See **Exhibit 9**.)

Around the globe, official stances on encryption and backdoor access varied. In the U.K., Prime Minister David Cameron pressed for legislation for backdoors, asking, "In extremis, it has been possible to read someone's letter, to listen to someone's call. . . . The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not."[67] In 2015, Chinese officials were considering counterterrorism laws that would mandate backdoor access. Yet in Germany, the government supported end-to-end encryption measures that two leading e-mail providers launched in 2015. As the interior minister said, "Germany wants to take a leading role in the use of digital services. Encryption is an important precondition for this."[68] Greece and Austria were among other countries that promoted the use of strong encryption.[69]

Criminal Investigations

U.S. local law enforcement encountered encrypted devices in many ordinary investigations, since the majority of criminal cases were filed and adjudicated in state courts.[70] From October 2014 to June 2015, the Manhattan district attorney's office could not access potential evidence from 74 of the 92 cases involving iPhones running iOS 8,[71] though privacy advocates noted that this was a negligible fraction of the 100,000 cases the office saw each year.[72] Nonetheless, Manhattan District Attorney Cyrus Vance and legal officers from the U.S. and Europe penned an op-ed in the *New York Times*, writing, "We

support the privacy rights of individuals. But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. The safety of our communities depends on it."[73] In August 2015, Comey and Deputy Attorney General Sally Quillian Yates testified before the Senate's judiciary and intelligence committees on the matter: "When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we . . . may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods."[74]

Cook noted that law enforcement had other ways to access relevant data, such as obtaining metadata from telecom providers or using data stored on backup computers or in the cloud.[75] Indeed, one cybersecurity expert argued that the Internet enabled "the golden age of surveillance" by making massive amounts of data and metadata available to collect and analyze.[76] But that was not always possible. In murder cases, Vance said, a passcode "effectively died with the victim."[77] U.S. law enforcement might not be able to compel a suspect to reveal his passcode if it would violate his Fifth Amendment right against self-incrimination.[78] Not all customers had this protection, though: In many countries, including the U.K. and Australia, law enforcement could legally compel a citizen to disclose a password or encryption key. (See **Exhibit 14** for examples of key disclosure laws.)

National Security

Comey warned, "We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted."[79] The head of the U.K.'s NSA equivalent said that Apple and other companies had "become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us."[80] Comey referred to ongoing investigations into the Islamic State of Iraq and the Levant (ISIL) to demonstrate the importance of monitoring digital communications: "ISIL operators in Syria [are] recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders."[81]

"The notion that we would market devices that would allow someone to place themselves beyond the law troubles me a lot," Comey said. "As a country, I don't know why we would want to put people beyond the law. That is . . . sell an apartment that could never be entered even by law enforcement."[82] Yet, as one observer countered, "The Fourth Amendment does not entitle law enforcement to regulate the manufacture of locks."[83] Still others worried that if the U.S. government demanded access to secured data, other governments would likely follow suit. As a former Yahoo! executive said, "Once we open the door an inch for the U.S. government, there are a number of countries that want to kick that door open. Once you give up that high ground for the U.S., then it's a matter of companies deciding which countries get what they want. Or don't."[84] Cautioned the *Guardian*, "It was Google's lawful interception backdoor that let the Chinese government raid the Gmail account of dissidents."[85]

Cybersecurity

Creating a backdoor would not be technologically difficult for companies such as Apple. Protecting the key(s), however, would be a significant challenge. As one cryptography expert wrote,

> [A]ny backdoor Apple might design would likely require the company to store some sort of master access key—or even . . . one for every phone it sells. . . . [T]hese keys might need to be carefully transported from the factory in China, to a locked and guarded room

> at Apple HQ in Cupertino, California. They would be kept isolated from the Internet to protect them from hackers, and Apple would have to constantly monitor its own employees to prevent abuse. None of this is cheap, and the stakes are high.[86]

"National security always matters," Cook explained not long after the launch of the iOS 9 privacy enhancements. "But the reality is that if you have an open door in your software for the good guys, bad guys get in there, too."[87] Hackers would target these keys and, a group of computer scientists warned, "if *any* of the private escrowing keys are *ever* compromised, then *all* data that *ever* made use of the compromised key is permanently compromised."[88]

Cybersecurity experts stressed that no backdoor for one government could be fully protected from others. According to the *Guardian*, "It was the lawful interception backdoor in Greece's national telephone switches that let someone—identity still unknown—listen in on the Greek Parliament and prime minister during a sensitive part of the [2004–2005] Olympic bid."[89] Peter Swire, a member of President Obama's Review Group on Intelligence and Communications Technology, asked, "How much trust would India place in its communications in the hands of Pakistan, China in the hands of Taiwan?"[90] He continued, "Think about important communications in the hands of the country you trust least in the world. That is the Internet that would result from limits on strong encryption."[91] The result, according to industry leaders, "would be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes."[92]

Business

"It is important to get the balance right between privacy, security, maintaining user trust and the cost to industry,"[93] the head of the U.K. Internet industry body ISPA explained. The business implications of weakened encryption policies were unknown. One tech executive wondered, "Do we lose 90% of our business in Germany? Or 20%? No idea."[94] In testimony before the House of Representatives in April 2015, one expert explained, "[F]oreign customers will not want to buy or use online services, hardware products, software products or any other information systems that have been explicitly designed to facilitate backdoor access for the FBI or the NSA."[95] American companies said they would consider creating two different products or services—one for Americans and one for foreigners—if faced with a backdoor policy from the U.S. government.[96]

Observers worried that U.S. officials in 2015 had forgotten the outcome of the Crypto Wars of the 1990s, when the government sought escrow keys from companies to gain backdoor access into encrypted products. At the time, American companies could not export products with strong encryption since encryption had primarily been used for military and intelligence purposes and therefore was considered "munition."[97] By the end of the 1990s, due to a seminal court decision in 1992 and pressure from the tech industry and privacy advocates, the White House abandoned the idea of key escrow and removed all restrictions on encryption exports.

Some critics, however, felt that Apple could face severe financial liabilities by not complying with data requests. In July 2015, a U.S. senator proposed that crime victims should be able to sue a company if its encrypted devices allowed a user to commit the crime. He explained, "Corporations [are] privatizing value and socializing cost," and proposed that a liability system would bring back a balance of responsibility.[98] Legal experts speculated about how such a liability case could play out: "[M]anufacturers may be liable if a product's risk outweighs its benefits. . . . A jury might conceivably conclude that it was negligent, particularly in light of Comey's repeated warnings, for Apple not only not to include a work-around [for encryption]—even if that work-around also created risks—but to

bombastically eliminate the ones it has used for years in a specific attempt to make itself law-enforcement proof."[99]

Privacy at Apple

Cook stressed the importance of protecting consumer data and stated that "privacy and security are built into every one of our products and services from their inception."[100] In 2015, Apple received a top rating from a digital rights organization in its report on privacy and transparency practices regarding government access to user data, an award only 9 of the 24 major tech companies earned.[101] At Apple, Cook declared, "[W]e believe that your data's yours."[102]

Some observers noted that tech companies made trade-offs between securing data and accessing it to improve services. Apple's strong privacy stance was facilitated by its business model. "Apple doesn't make most of its money through marketing," explained the *Wall Street Journal*, "so it hasn't needed to gather KGB-worthy dossiers on customers for better ad targeting."[103] In contrast, Google, with its advertising-driven business model, "seeks your name, phone number, gender, contacts, emails, calendar, searches, location—everything but the contents of your briefcase—when you sign in and use its services. . . . And with all that, Google can provide services that leave Apple's in the dust."[104]

Still, Apple possessed a considerable amount of customer data. By the end of 2014, Apple had 800 million iTunes accounts and therefore 800 million credit cards on file; each account also included basic registration information such as a customer's name, physical address, and contact information.[105] Apple tracked a customer's purchases on iTunes, as well as on its online store and at brick-and-mortar stores, with data including credit cards, shipping addresses, and IP addresses. From its 500 million iCloud accounts, Apple could access e-mail logs (e.g., date and recipient of an e-mail), contact lists, photos, and calendars that customers chose to store there.[106]

Global Customers

Apple's privacy decisions could affect security standards in the industry at large.[107] With its global iPhone installed base that neared 500 million in 2015, Apple's encrypted devices were available to consumers worldwide, including those in countries with fewer privacy protections. (See **Exhibit 15**.) Internet privacy and secure digital communications were crucial tools used to protect citizens living under repressive regimes. As one human rights expert wrote, "Where States impose unlawful censorship . . . , [j]ournalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment."[108]

Experts at Harvard University's Berkman Center for Internet & Society explained that private companies "serve as enthusiastic or reluctant agents of law enforcement mandates and at times as advocates for protecting users and a line of defense against governmental overreach."[109] "If the U.S. can access iPhone data, why can't its allies . . . ?" an industry observer asked. "What about nations that are either recovering from internal strife or still suffering from it . . . ? Any such decisions made by Cupertino would be messy, and involve dealing with many shades of grey."[110]

In China, one of Apple's fastest-growing markets where first-quarter 2015 iPhones sales outstripped those in the U.S., Apple had to navigate the government's privacy laws and security restrictions.[111] In August 2014, Apple had agreed to store data in China on the servers of the country's third-largest wireless carrier; the data was encrypted, and the keys were reportedly stored outside of China.[112]

In January 2015, Apple agreed to security audits from Chinese authorities who wanted to verify that the company was not sharing information with the U.S. government. The director of China's State Internet Information Office told Cook, "[Y]ou should let our internet safety department do a safety assessment. We need to reach our own conclusions to put the consumer at ease."[113] Details of the agreement were not released, but experts believed Chinese officials would be able to inspect Apple's hardware and software source codes. While sharing the code did not weaken the devices' security measures, it could make it easier for others to find potential vulnerabilities. As one reporter warned, the "Chinese government . . . could exploit its security flaws, paving the way for government to access communications of all Apple customers."[114] Critics opined that the audits violated Apple's privacy principles, but Cook firmly disagreed. "I don't support backdoor access for any government, ever," he declared. "We see that privacy is a fundamental human right."[115]

