HARVARD | BUSINESS | SCHOOL

9-318-079

REV: MAY 25, 2018

HENRY MCGEE

NIEN-HÊ HSIEH

NATHANIEL SCHWALB

Apple: Privacy vs. Safety (B)

From my American mind-set, I believe strongly in freedoms. . . . I also know each country in the world decides their laws and regulations.

— Tim Cook, Apple CEO[1]

This kind of partnership between an American company and a dictatorial regime is at odds with the image Apple has built as a company committed to privacy and a willingness to stand up to pressure from larger entities like the United States government.

— Chen Guangcheng, Chinese Civil Rights Activist[2]

In February 2016, Apple refused the Federal Bureau of Investigation (FBI)'s request to help access the encrypted iPhone of the husband of a married couple who professed allegiance to the Islamic State of Iraq and the Levant (ISIL) and killed 14 people in the San Bernardino terrorist attack. Investigators ultimately withdrew the request and gained access via third-party software.[3] However, this was a temporary fix. The next year, Apple encryption blocked investigators from accessing the iPhone belonging to a gunman who killed himself and 26 people as they worshipped at the First Baptist Church of Sutherland Springs, Texas.[4] In late 2017, the FBI claimed encryption had prevented them from accessing 6,900 devices, representing more than half of the devices that investigators had tried to access in the preceding 11 months.[a,5]

During that time, Apple had remained the most profitable player in the smartphone market[6] and the largest company in the world by market capitalization.[7] Apple sold phones with end-to-end encryption and explained that creating a technique to unlock encrypted phones would risk the privacy of customers, as "the technique could be used over and over again, on any number of devices."[8]

Apple also faced government pressures in China. Virtual Private Network (VPN) applications (apps) allowed Chinese smartphone users to bypass government censors online and browse any website available in other countries. Chinese regulations required that VPNs operate only with an official government license, which was expensive and difficult to obtain. This effectively restricted

[a] In May 2018, the FBI announced that it had miscounted the number of inaccessible devices. An FBI statement blamed the miscount on "programming errors." An internal report estimated the correct number to be 1,000 to 2,000 devices. Devlin Barrett, "FBI repeatedly overstated encryption threat figures to Congress, public," *The Washington Post*, May 22, 2018, https://wapo.st/2sd9iNq, accessed May 2018.

Senior Lecturer Henry McGee, Professor Nien-hê Hsieh, and Associate Case Researcher Nathaniel Schwalb (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.

Copyright © 2018 President and Fellows of Harvard College. To order copies or request permission to reproduce materials, call 1-800-545-7685, write Harvard Business School Publishing, Boston, MA 02163, or go to www.hbsp.harvard.edu. This publication may not be digitized, photocopied, or otherwise reproduced, posted, or transmitted, without the permission of Harvard Business School.

This document is authorized for use only in Prof. Sourya Joyee De's Cyber Security Risk Management 1.16.2020 at Indian Institute of Management - Raipur from Jan 2020 to Jul 2020.

access to a few high-paying corporate users. In January 2017, Chinese authorities announced a crackdown on unlicensed VPNs.[9] In July, Apple notified developers that VPN apps would be removed from its App Store in China.[10] Apple CEO Tim Cook explained, "We would obviously rather not remove the apps, but [. . .] we follow the law wherever we do business. We strongly believe participating in markets and bringing benefits to customers is in the best interest of the folks there and in other countries as well."[11] Chinese Android app stores also removed VPN apps.[12]

Cook's decision in China, one of Apple's most important markets, drew sharp criticism both in the U.S. and abroad. U.S. senators noted that Cook's decision could be construed as a betrayal of the 2017 Free Expression Award Cook had accepted earlier in the year.[13] One *New York Times* columnist wrote that Cook "made clear that Apple would obey American law—but only after trying to shape the law."[14] The columnist continued, "Search Apple's website for a letter from Mr. Cook issuing a public rebuke of China's intrusion into his customers' privacy and freedom of expression—you won't find it. The company has not fully tested its political and economic leverage in China."[15] A Chinese investor in one of the affected VPN services spoke bluntly in an anonymous interview: "Apple is kissing ass, so that they can protect their revenue stream in China."[16] One Chinese writer living abroad wrote, "Apple CEO Tim Cook was woefully ignorant about the true meanings of 'openness' and 'shared benefits,'" and that as a result of censorship, "public discussion is stunted, grievances are suppressed, and wrongdoers are not held accountable."[17] Others compared Apple to its rival Google, which withdrew from China in 2010 rather than comply with policies to censor certain search results.[18]

