Tim Cook, a Case Study on the Effects of Transformational Leadership on Privacy and IT Security

Author: Scott Perry, perry.sans@gmail.com
Accepted: December 21st 2016

Abstract

After the tragic events in December 2015, where two attackers killed 14 people in San Bernardino, California, the Federal Bureau of Investigation (FBI) requested Apple to assist in unlocking an iPhone used by one of the attackers (Lichtblau & Benner, 2016). This request sparked a firestorm debate between the US Federal Government and Apple that lasted 43 days and left lasting repercussions for privacy, encryption, and IT security. In the center of this debate was Apple Chief Executive Officer (CEO) Tim Cook, demonstrating transformational leadership and idealized influence by ensuring governments cannot force companies to compromise the security of their products or invade the privacy of their customers.

1. Introduction

In both business and IT security, when someone is appointed a manager, it is a common misconception that person is also going to be a leader. The misconception is that "management" and "leadership" can be used interchangeably (Kotter, 2013). Unfortunately, these two terms are not synonymous, but they can be complimentary and exceptional when they are used to describe someone like Tim Cook, the Chief Executive Officer (CEO) of Apple Inc. What makes Cook exceptional is his use of the transformational leadership principles to not only influence and guide Apple, but to affect change in the IT security industry worldwide by becoming a role model for advocating privacy and encryption. Cook's stance on privacy and encryption came to the public's attention after he stated Apple would not unlock an iPhone of a suspect in a domestic terrorist attack, even under enormous legal and political pressure. But this request is only the most recent battle between the IT industry and governments for privacy of personal data, battles such as the proposed "Clipper Chip" in the 1990's (Abelson et al., 2015, p. 1)

Before examining Tim Cook's influence and use of transformational leadership, transformational leadership needs to be defined. Transformational leadership "is the ability to get people to want to change, to improve, and to be led" (Hall et al. 2015). Transformational leadership can then be distilled down into four main factors: idealized influence, inspirational motivation, intellectual stimulation, and individual consideration. These four factors can be used to describe Cook in various ways; however, "idealized influence" is the most applicable when discussing Tim Cook's direct influence on Apple's policy on privacy and encryption. Idealized influence "describes managers who are exemplary role models for associates. Managers with idealized influence can be trusted and respected by associates to make good decisions for the organization" (Hall et al. 2015). This factor is particularly evident in Tim Cook because of his unwavering stance to protect the privacy and security of Apple devices, and subsequently, Apple's customers.

Scott Perry;perry.sans@gmail.com

1.1. Influence at Apple

Before Tim Cook came to the forefront of the privacy battle between government and citizens in 2016, he came to the forefront of Apple leadership in August of 2011 when he was named the CEO of Apple Inc ("Apple - Press Info - Steve Jobs Resigns as CEO of Apple," 2011). Since then, his leadership style emphasized the idealized influence of transformational leadership, but in a stark contrast to how Steve Jobs led Apple. Jobs managed at the "pixel" level, where Cook embodies idealized influence, becoming an exemplary role model, instead of a micromanager. Steve Jobs can be viewed as a "wartime" leader where he had to take aggressive actions to bring his company back from the brink of destruction. Tim Cook, on the other hand, can be viewed as a "peacetime" leader who needs to perpetuate and grow the most valued company in the world (Lashinsky, 2015). Successes such as the iWatch, Apple Pay, and the recent versions of the iPhone have proven his leadership style as effective. Cook's willingness to take on the tough battles, such as the fight for privacy, makes him a role model and inspiration to his employees. In a commencement speech at George Washington University in 2015, Cook emphasized his point when he stated, "The sidelines are not where you want to live your life. The world needs you in the arena" (Eadicicco, 2015).

2. The Battle for Privacy

After the tragic events in December 2015, where two attackers killed 14 people in San Bernardino, California, the Federal Bureau of Investigation (FBI) requested Apple to assist in unlocking an iPhone used by one of the attackers (Lichtblau & Benner, 2016). This request sparked a firestorm debate which intensified on February 16, 2016 when Federal Magistrate Judge, Sheri Pym, ordered Apple to assist the FBI in unlocking one of the attacker's iPhone 5c (Weise, 2016). On the same day, Tim Cook published a 1,100-word response to the request on Apple's website. The response was not a simple refusal to comply with the court order but a demonstration of how his transformational leadership extends outside his sphere of influence at Apple. Because it is not just a single iPhone at stake, but the precedence the government can have access to your encrypted

data; Cook's reply stated, "This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake" (Cook, 2016). Cook goes on to argue that customers of Apple "…carry so much personal information on our phones today, and there are new data breaches every week affecting individuals, companies, and governments…if we lose control of our data, we put both our privacy and our safety at risk" (Cook, 2016). Cook points out granting access to customer encrypted data would set a legal precedent to expand the powers of the government and could lead to other means of uncontrolled electronic surveillance such as intercepting customer data transmissions, tracking locations, or even accessing the camera and microphone without the customer knowing (Cook, 2016). This unfettered access to customer data would undermine Apple, and consequently IT security globally, as the legal precedent would be set and other companies would have to comply.