Hacking the iCloud

The same iPhone encryption measures did not apply to iCloud storage, which many customers used to back up their data from Apple devices. While iCloud was encrypted, Apple—if compelled by law enforcement—could still access information stored there because it retained a master key. In 2014, hackers broke into the iCloud accounts of many famous actresses and posted their private photos publicly. In what was known as a "social engineering attack," the hackers gained access by answering security questions correctly or guessing passwords, as there was no limit to the number of password guesses on iCloud. Critics blamed Apple for its weak security measures. Cook defended Apple's products—Apple's servers and services were not compromised—noting that the targeted attack on accounts and passwords was "a practice that has become all too common on the Internet."[116]

Following the scandal, Cook wrote an open letter to Apple's customers:

> [A]t Apple, we believe a great customer experience shouldn't come at the expense of your privacy. . . . 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. . . . Finally, I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will.[117]

San Bernardino

On December 2, 2015, a husband and wife, professed supporters of ISIL, opened fired at an office party in San Bernardino, California. They killed 14 people and died in a police shootout that followed.[118] The terrorism came only a month after an ISIL attack in Paris, France, killed over 120 people. Evidence suggested the Paris terrorists used encrypted communications to plot the attack, renewing the debate on backdoors and bringing a heightened awareness to national security issues.[119]

The San Bernardino terrorists destroyed their personal phones and laptop hard drive before the attacks,[120] but law enforcement recovered one shooter's work-issued phone: an iPhone 5C running iOS 9. Through subpoenas and search warrants, the FBI asked Apple to extract the data backed up from the phone to iCloud.[121] Apple complied but discovered that the last backup had occurred more than a month before the attack. The FBI believed important evidence remained locked on the passcode-protected, encrypted phone, but the agency could not break the encryption or guess the passcode, since iOS 9 software erased the device's data after 10 incorrect passcode attempts.

On February 16, 2016, a federal judge ordered Apple to provide technical assistance to unlock the iPhone. The court called on Apple to write new software to allow the FBI to use a "brute force" method of entering all possible passcode combinations on the phone. The FBI also asked for the ability to enter the passcodes electronically and without the built-in five-second delay between passcode attempts.[122]

The demands came under the directive of the All Writs Act of 1789, which allowed the federal court to issue "necessary or appropriate" orders where laws did not exist.[123] The eighteenth-century law was first applied to modern technologies in the 1970s, when the court forced telecom companies to install wiretaps for surveillance.[124] In the San Bernardino case, Apple had "positioned itself to be essential to gaining access" to the device, the court said, and therefore could be compelled to assist the FBI.[125] Yet the request differed from previous surveillance issues. As one cyber law expert explained, "[T]he government isn't just seeking information. . . . It's asking Apple to undertake software engineering."[126]

The U.S. government stated that the software would be used only on the phone in question—a narrow request, according to Comey.[127] But privacy experts worried the case would set a dangerous precedent, both in the U.S. and around the world. "The government suggests this tool could only be used once, on one phone," Cook said. "But that's simply not true. Once created, the technique could be used over and over again, on any number of devices."[128] He called the order the "software equivalent of cancer"[129] and worried about demands that could follow; at the time, the government was requesting that Apple help extract data in 13 other cases.[130] One instance included an ongoing case in New York City where the government had issued an order in 2015 for Apple to unlock an iPhone in a routine drug case.[131] (New York authorities had 175 locked iPhones with potential evidence for other cases.[132]) The software would also become a target for hackers and cybercriminals, Cook warned.[133]

Cook said, "The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers."[134] Apple had the technical capability to build the software but refused to comply with the order. Apple asked the government to withdraw its demand and requested that Congress form a commission of experts to discuss the implications of the case. At the end of February, Apple filed a formal opposition and a court hearing was scheduled for March. Cook indicated Apple was prepared to take the case to the Supreme Court.[135]

Public opinion was divided: a survey of Americans found that 51% of respondents thought Apple should unlock the phone.[136] Many privacy experts and executives from Twitter, Facebook, and Google applauded Apple's stance, as did a former head of the NSA.[137] Microsoft founder Bill Gates, meanwhile, criticized Apple's decision, saying that the government should be allowed to compel companies to assist with terrorism investigations.[138]

"Positions of Responsibility"

"If those of us in positions of responsibility fail to do everything in our power to protect the right of privacy, we risk something far more valuable than money. We risk our way of life," Cook declared at a White House Summit on Cybersecurity and Consumer Protection in 2015. "Fortunately, technology gives us the tools to avoid these risks. And it is my sincere hope that by using them and by working together, we will."[139] Following the court order in 2016, he reiterated the belief: "At stake is the data security of hundreds of millions of law-abiding people and setting a dangerous precedent that threatens everyone's civil liberties."[140]

As the court cases unfolded in California and New York, Cook considered the wider implications of his decisions. Many of his employees prided themselves on building secure products, and, as one observer noted, making them break their own encryption "would not be just politically and commercially difficult for Apple but emotionally hard for engineers."[141] *New York Times* journalist

Andrew Ross Sorkin questioned how Apple would balance the needs of other stakeholders: "[D]oes Apple have a moral obligation to help the government learn more about the attack? Or does it have a moral obligation to protect its customers' privacy? Or how about its shareholders? And which of these should take precedence?"[142] Cook pondered his responsibilities as he awaited the outcome in the courts—and potentially on Capitol Hill.

Exhibit 1 Apple Summary Financial Data (in millions of dollars), 2010 to 2014

	2014	2013	2012	2011	2010
Net sales	182,795	170,910	156,508	108,249	65,225
Net income	39,510	37,037	41,733	25,922	14,013
Total assets	231,839	207,000	176,064	116,371	75,183
Total cash, cash equivalents and marketable securities	155,239	146,761	121,251	81,570	51,011
Long-term debt	28,987	16,960	-	-	-
Other long-term obligations[a]	24,826	20,208	16,664	10,100	5,531
Total liabilities	120,292	83,451	57,854	39,756	27,392
Total shareholders' equity	111,547	123,549	118,210	76,615	47,791

Source: Apple Inc., September 27, 2014, Form 10-K, p. 24, http://investor.apple.com/secfiling.cfm?filingid=1193125-14-383437&cik=#D783162D10K_HTM_TOC783162_1, accessed August 2015.

Note: [a] Other long-term obligations exclude non-current deferred revenue.

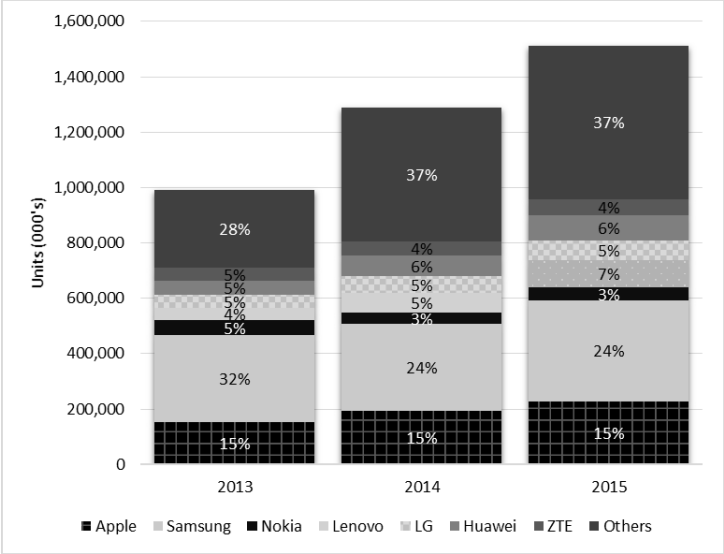
Exhibit 2 Apple Financials by Operating Segment (in millions of dollars), 2012 to 2014

	2014	2013	2012
Americas			
Net sales	65,232	62,739	57,512
Operating income	24,316	22,817	23,414
Europe			
Net sales	40,929	37,883	36,323
Operating income	14,771	13,025	14,869
Greater China			
Net sales	29,846	25,417	22,533
Operating income	11,016	8,541	9,843
Japan			
Net sales	14,982	13,462	10,571
Operating income	7,183	6,819	5,861
Rest of Asia Pacific			
Net sales	10,344	11,181	10,741
Operating income	3,636	3,753	4,253
Retail			
Net sales	21,462	20,228	18,828
Operating income	4,575	4,025	4,613

Source: Apple Inc., September 27, 2014, Form 10-K, p. 78, http://investor.apple.com/secfiling.cfm?filingid=1193125-14-383437&cik=#D783162D10K_HTM_TOC783162_1, accessed August 2015.

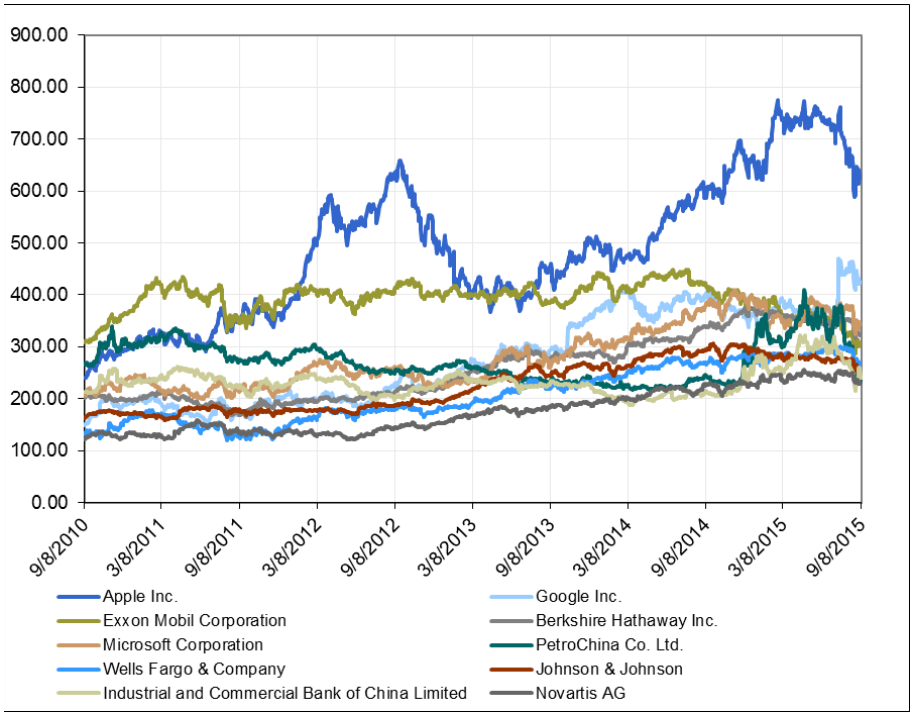
Note: Europe included India, the Middle East, and Africa; Greater China included Hong Kong and Taiwan; the Rest of Asia Pacific included Australia and other Asian countries. Geographic segments did not include results from Retail.