In China, during December 2017, Cook took the opportunity to defend Apple's position: "When you go into a country and participate in a market, you are subject to the laws and regulations of that country. [. . .] Your choice is, do you participate or do you stand on the sideline and yell at how things should be. My own view very strongly is you show up and you participate, you get in the arena, because nothing ever changes from the sideline."[19]

By early 2018, Chinese government regulations[b] requiring domestic storage of domestic data prompted Apple to offer its customers in China using iCloud, its backup storage, a choice.[20] They could stop using iCloud, or they could continue using the service by agreeing to let Apple migrate their data to the care of a state-owned enterprise, Guizhou-Cloud Big Data (GCBD). In migrating to GCBD, customers had to accept new terms of service that asked users to "agree that Apple and GCBD will have access to all data [stored] on this service, including the right to share, exchange and disclose all user data, including content, to and between each other under applicable law."[21]

While Chinese customers' iCloud data would remain encrypted, Apple agreed to store the encryption keys in China. As a result, Chinese authorities could make requests for user data without going through U.S. courts. China did not have its own system for independent judicial review of warrants, and there were only light penalties to police for overreach. Human rights groups worried that authorities would use their powers to spy on texts, emails, and other data from dissident users.[22]

Apple said that it would indeed comply with any legal request from the Chinese government for iCloud search, as it complied with legal requests for such data in the U.S. However, Apple said that it would refuse any "bulk" data-gathering requests and had not built a "backdoor" to data for the Chinese authorities.[23] Furthermore, Apple reminded customers that iPhone end-to-end encryption remained in place, and users could store all data on their phones without using iCloud storage at all.[24]

[b] In 2016, China had passed a cybersecurity law that required cloud companies to store Chinese citizens' data domestically and allow authorities to spot-check network operations. Jack Wagner, "China's Cybersecurity Law: What You Need to Know," The Diplomat, June, 1, 2017, https://bit.ly/2knS6Bg, accessed March 2018.

This document is authorized for use only in Prof. Sourya Joyee De's Cyber Security Risk Management 1.16.2020 at Indian Institute of Management - Raipur from Jan 2020 to Jul 2020.

Endnotes

[1] Dan Strumpf, "Apple's Tim Cook: No Point Yelling at China," *The Wall Street Journal,* December 7, 2017, https://www.wsj.com/article_email/apples-tim-cook-no-point-yelling-at-china-1512563332-lMyQjAxMTI3NDAwNzgwMjc5Wj/, accessed December 2017.

[2] Chen Guangcheng, "Apple Can't Resist Playing by China's Rules," *The New York Times,* January 23, 2018, https://www.nytimes.com/2018/01/23/opinion/apple-china-data.html, accessed March 2018.

[3] Elizabeth Weise, "Apple v FBI timeline: 43 days that rocked tech," *USA Today,* March 30, 2016, https://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/, accessed November 2017.

[4] Devlin Barrett and Ellen Nakashima, "Texas gunman's iPhone could reignite FBI-Apple feud over encryption," *The Washington Post,* November 8, 2017, https://www.washingtonpost.com/world/national-security/texas-gunmans-iphone-could-reignite-fbi-apple-feud-over-encryption/2017/11/08/0c2b3eb6-c48f-11e7-aae0-cb18a8c29c65_story.html?, accessed November 2017.

[5] Mikey Campbell, "FBI director says smartphone encryption hindering investigations 'across the board,'" *Apple Insider*, October 23, 2017, http://appleinsider.com/articles/17/10/23/fbi-director-says-smartphone-encryption-hindering-investigations-across-the-board, accessed November 2017.