In Tim Cook's letter to Apple's customers, he frankly admits Apple engineers could design and implement a unique and vulnerable operating system (OS) which could undermine the security features of the iPhone 5c the FBI wants unlocked (Cook, 2016). But Cook has the foresight to know Apple's customers and employees need to trust both Cook, and the Apple products they buy. If a unique and vulnerable OS was developed for this specific event (or even a security backdoor or access in future OS's) such a vulnerability would make its way outside of Apple's control and undermine the privacy, security, trust in Apple products, and ultimately Cook' leadership.

3. Privacy and IT Security

The legal battle between Apple and the FBI brought to the public's attention an ongoing war, or more fittingly, an arms race, which has been raging since someone first used an electronic device as an instrument to commit a crime. This arms race is between the developers of the OS, such as Apple, and the investigators and computer forensic experts who want to examine the computers for evidence of criminal activity. The developers of the OS want to make a more secure and stable OS while forensic experts want to be able to examine those devices for evidence. Encryption is certainly nothing new, nor is it unique to computing devices as has been demonstrated using Battista cipher

disks, Jefferson disks, and later communication devices like the Enigma Machine (Security 401 "Security Essentials Bootcamp Style", 2015). What is new, is the complexity and speed of modern day computers and especially mobile devices such as the iPhone.

In fact, the iPhone is a perfect example of the evolution of mobile devices and their impact on privacy, security, and law enforcement's quest to find justice by examining suspect devices like the iPhone 5c in the San Bernardino attack. The iPhone 5c has an A5 processor which means this model of iPhone is encrypted with 256bit AES at the hardware level (Edwards, Mahalik, & Murphy, 2016). This hardware-level encryption allows the user data on the phone to remain encrypted and out of the hands of computer forensic experts when a passcode is not available, such as in the case of the iPhone 5c in the San Bernardino attack. Previously to the A5 processor, law enforcement and computer forensic experts could use specialized tools which would alter the boot code of an iPhone or similar device to allow access to the decrypted, full content. But, each time an exploit or means to access the data is found, Apple patches the flaw and makes the data more secure. Continuing that trend, the descendent processor chips, such as the A6, A7, and A8, have become more and more secure with each release (Edwards, Mahalik, & Murphy, 2016). Apple's ongoing quest to make its customers' data more secure is a direct result of Cook's leadership: "Customers expect Apple…to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data" (Cook, 2016). However, this safeguarding of data is in direct conflict with the government and law enforcement's war for "exceptional access" in the name of national security (Abelson et al., 2015, p. 1) and is at the root of the battle between the Apple and the FBI.

3.1. Historical Reference

The government's request for "exceptional access" to digital media is a well-established request in response to a developing threat to national security and domestic terrorism. In the late 1990's, the governments in the United States and the United Kingdom were lobbying to have networked systems on the Internet redesigned to ensure

the government still had access (Abelson et al., 2015, p. 1). The governments wanted a repository of keys for encryption which would grant them immediate and exclusive access to systems for criminal and national security investigations. One of the proposed solutions was the "Clipper Chip", which was specifically targeted towards encrypted voice communications ("Clipper Chip," 2016). The clipper chip would enable a trusted third party to retain a copy of all the keys necessary for the government to access the encrypted communications. Even under the enormous pressure of the federal government, technology firms and telecommunication agencies prevented the implementation of the Clipper Chip because of the potential cost, governance issues, and the overall risk to security (Abelson et al., 2015, p. 1).

Since the debate in the late 1990's, the Internet has exploded and the use of Data Encryption Standard (DES) and then more advanced encryption such as the Advanced Encryption Standard (AES) has made the argument moot as the wheels of industry and commerce move much faster than the development and implementation of laws (Abelson et al., 2015, p. 8)

The merit of the prevention of a key escrow system and the preservation of encryption systems has been further highlighted by large data breaches such as the OPM hack and the RSA/EMC hack (Abelson et al., 2015, p. 9). These compromises are especially poignant because the OPM breach exposed an extremely large data-set of personal information and the RSA/EMC breach undermined the legitimacy of a large certificate-issuing authority (Zetter, 2012). These attacks help highlight the need to protect valuable data that needs to be encrypted and safeguarded. If an attacker had access to a key-escrow system, large-scale data compromises will become exponentially easier and wide-spread. This is the rationale behind Cook's refusal to compromise the encryption integrity of Apple products and to grant exceptional access. If Apple modified the iPhone OS to allow exceptional access to law enforcement, that exceptional access would eventually become public and be compromised as has been highlighted by breach after breach. Companies can no longer design products with access or "back doors", governments and law enforcement must continue to ensure due legal process and advance their arms race to unlock the encryption where they can.