Exhibit 3 Global Smartphone Market by Manufacturer (%), 2013 to 2015



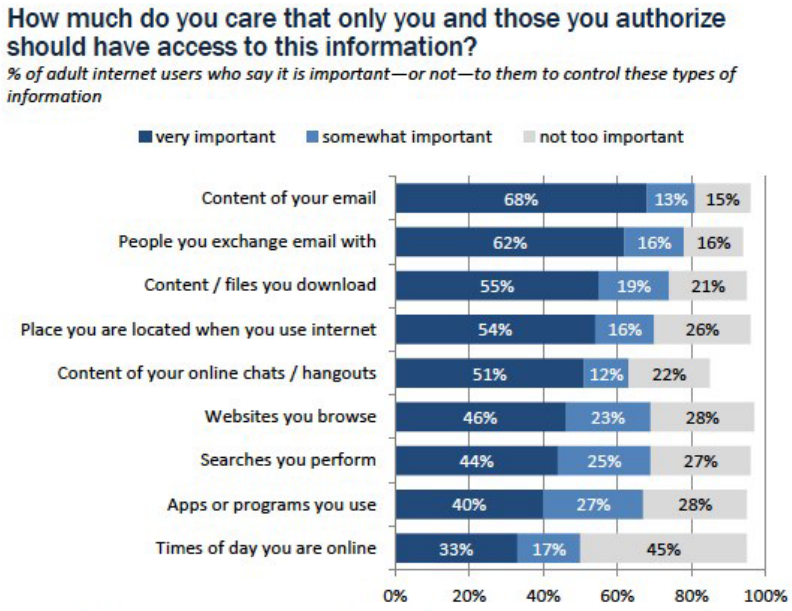
Source: Adapted from Todd Day, "Global Smartphone and Mobile OS Market," March 13, 2015, via Frost & Sullivan, accessed September 2015.

Exhibit 4 Top 10 Companies by Market Capitalization (in billions of dollars), 2010 to 2015



Source: Capital IQ, a division of Standard & Poor's, accessed September 2015.

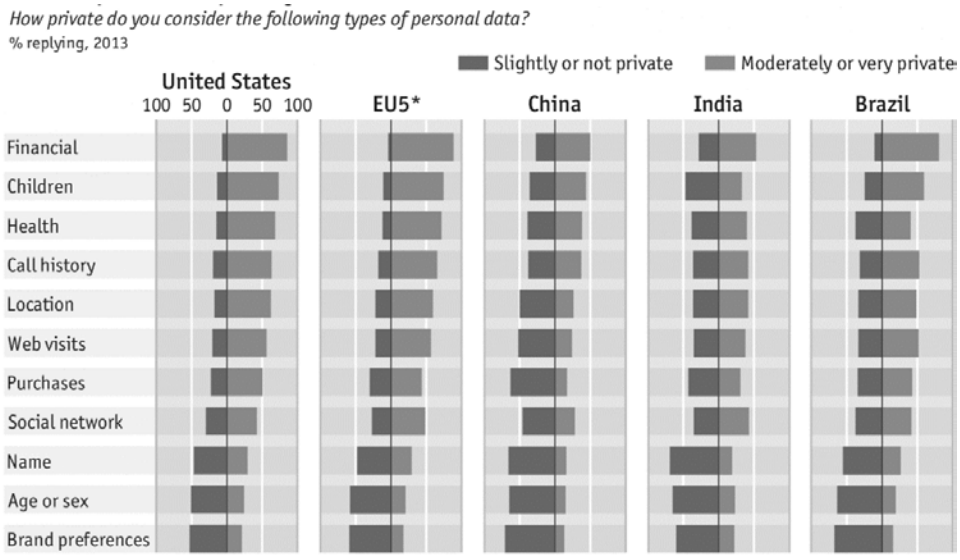
Exhibit 5a U.S. Adult Internet Users' Attitudes about Controlling Data (%), 2013



Source: Pew Research Center's Internet & American Life Project Omnibus Survey, conducted July 11-14, 2013, on landline and cell phones. N=792 for internet users and smartphone owners. Interviews were conducted in English on landline and cell phones. The margin of error on the sample is +/- 3.8 percentage points.

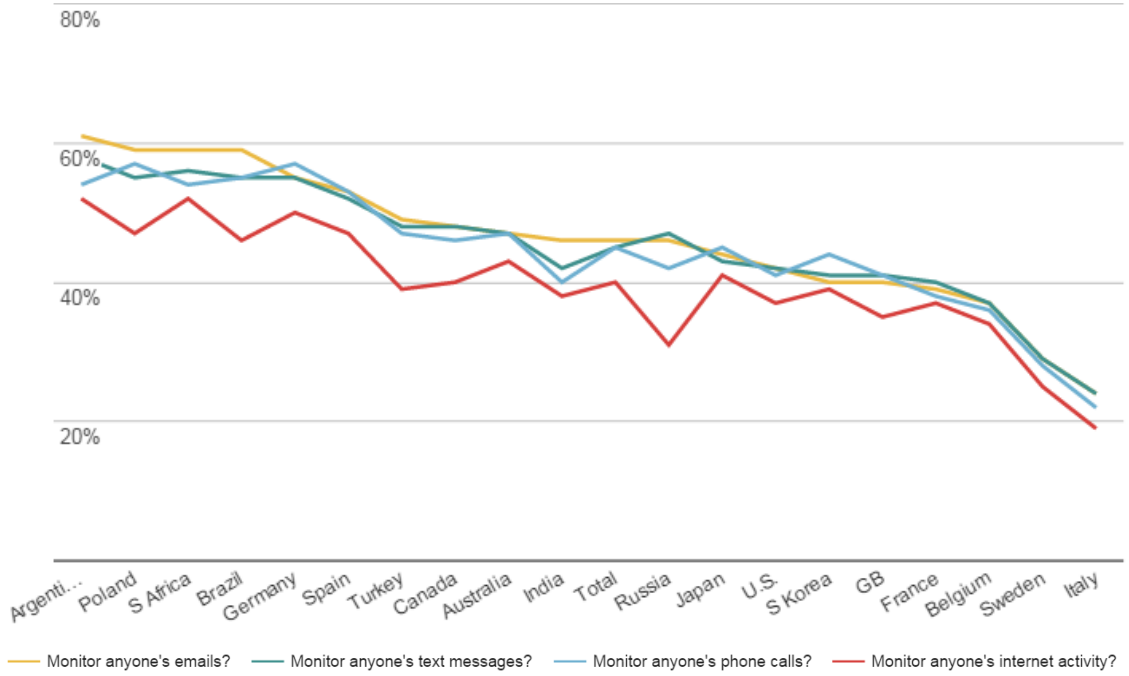
Source: Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online," Pew Research Center, September 5, 2013, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/, accessed September 2015.

Exhibit 5b Public Opinion on Privacy by Country (%), 2013



Source: "Private Parts," *The Economist*, November 7, 2013, http://www.economist.com/blogs/graphicdetail/2013/11/daily-chart-2, accessed October 2015.

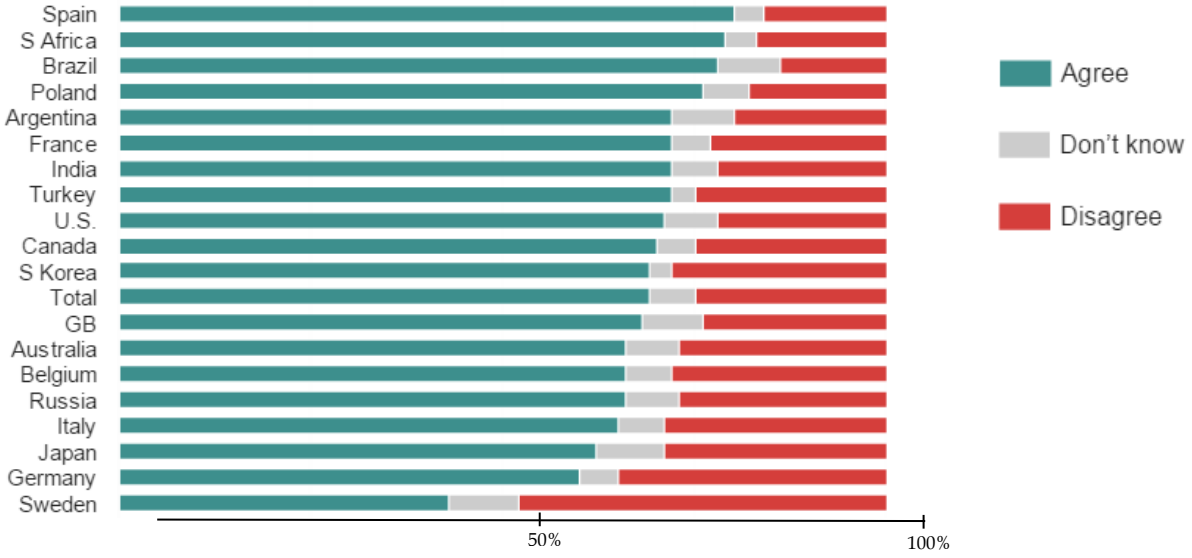
Exhibit 6a Citizens' Attitudes Towards Their Governments Monitoring Data Without Consent to Combat Crime (% completely unacceptable), 2014



Source: Ipsos MORI, "Surveillance," *Global Trends 2014*, http://www.ipsosglobaltrends.com/surveillance.html, accessed October 2015.