[6] Ben Lovejoy, "Apple Once Again Dominates Smartphone Profits," *9To5Mac,* March 8, 2017, https://9to5mac.com/2017/03/08/aapl-iphone-profits-profitability-2016-strategy-analytics/, accessed November 2017.

[7]Anita Balakrishnan, "Apple market cap tops $800 billion for the first time," CNBC, May 8, 2017, https://www.cnbc.com/2017/05/08/apple-market-capitalization-hits-800-billion.html, accessed November 2007.

[8] Evan Perez and Tim Hume, "Apple opposes judge's order to hack San Bernardino shooter's iPhone," CNN.com, February 18, 2016, https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html, accessed March 2018.

[9] Leonhard Weese, "What does China's VPN Ban Really Mean?," *Forbes,* January 25, 2017, https://www.forbes.com/sites/leonhardweese/2017/01/25/what-does-chinas-vpn-ban-really-mean/#3f1663d650e3, accessed March 2018.

[10] Daniel Cooper, "What you need to know about Apple, VPNs and China," *Engadget,* August 2, 2017, https://www.engadget.com/2017/08/02/apple-vpn-restrictions-china/, accessed November 2017.

[11] Fitz Tepper, "Here's Tim Cook's explanation on why some VPN apps were pulled in China," Techcrunch.com, August 1, 2017, https://techcrunch.com/2017/08/01/heres-tim-cooks-explanation-on-why-some-vpn-apps-were-pulled-in-china/, accessed March 2018.

[12] Christina Larson, Steven Yang, and Yuan Gao, "What China's VPN Ban Means for Internet Users: Quicktake Q&A," Bloomberg, July 11 2017, https://www.bloomberg.com/news/articles/2017-07-11/how-china-s-vpn-ban-asserts-digital-sovereignty-quicktake-q-a, accessed November 2017.

[13] Senators Ted Cruz and Patrick Leahy, "Letter to Tim Cook," October 17, 2017, U.S. Senate Website, https://www.cruz.senate.gov/files/documents/Letters/20171017_tim_cook_letter.pdf, accessed November 2017.

[14] Farhad Manjoo, "Apple's Silence in China Sets a Dangerous Precedent," *The New York Times*, July 31, 2017, https://www.nytimes.com/2017/07/31/technology/apple-vpn-china-dangerous-precedent.html, accessed November 2017.

[15] Farhad Manjoo, "Apple's Silence in China Sets a Dangerous Precedent."

[16] Kyle Mullin, "Apple 'Kisses Ass' as Mainland Techies Bemoan App Store's Removal of Major VPNs," *The Beijinger*, July 30, 2017, https://www.thebeijinger.com/blog/2017/07/30/apple-kissing-ass-protect-their-revenue-china-mainland-techies-bemoan-removal-major, accessed March 2018.

[17] Yifu Dong, "Apple in China: WTF? A ChinaFile Conversation," *ChinaFile*, December 8, 2017, http://www.chinafile.com/conversation/apple-china-wtf, accessed March 2018.

18 Melissa Chan, "Apple is not the only tech company kowtowing to China's censors," *The Guardian,* January 6, 2017, https://www.theguardian.com/commentisfree/2017/jan/06/apple-china-censors-new-york-times, accessed March 2018.

[19] Dan Strumpf, "Apple's Tim Cook: No Point Yelling at China."

This document is authorized for use only in Prof. Sourya Joyee De's Cyber Security Risk Management 1.16.2020 at Indian Institute of Management - Raipur from Jan 2020 to Jul 2020.

[20] Chen Guangcheng, "Apple Can't Resist Playing by China's Rules."

[21] Apple, "iCloud operated by GCBD Terms and Conditions," https://www.apple.com/legal/internet-services/icloud/en/gcbd-terms.html, accessed March 2018.

[22] Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears," Reuters, February 24, 2018, https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060, accessed March 2018.

[23] Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears."

[24] Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears."

This document is authorized for use only in Prof. Sourya Joyee De's Cyber Security Risk Management 1.16.2020 at Indian Institute of Management - Raipur from Jan 2020 to Jul 2020.