Scott Perry;perry.sans@gmail.com

4. Conclusions

The Apple vs FBI battle ended on March 29, 2016, when Federal Magistrate Judge, Sheri Pym, rescinded her original order for Apple to assist the FBI in unlocking the iPhone 5c. However, the repercussions of that battle will be evident for a long time. Because of Tim Cook's idealized influence in becoming a role model and a leader for the advocacy of privacy, Apple won the latest battle for privacy between the governments and private citizens. Sensitive data will continue to be produced by individuals and companies; such data must be safeguard with encryption at rest and in transit. Leaders such as Tim Cook will need to continue to come forward to protect the data, rationale, and ideals behind protecting that data.

Scott Perry;perry.sans@gmail.com

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Weitzner, D. J. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *J Cyber Secur*, tyv009. doi:10.1093/cybsec/tyv009

Apple - Press Info - Apple Leadership - Tim Cook. (n.d.). Retrieved from http://www.apple.com/pr/bios/tim-cook.html

Apple - Press Info - Steve Jobs Resigns as CEO of Apple. (2011, August 24). Retrieved from http://www.apple.com/pr/library/2011/08/24Steve-Jobs-Resigns-as-CEO-of-Apple.html

Clipper Chip. (2016, June 26). Retrieved November 21, 2016, from http://www.cryptomuseum.com/crypto/usa/clipper.htm

Cook, T. (2013, May 29). Apple CEO and Fuqua alum Tim Cook talks leaderhship at Duke. Interview. Retrieved November 20, 2016, from http://www.fuqua.duke.edu/news_events/feature_stories/tim-cook-talks-leadership/#.WDGhw_krKHt

Cook, T. (2016, February 16). Customer Letter - FAQ - Apple. Retrieved November 19, 2016, from http://www.apple.com/customer-letter/answers

Eadicicco, L. (2015, October 15). Best quotes from Apple CEO Tim Cook - Business Insider. Retrieved December 19, 2016, from http://www.businessinsider.com/apple-ceo-tim-cook-best-quotes-2015-10/#the-sidelines-are-not-where-you-want-to-live-your-life-the-world-needs-you-in-the-arena-1

Edwards, S., Mahalik, H., & Murphy, C. (2016, February 23). SANS Digital Forensics and Incident Response Blog | A Technical Autopsy of the Apple - FBI Debate using iPhone forensics | SANS Institute. Retrieved November 19, 2016, from https://digital-forensics.sans.org/blog/2016/02/23/iphone-forensics-separating-the-facts-from-fiction-a-technical-autopsy-of-the-apple-fbi-debate/

Scott Perry;perry.sans@gmail.com

Hall, J., Johnson, S., Wysocki, A., Kepner, K., Farnsworth, D., & Clark, J. L. (2015, October). Transformational Leadership: The Transformation of Managers and Associates. Retrieved November 11, 2016, from http://edis.ifas.ufl.edu/pdffiles/HR/HR02000.pdf

Johnson, K., Swartz, J., & Cava, M. (2016, March 29). FBI hacks into terrorist's iPhone without Apple. Retrieved November 18, 2016, from http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/

Kotter, J. P. (2013, January 9). Management Is (Still) Not Leadership. Retrieved November 20, 2016, from https://hbr.org/2013/01/management-is-still-not-leadership

Lashinsky, A. (2015, March 26). Apple's Tim Cook leads different. Retrieved November 20, 2016, from http://fortune.com/2015/03/26/tim-cook/

Lichtblau, E., & Benner, K. (2016, February 17). Apple Fights Order to Unlock San Bernardino Gunman's iPhone - The New York Times. Retrieved November 18, 2016, from http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0

Metz, C. (2016, April 5). Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People | WIRED. Retrieved November 21, 2016, from https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

Schwartz, N. D. (2001, June 7). RSA Security Faces Angry Users Over Breach - The New York Times. Retrieved November 18, 2016, from http://www.nytimes.com/2011/06/08/business/08security.html

Security 401 Security Essentials Bootcamp Style. (2015). Baltimore, MD: SANS Institute.

Weise, E. (2016, March 30). Apple v FBI timeline: 43 days that rocked tech. Retrieved November 18, 2016, from http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/

Scott Perry;perry.sans@gmail.com

Zetter, K. (2012, February 2). VeriSign Hit by Hackers in 2010 | WIRED. Retrieved November 18, 2016, from https://www.wired.com/2012/02/verisign-hacked-in-2010/

Scott Perry;perry.sans@gmail.com