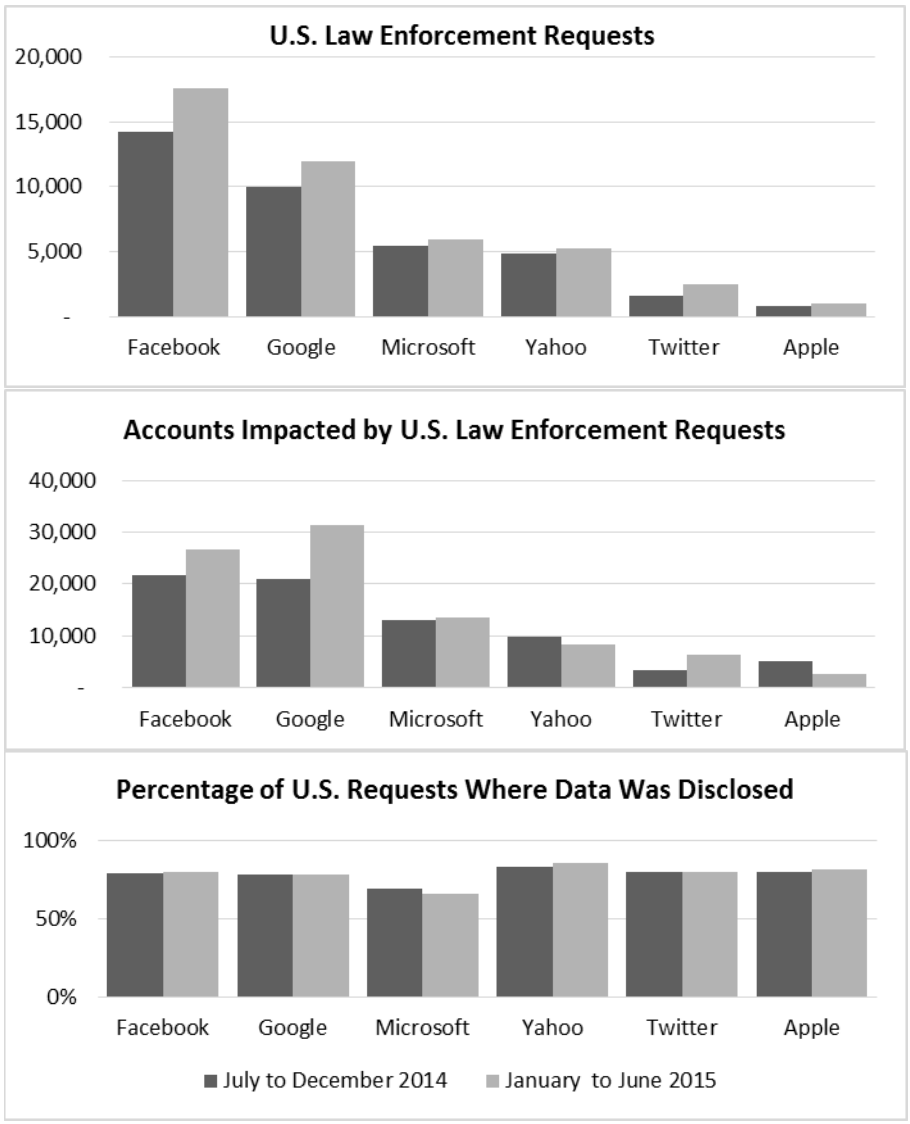
Exhibit 6b Concern About How Online Data Was Used by Own Government by Country (%), 2014

To what extent do you agree or disagree? I am concerned about how information collected about me when I go online is being used by my own government.



Source: Ipsos MORI, "Personalisation vs Privacy," *Global Trends 2014*, http://www.ipsosglobaltrends.com/personalisation-vs-privacy.html, accessed October 2015.

Exhibit 7a U.S. Law Enforcement Requests for User Data, 2014 to 2015



Source: Casewriter research from companies' July 1–December 31, 2014, and January 1–June 30, 2015, transparency reports, https://govtrequests.facebook.com/; https://www.google.com/transparencyreport/; https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/; https://transparency.yahoo.com/, https://transparency.twitter.com/; and http://www.apple.com/privacy/transparency-reports/; all accessed November 2015.

Note: Percentage of data disclosed included both content and non-content data.

Exhibit 7b U.S. National Security FISA Orders under Section 702, June to December 2014

	Orders seeking disclosure of content	Accounts affected by orders seeking content	Orders seeking disclosure of only non-content	Account affected by orders seeking non-content
Facebook	0-999	7,000-7,999	0-999	0-999
Google	500-999	17,500-17,999	0-499	0-499
Microsoft	0-999	18,000-18,999	0-999	0-999
Yahoo	0-999	42,000-42,999	0-999	0-999
Apple	250-499	0-249	n/a	n/a

Source: Casewriter research from company transparency reports, https://govtrequests.facebook.com/; https://www.google.com/transparencyreport/; https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/; https://transparency.yahoo.com/; https://transparency.twitter.com/; and http://www.apple.com/privacy/transparency-reports/; all accessed November 2015.

Note: Companies were only permitted to report the number of requests in bands of 250 or 500. Apple chose to report in the 250 band and therefore was required to combine both Foreign Intelligence Surveillance Act (FISA) and National Security Letter (NSL) requests under "national security orders."

Exhibit 8 Privacy Clauses in International Treaties

Universal Declaration of Human Rights, Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

International Covenant on Civil and Political Rights, Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

European Convention on Human Rights, Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14

No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

Source: Compiled by casewriter.

Exhibit 9 U.S. Electronic Communications Surveillance and Cybersecurity Laws

Law	Enacted	Scope	Description
Criminal Investigations			
Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act)	1968	Real-time interception of electronic communications	• Prohibited real-time interception of electronic communications, except as authorized by the act • Required government authorities to obtain a search warrant for a wiretap by establishing probable cause of criminal activity and proving the wiretap was necessary for the investigation • Restricted interceptions to an authorized period of time and excluded data obtained in violation of the statute from evidence • Required wire or electronic communications service providers to assist government requests with "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services"
Electronic Communications Privacy Act (ECPA)	1986	Surveillance of real-time communications and stored communications	• Amended the Wiretap Act • Prohibited interception of electronic communications in real-time and stored for up to 180 days,[a] except as authorized by the act • Allowed government to require providers of electronic communication services to disclose contents of stored communications less than 180 days old with a search warrant • Allowed government to require a provider of "remote computing service" to disclose the contents of communications stored by the provider or older than 180 days with a warrant, court order, or administrative subpoena (did not require judge approval)
Communications Assistance for Law Enforcement Act (CALEA)	1994	Cooperation with wiretapping	• Amended the Wiretap Act and ECPA • Required communications service providers to deploy intercept solutions in networks for government surveillance • Stipulated that a provider was not "responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication" • Expanded In 2006 to cover Voice over Internet Protocol services (voice communications over the Internet) connected to the public switch telephone network (e.g., Vonage, but not Google Voice)

National Security

Foreign Intelligence Surveillance Act (FISA)	1978	Surveillance of physical and electronic data	• Authorized electronic surveillance without court order for specific foreign intelligence purposes (i.e., protecting against potential sabotage or espionage) for up to one year • Required law enforcement to receive approval from the Foreign Intelligence Surveillance Court (FISC) for other intelligence gathering purposes by proving that the target was a foreign power or an agent of a foreign power (did not need to prove probable cause of criminal activity)
USA Patriot Act	2001	Expanded surveillance for electronic communications	• Granted law enforcement permission to obtain telephone and e-mail records of suspected terrorists, including American citizens, without a court order • Section 215 authorized the FBI to issue "National Security Letters" (NSL) to obtain and inspect "tangible things (including books, records, papers, documents, and other items)" deemed relevant to a terrorism investigation from third parties; law enforcement did not need to establish probable cause or seek judicial authorization, and recipients of NSLs were prohibited from disclosing the request. (Section 215 provisions would cease in November 2015) • Changed stored voicemails to fall under search and seizure laws, not surveillance laws • Authorized the use of "roving wiretaps" (court could grant a surveillance warrant targeting all of an individual's communications, without specifying the communications carrier(s) or third-parties involved in the wiretap)
Cyber Security Enhancement Act (CSEA)	2002	Disclosure of information related to an immediate danger	• Broadened restrictions for when an Internet service provider could disclose subscriber information and communication content to a government entity (changed from "reasonable" belief to a "good faith" belief of emergency)
Cybersecurity Information Sharing Act (CISA)	In Senate for vote, 2015	Information sharing related to cybersecurity threats	• Would authorize companies to monitor private communications and disclose to government agencies (without a warrant) information related to cybersecurity threats

Source: Casewriter research from 18 U.S. Code, 47 USC 1002(b)(3), section 2518 (4), 18 U.S. Code, section 2518 (4), USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), and adapted from Lisa Hay, "Beyond *Jones*: Electronic Surveillance And The Fourth Amendment," June 2012, http://www.fd.org/docs/select-topics---search-and-seizure/beyond-jones-electronic-surveillance-and-the-fourth-amendment.pdf?sfvrsn=4, accessed September 2015.

Note: [a] When the law was enacted, e-mail service providers offered limited storage space and therefore users frequently deleted e-mails or downloaded them to a hard drive. Data stored on a server for over 180 days was considered abandoned.

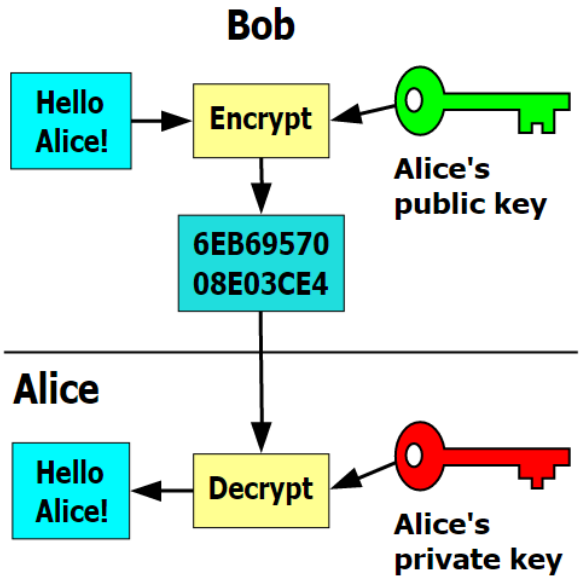
Exhibit 10 Examples of Large Data Breaches Worldwide, 2013 to 2014

Entity	Story	Year	Type	Method of Leak	No. Records Stolen
Sony Pictures	Wide-ranging hack of potentially every piece of data held by the company, including: unreleased films & scripts, employee Social Security numbers, salaries and health check results, sensitive internal business documents relating to lay-offs, restructures and executive salaries. Lead suspects are "North Korean hackers."	2014	Media	Hacked	10,000,000
JP Morgan Chase	The U.S.'s largest bank was compromised by hackers, stealing names, addresses, phone numbers, and e-mails of account holders. The hack began in June but was not discovered until July, when the hackers had already obtained the highest level of administrative privilege to dozens of the bank's servers.	2014	Financial	Hacked	76,000,000
Home Depot	Malware installed on cash register systems across 2,200 stores syphoned credit card details of up to 56 million customers. The same group of Russian and Ukrainian hackers responsible for other data breaches may be responsible.	2014	Retail	Hacked	56,000,000
Community Health Services	Community Health Systems, which operates 206 hospitals across the U.S., had patient data from the last 5 years breached. Details included names, addresses, and Social Security numbers. Suspected "Chinese hackers" were thought responsible.	2014	Healthcare	Hacked	4,500,000
Korea Credit Bureau	A contractor stole names, Social Security numbers, and credit card details of 20 million customers and sold them to marketing firms.	2014	Financial	Inside job	20,000,000
Target	Investigators believe the data was obtained via software installed on machines that customers used to swipe magnetic strips on their credit cards when paying for merchandise.	2014	Retail	Hacked	70,000,000
South Africa police	Hacker collective Anonymous hacked an anonymous whistleblowing website run by the South Africa Police Service (SAPS), revealing the identities of thousands of its users.	2013	Gov.	Hacked	16,000
Crescent Health Inc., Walgreens	Names, Social Security numbers, health insurance ID numbers, health insurance information, dates of birth, diagnoses, other medical information, disability codes, addresses, and phone numbers may have been exposed via a laptop theft.	2013	Healthcare	Lost / stolen computer	100,000
Florida Dept. of Juvenile Justice	On January 2, 2013, three computers that contained both youth and employee records were reported stolen. Over 100,000 records were on the device and may have been exposed.	2013	Gov.	Lost / stolen computer	100,000
Nintendo	Club Nintendo service was hacked following thousands of unauthorized accesses. Customer information compromised included full names, phone numbers, home and e-mail addresses.	2013	Gaming	Hacked	239,326
Vodafone	An IT contractor for the firm used his access to the telecom's system to copy customer names and bank account details.	2013	Telecom	Inside job	2,000,000

Source: Adapted from Information is Beautiful, "World's Biggest Data Breaches," August 11, 2015, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, accessed September 2015.

Exhibit 11 Description of Public Key Encryption

- Alice has generated a pair of keys: a public key that can be shared with everyone and a private key that she never shares.
- Bob wants to send Alice a message over a network (e.g., e-mail) without Eve being able to eavesdrop, so he asks Alice for her public key.
- Alice sends her public key to Bob but keeps her private key secret.
- Bob encrypts his message with her public key and sends it back to Alice. Eve may intercept the message, but she cannot decrypt it without Alice's private key.
- Alice receives the message and decrypts it with her private key.
- Alice wants to respond to Bob, so she asks Bob for his public key.
- She encrypts her reply with his public key and sends the message to Bob.
- Bob decrypts the message with his private key.



Source: Casewriter and "Public Key Encryption," August 7, 2006, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Public_key_encryption.svg, accessed February 2016.

Note: "Forward secrecy" was an increasingly popular technique for public key encryption wherein a key was created for each transaction and discarded immediately after it was used in its intended session. A hacker would have to intercept the key in real time and could only retrieve the data made available during the session; no historical data could be accessed.

Exhibit 12 Apple and iPhone iOS 9 Data Access, 2015

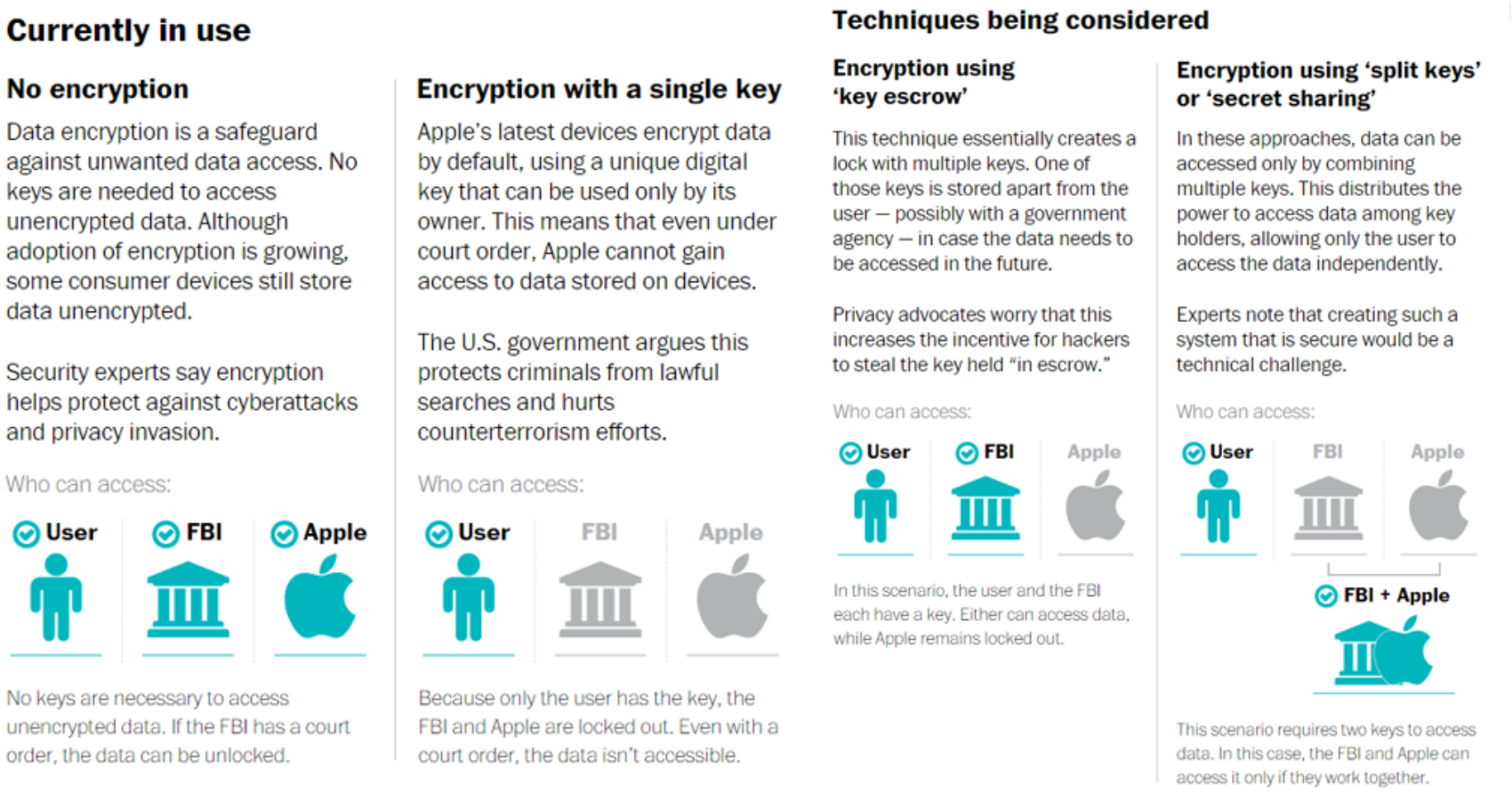
iPhone Can See, But Apple Cannot
Email, calendars, and contacts from outside providers
HomeKit smart-home device activity
Fingerprint patterns for TouchID
Apple Pay Device Account Number
FaceTime calls
App usage habits[a]
Health data[a]
iMessages[a]
Apple Can See, But It Is Anonymous
Location (for Apple services)
News app reading habits
Siri dictation and searches
Error reports
Apple Can See—And Knows It Is the Customer's
Apple Music streaming habits
iTunes app and media purchase history
Apple Stores in iCloud but Does Not Read[b]
Apple-provided iCloud email, calendars, and contacts
Photos and documents
Bookmarks and Safari history
Passwords in iCloud Keychain
iOS device backups (including iMessages and Health data)

Source: Adapted from Geoffrey A. Fowler, "What Your iPhone Doesn't Tell Apple," *Wall Street Journal*, September 15, 2015, http://www.wsj.com/articles/what-your-iphone-doesnt-tell-apple-1442338939, accessed September 2015.

Note: [a] May be included in device backups to iCloud.

[b] Apple could be required by law to unlock and examine iCloud-stored files other than data from Keychain and Find My iPhone.

Exhibit 13 Types of Encryption and Backdoor Access, 2015



Source: Kevin Schaul, "Encryption techniques and access they give," *Washington Post*, April 10, 2015, https://www.washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/, accessed August 2015.

Exhibit 14 Sample Key Disclosure Laws

Country	Law	Description	Penalty
Australia	Cybercrime Act (2001)	Upon a magistrate's order, law enforcement may compel a person to disclose encryption keys or passwords if relevant evidence is suspected to be on a suspect's computer	2 years in prison
France	Law 2001-1062 of 15 November 2001 on Daily Security	Attorney General may compel all "qualified persons" to decrypt or provide decryption keys if encrypted data are encountered in an investigation	Up to 3 years in prison and €45,000 fine or 5 years in prison and €75,000 fine
India	Information Technology Act (2000)	Government may compel the "subscriber or intermediary or any person in charge of the computer" to decrypt information	Up to 7 years in prison
Malaysia	Communications and Multimedia Act (1998)	During a search, law enforcement may compel a suspect to provide encryption keys and passwords	6 months in prison or a fine
South Africa	Regulation of Interception of Communications and Provision of Communication-Related Information Act (2002)	Law enforcement may request that a judge issue a decryption direction to a service provider before or during a telecom interception	Up to 10 years in prison or a fine
U.K.	Regulation of Investigatory Powers Act (2000)	With permission from a high-ranking official (judge, chief of police, etc.), law enforcement may compel a suspect to provide encryption keys or passwords	Up to 5 years in prison

Source: Compiled from Bert-Jaap Koops, "Crypto Law Survey," http://www.cryptolaw.org/, accessed September 2015.

Exhibit 15 Freedom on the Internet (FOTN) Rankings and Key Internet Controls by Country (2015)

Country	Score	Free, Partly Free, Not Free	Social media/ comm. apps blocked	Political, social, religious content blocked	ICT shut-down	Pro-gov. commenters manipulate online discussion	New law increasing censorship/ punishment	New law increasing surveillance, restricting anonymity	ICT user arrested, detained for political/soc. content	ICT user attacked or killed for political/soc. content	Technical attacks against gov. critics, human rights	Total
Iceland	6	F										0
Estonia	7	F										0
Canada	16	F						●				1
Germany	18	F										0
Australia	19	F						●				1
U.S.	19	F										0
Japan	22	F										0
Italy	23	F						●				1
France	24	F					●	●	●			3
Georgia	24	F										0
Hungary	24	F										0
U.K.	24	F					●	●				2
Argentina	27	F										0
Philippines	27	F			●							1
South Africa	27	F										0
Armenia	28	F									●	1
Brazil	29	F								●		1
Kenya	29	F						●	●			2
Colombia	32	PF										0
Nigeria	33	PF							●		●	2
South Korea	34	PF		●					●			2
Kyrgyzstan	35	PF		●		●		●				3
Uganda	36	PF							●		●	2
Ecuador	37	PF				●					●	2
Ukraine	37	PF		●					●	●	●	4
Tunisia	38	PF							●		●	2
Angola	39	PF							●		●	2
Mexico	39	PF				●		●	●	●	●	5
India	40	PF	●	●	●				●	●		5
Malawi	40	PF										0
Zambia	40	PF										0
Singapore	41	PF							●			1
Indonesia	42	PF	●	●			●		●			4
Malaysia	43	PF		○		●	●		●			4
Morocco	43	PF				●			●		●	3
Lebanon	45	PF		●					●		●	3
Sri Lanka	47	PF		●								1
Cambodia	48	PF		●								1
Jordan	50	PF		●					●			2
Rwanda	50	PF		●								1
Bangladesh	51	PF	●	●					●	●		4
Libya	54	PF		●	●					●		3
Azerbaijan	56	PF				●	●		●		●	4
Zimbabwe	56	PF						●	●	●	●	4
Venezuela	57	PF		●		●			●		●	4
Turkey	58	PF	●	●		●	●	●	●		●	7
Egypt	61	NF				●	○		●	●	●	5
Kazakhstan	61	NF	●	●	●	●	●		●		●	7
Russia	62	NF		●		●	●		●	●	●	6
Myanmar	63	NF				●			●	●	●	4
Thailand	63	NF		●		●	●	●	●	●		6
Belarus	64	NF		●		●	●	●	●		●	6
Gambia	65	NF		●					●	●		3
Sudan	65	NF				●	●		●		●	4
UAE	68	NF	●	●			●		●			4
Pakistan	69	NF	●	●	●		●		●	●		6
Bahrain	72	NF	●	●		●		●	●		●	6
Saudi Arabia	73	NF	●	●		●			●	●	●	6
Vietnam	76	NF		●		●	●		●	●	●	6
Uzbekistan	78	NF	●	●		●	●		see note		●	6
Cuba	81	NF	●	●		●			●	●		5
Ethiopia	82	NF	●	●		●			●	●	●	6
Iran	87	NF	●	●		●			●		●	5
Syria	87	NF	●	●	●	●			●	●	●	7
China	88	NF	●	●	●	●	●	●	●	●	●	9
Total			15	31	7	24	17	14	40	19	28	

Source: Adapted from Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, Mai Truong, "Freedom on The Net," Freedom House, October 2015, p. 16-17, https://freedomhouse.org/report/freedom-net/freedom-net-2015, accessed November 2015.

Note: Information and communication technologies (ICT) user arrested before coverage period but serving part or all of sentence during coverage period.

Endnotes

[1] Tim Cook, speech at Electronic Privacy Information Center Champion of Freedom Award Ceremony, Washington, D.C., June 1, 2015, in Matthew Panzarino, "Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy," Tech Crunch, June 2, 2015, http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.tx7ck5:HGwE, accessed August 2015.

[2] Cyrus Vance, in Nicole Perlroth and David E. Sanger, "F.B.I. Director Repeats Call That Ability to Read Encrypted Messages Is Crucial," *The New York Times*, November 18, 2015, http://www.nytimes.com/2015/11/19/us/politics/fbi-director-repeats-call-that-ability-to-read-encrypted-messages-is-crucial.html, accessed November 2015.

[3] Philip Elmer-DeWitt, "Here are the 10 top-selling smartphones for April," *Fortune*, June 2, 2015, http://fortune.com/2015/06/02/here-are-the-10-top-selling-smartphones-for-april/, accessed September 2015.

[4] Ben Taylor, "The Top 10 Smartphones on the Market for Fall 2014," *Time*, September 25, 2014, http://time.com/3427905/best-phones-fall-2014/, accessed September 2015.

[5] Catherine Crump, in Cyrus Farivar, "Apple expands data encryption under iOS 8, making handover to cops moot," *Ars Technica*, September 18, 2014, http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/, accessed September 2015.

[6] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech given at Brookings Institution, Washington, DC, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course, accessed August 2015.

[7] Jonny Evans, "Apple's 2014 in 33 Stats," *Computer World*, December 18, 2014, http://www.computerworld.com/article/2858887/apples-2014-in-33-stats.html#slide2, accessed August 2015.

[8] Apple Inc., September 27, 2014, Form 10-K, http://investor.apple.com/secfiling.cfm?filingid=1193125-14-383437&cik=#D783162D10K_HTM_TOC783162_1, accessed August 2015.

[9] Shira Ovide and Daisuke Wakabayashi, "Apple's Share of Smartphone Industry's Profits Soars to 92%," *Wall Street Journal*, http://www.wsj.com/articles/apples-share-of-smartphone-industrys-profits-soars-to-92-1436727458, accessed October 2015.

[10] Apple Inc., September 27, 2014, Form 10-K.

[11] Gerard Baker, "Tim Cook Answers the Skeptics: Apple's CEO on Apple Pay, the Apple Watch—and killing the iPod classic," *Wall Street Journal*, November 3, 2014, http://www.wsj.com/articles/apples-tim-cook-answers-the-skeptics-1414962373, accessed August 2015.

[12] Google Inc., December 31, 2014, Form 10-K, pp. 7, 14, https://investor.google.com/pdf/20141231_google_10K.pdf, accessed September 2015.

[13] *Time* Staff, "Interactive Timeline: Tim Cook and the Rise of Apple," *Time*, December 19, 2012, http://poy.time.com/2012/12/19/interactive-timeline-tim-cook-and-the-rise-of-apple/, accessed August 2015.

[14] Yukari Iwatani Kane, "The Job After Steve Jobs: Tim Cook and Apple," *Wall Street Journal*, February 28, 2014, http://www.wsj.com/articles/SB10001424052702304610404579405420617578250, accessed August 2015.

[15] Adam Lashinsky, "Apple's Tim Cook leads different," *Fortune*, March 26, 2015, http://fortune.com/2015/03/26/tim-cook/, accessed August 2015.

[16] Tim Cook, in Bob Brown, "Transcript of Apple CEO Tim Cook's commencement address at George Washington University," *Network World*, May 18, 2015, http://www.networkworld.com/article/2923554/education/apples-tim-cook-tells-gw-grads-ignore-the-cynics-change-the-world-like-steve-jobs-did.html, accessed August 2015.

[17] Tim Cook, in Katie Benner and Paul Mozur, "Apple Sees Value in Its Stand to Protect Security," *New York Times*, February 20, 2016, http://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html, accessed February 2016.

[18] Craig Timberg, "U.S. threatened massive fine to force Yahoo to release data," *Washington Post*, September 11, 2014, https://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html, accessed November 2015.

[19] Matt Buchanan, "How the N.S.A. Cracked the Web," *New Yorker*, September 6, 2013, http://www.newyorker.com/tech/elements/how-the-n-s-a-cracked-the-web, accessed September 2015.

[20] "NSA slides explain the PRISM data-collection program," *Washington Post*, July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, accessed August 2015.

[21] Evan Perez, "U.S. Charges Snowden in Security-Leak Case," *Wall Street Journal*, June 22, 2013, http://www.wsj.com/articles/SB10001424127887323893504578560071189477346, accessed August 2015.

[22] Neil MacFarquhar, "Snowden Asks Russia to Extend Asylum," *New York Times*, July 9, 2014, http://www.nytimes.com/2014/07/10/world/europe/edward-snowden-asks-russia-to-extend-asylum.html?_r=0, accessed August 2015.

[23] Cecilia Kang and Ellen Nakashima, "Tech executives to Obama: NSA spying revelations are threatening business," *Washington Post*, December 17, 2013, http://www.washingtonpost.com/business/technology/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html, accessed August 2015.

[24] Danielle Kehl, Kevin Bankston, Robyn Greene, and Robert Morgus, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," New America's Open Technology Institute, July 2014, p. 10, https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf, accessed August 2015.

[25] Jason Lee, "Apple iPhone a danger to China national security: state media," Reuters, July 11, 2014, http://www.reuters.com/article/2014/07/11/us-apple-china-idUSKBN0FG0S520140711, accessed September 2015.

[26] Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times*, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html, accessed September 2015.

[27] Kehl et al., "Surveillance Costs," July 2014.

[28] Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness," Information Technology & Innovation Foundation, June 2015, p. 3, http://www2.itif.org/2015-beyond-usa-freedom-act.pdf, accessed August 2015.

[29] Mary Madden, "Privacy and Cybersecurity: Key findings from Pew Research," Pew Research Center, January 16, 2015, http://www.pewresearch.org/key-data-points/privacy/, accessed August 2015.

[30] George Gao, "What Americans think about NSA surveillance, national security and privacy," Pew Research Center, May 29, 2015, http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/, accessed August 2015.

[31] "Mobile Phones—US—February 2015," Mintel, accessed August 2015.

[32] Timothy Morey, Theodore Forbath, and Allison Schoop, "Customer Data: Designing for Transparency and Trust," *Harvard Business Review*, May 2015, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust, accessed September 2015.

[33] EMC Privacy Index, 2014, http://www.emc.com/campaign/privacy-index/global.htm, accessed October 2015.

[34] Monica Anderson, "6 facts about Americans and their smartphones," Pew Research Center, April 1, 2015, http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/, accessed August 2015.

[35] Symantec, "State of Privacy Report 2015," https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf, accessed October 2015.

[36] EMC Privacy Index, 2014.

[37] EMC Privacy Index, 2014.

[38] Kang and Nakashima, "Tech executives to Obama."

[39] Craig Timberg, "Google encrypts data amid backlash against NSA spying," *Washington Post*, September 6, 2013, https://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html, accessed November 2015.

[40] Sara Sorcher, "The battle between Washington and Silicon Valley over encryption," *Christian Science Monitor*, July 7, 2015, http://www.csmonitor.com/World/Passcode/2015/0707/The-battle-between-Washington-and-Silicon-Valley-over-encryption, accessed August 2015.

[41] Geoffrey Smith, "Apple to spend $1.9 billion on two data centers in Europe," *Fortune*, February 23, 2015, http://fortune.com/2015/02/23/apple-to-spend-1-9-billion-on-two-data-centers-in-europe/, accessed August 2015.

[42] Kashmir Hill, "Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government," *Forbes*, November 14, 2013, http://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/, accessed August 2015.

[43] Jesse J. Holland, "Silicon Valley companies will receive more freedom to disclose data requests in deal with government," *San Jose Mercury News*, January 27, 2014, http://www.mercurynews.com/business/ci_25003875/silicon-valley-companies-will-receive-more-freedom-disclose, accessed August 2015.

[44] U.S. Constitution, amendment IV.

[45] Digital 4th, "The Problem," http://www.digital4th.org/the-problem/, accessed August 2015.

[46] Rainey Reitman, "Deep Dive: Updating the Electronics Communications Privacy Act," Electronic Frontier Foundation, December 6, 2012, https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act, accessed August 2015.

[47] Robert Barnes, "Supreme Court says police must get warrants for most cellphone searches," *Washington Post*, June 25, 2014, http://www.washingtonpost.com/national/supreme-court-police-must-get-warrants-for-most-cellphone-searches/2014/06/25/e2ff1326-fc6b-11e3-8176-f2c941cf35f1_story.html, accessed August 2015.

[48] *Riley v. California*, 573 S. Ct., No. 13-132, (2014).

[49] *Riley v. California*, 573 S. Ct., No. 13-132, (2014).

[50] Barack Obama, in "Barack Obama defends US surveillance tactics," BBC News, June 8, 2013, http://www.bbc.com/news/world-us-canada-22820711, accessed September 2015.

[51] "Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II," Center for Strategic and International Studies, June 2014, p. 2, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, accessed September 2015.

[52] Ellen Nakashima, "U.S. developing sanctions against China over cyberthefts," *Washington Post*, August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html, accessed September 2015.

[53] Gregory S. McNeal, "Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee," *Forbes*, July 9, 2014, http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/, accessed September 2015.

[54] "Is Breaking Web Encryption Illegal?," Center for Democracy & Technology, February 20, 2015, https://cdt.org/insight/is-breaking-web-encryption-legal/, accessed September 2015.

[55] Josephine Wolff, "What Exactly Does *Reasonable* Mean?," *Slate*, September 1, 2015, http://www.slate.com/articles/technology/future_tense/2015/08/the_ftc_punishes_wyndham_for_failing_to_protect_customer_data.html, accessed September 2015.

[56] Patricia Bailin, "Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices," IAPP, https://iapp.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices/, accessed September 2015.

[57] Zoe Bedell and Benjamin Wittes, "Civil Liability for End-to-End Encryption: Threat or Fantasy? Part I," LawFare blog, July 21, 2015, https://www.lawfareblog.com/civil-liability-end-end-encryption-threat-or-fantasy-part-i, accessed August 2015.

[58] Matthew Green, "Is Apple Picking a Fight With the U.S. Government?," *Slate*, September 23, 2014, http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html, accessed August 2015.

[59] Devlin Barrett, Danny Yadron, and Daisuke Wakabayashi, "Apple and Others Encrypt Phones, Fueling Government Standoff," *Wall Street Journal*, November 18, 2014, http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801, accessed August 2015.

[60] Apple, "Privacy," http://www.apple.com/privacy/government-information-requests/, accessed September 2015.

[61] Apple, "App Store," September 19, 2015, https://developer.apple.com/support/app-store/, accessed October 2015.

[62] Timothy J. Seppala, "Google won't force Android encryption by default (update)," *Engadget*, March 2015, http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/, accessed August 2015.

[63] Timothy B. Lee, "NSA-proof encryption exists. Why doesn't anyone use it?," *Washington Post*, June 14, 2013, http://www.washingtonpost.com/news/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/, accessed September 2015.

[64] John Naughton, "Humans are the weakest link when it comes to encryption," *Guardian,* July 5, 2015, http://www.theguardian.com/commentisfree/2015/jul/05/encryption-humans-weakest-link, accessed August 2015.

[65] Mihaita Bamburic, "Android 5.0 Lollipop encryption severely impacts performance," betanews, November 21, 2014, http://betanews.com/2014/11/21/android-5-0-lollipop-encryption-severely-impacts-performance/, accessed November 2015.

[66] James B. Comey, Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy, July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy, accessed August 2015.

[67] David Cameron, in Nicholas Watt, Rowena Mason, and Ian Traynor, "David Cameron pledges anti-terror law for internet after Paris attacks," *Guardian*, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg, accessed August 2015.

[68] Associated Press, "German government backs end-to-end encryption for email," *Mashable*, http://mashable.com/2015/03/10/german-government-email-encryption/#AL7McImwx8qV, accessed October 2015.

[69] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Human Rights Council 29/32, May 22, 2015, p. 13, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc, accessed September 2015.

[70] Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary, Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, July 8, 2015, p. 1, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf, accessed August 2015.

[71] Andy Greenberg, "Manhattan DA: iPhone Crypto Locked Out Cops 74 Times," *Wired*, July 8, 2015, http://www.wired.com/2015/07/manhattan-da-iphone-crypto-foiled-cops-74-times/, accessed August 2015.

[72] Greenberg, "Manhattan DA: iPhone Crypto Locked Out Cops 74 Times."

[73] Cyrus R. Vance Jr., François Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times*, August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0, accessed August 2015.

[74] Comey and Quillian Yates Before the Senate Judiciary Committee, Going Dark.

[75] Barrett et al., "Apple and Others Encrypt Phones."

[76] Bruce Schneier, in Taylor Armerding, "Schneier: Internet Has Delivered a 'Golden Age of Surveillance,'" Schneier on Security blog, April 11, 2014, https://www.schneier.com/news/archives/2014/04/schneier_internet_ha.html, accessed October 2015.

[77] Vance, Before the United States Senate Committee on the Judiciary, Going Dark, p. 4.

[78] Vance, Before the United States Senate Committee on the Judiciary, Going Dark.

[79] Comey and Quillian Yates, Before the Senate Judiciary Committee, Going Dark.

[80] Barrett et al., "Apple and Others Encrypt Phones."

[81] James Comey, "Encryption, Public Safety, and 'Going Dark,'" *LawFare* blog, July 6, 2015, https://www.lawfareblog.com/encryption-public-safety-and-going-dark, accessed August 2015.

[82] James Comey, in Neil Hughes, "FBI director continues crusade against Apple's encryption of iPhone data," *Apple Insider*, October 13, 2014, http://appleinsider.com/articles/14/10/13/fbi-director-continues-crusade-against-apples-encryption-of-iphone-data, accessed August 2015.

[83] Benjamin Wittes, "Five Hard Encryption Questions," *LawFare* blog, August 7, 2015, https://www.lawfareblog.com/five-hard-encryption-questions, accessed August 2015.

[84] Sorcher, "The battle between Washington and Silicon Valley over encryption."

[85] Cory Doctorow, "Crypto wars redux: why the FBI's desire to unlock your private life must be resisted," *Guardian*, October 9, 2014, http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted, accessed August 2015.

[86] Green, "Is Apple Picking a Fight With the U.S. Government?"

[87] Tim Cook, interview by Robert Siegel, "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right,'" NPR, October 1, 2015, http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right, accessed October 2015.

[88] Harold Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," MIT Computer Science and Artificial Intelligence Laboratory Technical Report, p. 12, July 6, 2015, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8, accessed July 2015.

[89] Doctorow, "Crypto wars redux."

[90] Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science & Technology Law Review* 13, no. 416 (2012): 419, http://stlr.org/download/volumes/volume13/Swire.pdf, accessed September 2015.

[91] Peter Swire and Kenesa Ahmad, in Peter Swire, Testimony before the Senate Judiciary Committee Hearing, Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy, September 17, 2015, p. 18, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf, accessed August 2015.

[92] Open Letter on Encryption to President Barack Obama, May 19, 2015, https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf, accessed August 2015.

[93] Nicholas Lansman, in Ewen MacAskill and Alan Travis, "MI5 chief calls for more up-to-date surveillance powers," *Guardian*, September 17, 2015, http://www.theguardian.com/world/2015/sep/17/mi5-chief-calls-for-more-up-to-date-surveillance-powers, accessed September 2015.

[94] Sorcher, "The battle between Washington and Silicon Valley over encryption."

[95] Bankston, in Swire, Testimony before the Senate Judiciary Committee Hearing, Going Dark, p. 20.

[96] Sorcher, "The battle between Washington and Silicon Valley over encryption."

[97] Danielle Kehl, "The lessons of the Crypto Wars," *Slate*, June 23, 2015, http://www.slate.com/articles/technology/future_tense/2015/06/safe_act_the_right_to_strong_encryption_almost_became_law_in_the_90s.html, accessed August 2015.

[98] Sheldon Whitehouse, in Conor Friedersdorf, "Do Encrypted Phones Threaten National Security?" *Atlantic*, July 15, 2015, http://www.theatlantic.com/politics/archive/2015/07/does-encryption-threaten-national-security/398573/, accessed August 2015.

[99] Bedell and Wittes, "Civil Liability for End-to-End Encryption." In the source document, the second instance of "work-around" is not hyphenated.

[100] Tim Cook, speech at The White House Summit on Cybersecurity and Consumer Protection, Stanford University, February 13, 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit, accessed August 2015.

[101] Nate Cardozo, Kurt Opsahl, and Rainey Reitman, "Who Has Your Back?" Electronic Frontier Foundation, June 17, 2015, https://www.eff.org/who-has-your-back-government-data-requests-2015#results-summary, accessed August 2015.

[102] Tim Cook, interview by Gerard Baker, "Tim Cook Answers the Skeptics," *Wall Street Journal*, November 3, 2014.

[103] Geoffrey A. Fowler, "What Your iPhone Doesn't Tell Apple," *Wall Street Journal*, September 15, 2015, http://www.wsj.com/articles/what-your-iphone-doesnt-tell-apple-1442338939, accessed September 2015.

[104] Fowler, "What Your iPhone Doesn't Tell Apple."

[105] Horace Dediu, "How big is iCloud?" Asymco, November 15, 2014, http://www.asymco.com/2014/11/15/how-big-is-icloud/, accessed September 2015.

[106] Dediu, "How big is iCloud?"

[107] Jennifer Booton, "Apple's iPhone installed base could surpass 500 million this year," *Market Watch*, September 21, 2015, http://www.marketwatch.com/story/apples-iphone-installed-base-could-surpass-500-million-this-year-2015-09-21, accessed February 2016.

[108] Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom."

[109] Urs Gasser, Jonathan Zittrain, Robert Faris, and Rebekah Heacock Jones, "Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse," Berkman Center for Internet & Society at Harvard University, p. 31, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538813, accessed July 2015.

[110] Chris Duckett, "For simplicity and security, Apple needs to draw a line now to prevent further ones," ZDNet, February 21, 2016, http://www.zdnet.com/article/for-simplicity-and-security-apple-needs-to-draw-a-line-now-to-prevent-further-ones/, accessed February 2016.

[111] Tim Higgins, "Apple IPhones Sales in China Outsell the U.S. for the First Time," Bloomberg Business, April 27, 2015, http://www.bloomberg.com/news/articles/2015-04-27/apple-s-iphones-sales-in-china-outsell-the-u-s-for-first-time, accessed August 2015.

[112] Gerry Shih and Paul Carsten, "Apple begins storing users' personal data on servers in China," Reuters, August 15, 2014, http://www.reuters.com/article/2014/08/15/us-apple-data-china-idUSKBN0GF0N720140815, accessed October 2015.

[113] Heather Timmons, "Apple is reportedly giving the Chinese government access to its devices for 'security checks,'" *Quartz*, January 23, 2015, http://qz.com/332059/apple-is-reportedly-giving-the-chinese-government-access-to-its-devices-for-a-security-assessment/, accessed October 2015.

[114] Lauren Walker, "Is Apple Helping China Spy on Its Citizens?," *Newsweek*, March 5, 2015, http://www.newsweek.com/apple-helping-china-spy-its-citizens-311654, accessed October 2015.

[115] Cook, interview by Siegel, "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right.'"

[116] Apple, "Apple Media Advisory: Update to Celebrity Photo Investigation," press release, September 2, 2014, https://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html, accessed August 2015.

[117] Apple, "Privacy," https://www.apple.com/privacy/, accessed August 2015.

[118] Evan Perez and Tim Hume, "Apple opposes judge's order to hack San Bernardino shooter's iPhone," CNN, February 18, 2016, http://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/, accessed February 2016.

[119] Sean Gallagher, "Paris attacks 'would not have happened' without crypto, says NSA chief," *Ars Technica*, February 18, 2016, http://arstechnica.co.uk/tech-policy/2016/02/nsas-director-says-paris-attacks-would-not-have-happened-without-crypto/, accessed February 2016.

[120] Sam Thielman, Spencer Ackerman, and Amanda Holpuch, "FBI and Apple vie for public support in dispute over California shooter's iPhone," *Guardian*, February 22, 2016, http://www.theguardian.com/us-news/2016/feb/22/fbi-apple-san-bernardino-shooting-iphone, accessed February 2016.

[121] Tim Cook, "A Message to Our Customers," Apple website, February 16, 2016, http://www.apple.com/customer-letter/, accessed February 2016.

[122] Ben Thompson, "Apple Versus The FBI, Understanding iPhone Encryption, The Risks For Apple And Encryption," Stratechery blog, February 17, 2016, https://stratechery.com/2016/apple-versus-the-fbi-understanding-iphone-encryption-the-risks-for-apple-and-encryption/, accessed February 2016.

[123] Cyrus Farivar and David Kravets, "How Apple will fight the DOJ in iPhone backdoor crypto case," *Ars Technica*, February 18, 2016, http://arstechnica.com/tech-policy/2016/02/how-apple-will-fight-the-doj-in-iphone-backdoor-crypto-case/, accessed February 2016.

[124] Farivar and Kravets, "How Apple will fight the DOJ in iPhone backdoor crypto case."

[125] 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. 5:15-mj-00451, C.D. California, February 16, 2016, http://www.wired.com/wp-content/uploads/2016/02/SB-shooter-MOTION-seeking-asst-iPhone.pdf, accessed February 2016.

[126] Jonathan Zittrain, in Christina Pazzanese and Alvin Powell, "Apple bites back: Debate on privacy vs. security underpins showdown between tech giant and FBI," *Harvard Gazette*, February 18, 2016, http://news.harvard.edu/gazette/story/2016/02/apple-bites-back/, accessed February 2016.

[127] James Comey, "We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead," *Lawfare* blog, February 21, 2016, https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead, accessed February 2016.

[128] Cook, "A Message to Our Customers."

[129] Tim Cook, in Danny Yadron, "Apple CEO Tim Cook: FBI asked us to make software 'equivalent of cancer,'" *Guardian*, February 24, 2016, http://www.theguardian.com/technology/2016/feb/24/apple-ceo-tim-cook-government-fbi-iphone-encryption, accessed February 2016.

[130] Daisuke Wakabayashi and Devlin Barrett, "Apple Files Motion Opposing Order to Unlock iPhone," *Wall Street Journal*, http://www.wsj.com/articles/apple-files-motion-opposing-order-to-unlock-iphone-1456432357, accessed February 2016.

[131] Matt Apuzzo, Joseph Goldstein, and Eric Lichtblau, "Line in the Sand Over iPhones Was Over a Year in the Making," *New York Times*, February 19, 2016, http://www.nytimes.com/2016/02/19/technology/a-yearlong-road-to-a-standoff-with-the-fbi.html, accessed February 2016.

[132] Apuzzo et al., "Line in the Sand Over iPhones Was Over a Year in the Making."

[133] Apple, "Answer to your question about Apple and Security," February 2016, http://www.apple.com/customer-letter/answers/, accessed February 2016.

[134] Cook, "A Message to Our Customers."

[135] Fred Barbash and Justin Wm. Moyer, "Tim Cook: Protecting America from itself—and protecting Apple from America," *Washington Post*, February 25, 2016, https://www.washingtonpost.com/news/morning-mix/wp/2016/02/25/tim-cook-protecting-america-from-itself-and-protecting-apple-from-america/, accessed February 2016.

[136] "More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone," Pew Research Center, February 22, 2016, http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/, accessed February 2016.

[137] Sam Thielman, "Apple's encryption battle with the FBI has implications well past the iPhone," *Guardian*, February 20, 2016, http://www.theguardian.com/technology/2016/feb/19/apple-fbi-privacy-encryption-fight-san-bernardino-shooting-syed-farook-iphone, accessed February 2016.

[138] Stephen Foley and Tim Bradshaw, "Bill Gates backs FBI iPhone hack request," *Financial Times*, February 23, 2016, http://on.ft.com/1XK1nzv, accessed February 2016.

[139] Cook, speech at The White House Summit on Cybersecurity and Consumer Protection.

[140] Tim Cook, in Amanda Holpuch, "Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue," *Guardian*, February 22, 2016, http://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties, accessed February 2016.

[141] Nellie Bowles, "Apple v FBI: engineers would be ashamed to break their own encryption," *Guardian*, February 22, 2016, http://www.theguardian.com/technology/2016/feb/22/apple-vs-fbi-engineers-breaking-encryption-unholy, accessed February 2016.

[142] Andrew Ross Sorkin, "For Apple, a Search for a Moral High Group in a Heated Debate," *New York Times*, February 22, 2016, http://www.nytimes.com/2016/02/23/business/dealbook/for-apple-the-moral-high-ground-lacks-clearly-defined-boundaries.html?_r=0, accessed February 2016.