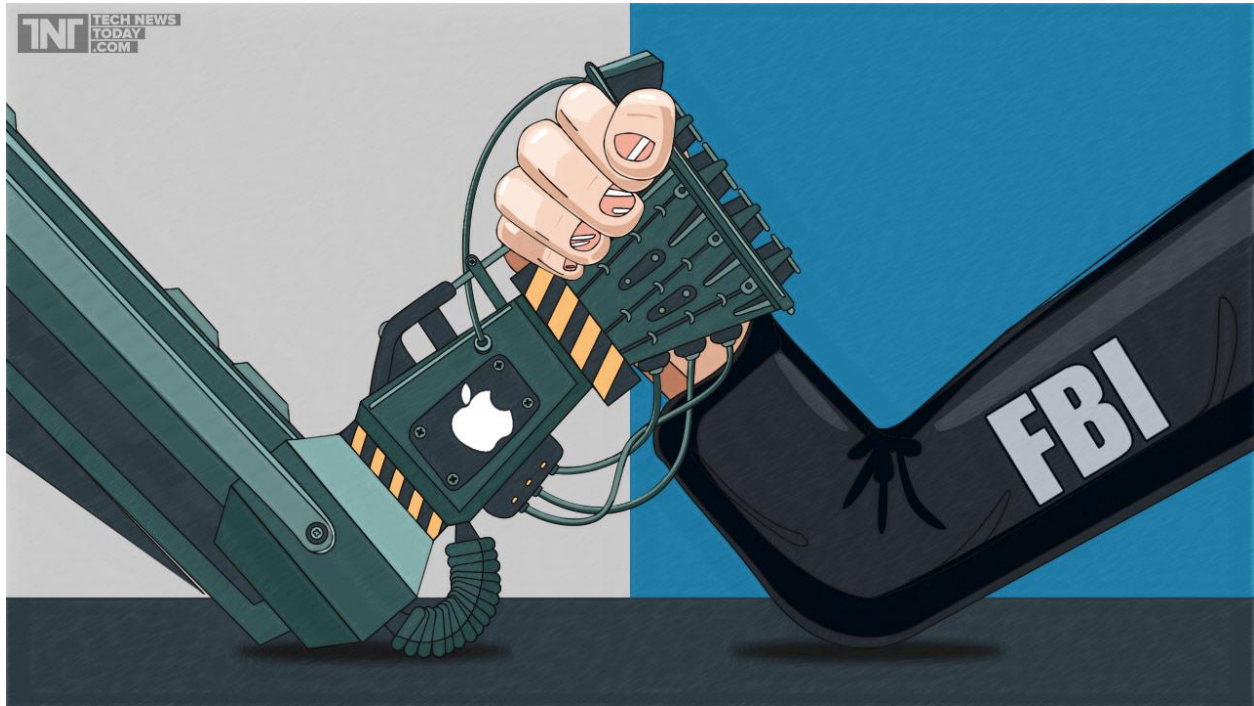


Arthur W. Page

ARTHUR W. PAGE SOCIETY

Walking the “Encryption Tightrope”: Getting to the Core of Apple’s Privacy and Security Battle with the FBI



(Graphic Source: Raza, 2016)



Abstract

Following the December 2015 San Bernardino shooting, the FBI asked Apple to provide access to the perpetrator's iPhone, forcing Apple to stand its ground on protecting consumer privacy. Agreeing to provide access would jeopardize its consumers' privacy by creating a "backdoor" into the iPhone which Apple deemed unacceptable. Apple's decision was met with praise and criticism by the public and other technology companies. Finally, the FBI used a third party to hack the iPhone. Although consumer privacy was eventually compromised, Apple's response set a precedent and started an important dialogue across the business world about customer privacy and security.



Table of Contents

Overview: Taking a Bite Out of The Apple	1
Company Background: Getting “Siri”ous	3
History of Apple	3
Mission Statement	4
“Core” Values	4
Corporate Reputation	5
Corporate Character	6
Situation Analysis	7
Legal Precedence and Implications	8
Timeline	8
Response: How the (Apple) Pie was Sliced	11
Public Response	11
Social Media Response	12
News Media Response	14
Response by Silicon Valley	16
Business Performance: Will One Bad Apple Spoil the Whole Bunch?	17
Financial Impact	17
Reputation Impact	19
Looking Ahead: Apple-y Ever After	20
References: Isn’t There an App for That?	21



Overview: Taking a Bite Out of The Apple

In December of 2015, a married couple named Syed Rizwan Farook and Tashfeen Malik burst through the doors of Farook's office holiday party in San Bernardino, CA. The couple had spent months planning a terrorist attack that came to fruition when they opened fire on Farook's co-workers killing 14 and injuring 22. Police were called to the scene, engaging in a gunfight with the perpetrators, killing Farook and Malik. After the incident, investigators searched the couple's home finding large amounts of ammunition, weapons and pipe bombs (Mozingo, 2015).



(Source: Newseum, 2015)

During the investigation, the FBI requested data from Farook's iPhone that might contain valuable information about the attack. Apple provided the data that had been backed up on iCloud, however, Farook had not backed up his phone for several weeks before the attack. Although the FBI had Farook's password protected-phone in their possession, the phone's operating system was setup to automatically erase all local data after too many



incorrect password attempts to unlock the phone. Because no one knew Farook’s password, this left the FBI with few options for unlocking the phone and accessing the data.

The FBI then turned to Apple again, requesting that the company unlock Farook’s phone, specifically asking Apple to create a custom version of iOS for Farook’s phone, also known as a “backdoor” in. This would allow someone to connect an external computer to the phone and unlock the device by “brute force.” Apple’s CEO, Tim Cook, refused to meet this demand, due to the customer privacy and safety concerns that would arise from the creation of this software.

In a public letter to Apple’s customers, Cook called this request, “an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority (Apple, 2016).” Apple appealed the request because it believed that the creation of this “backdoor” to the iPhone was too dangerous. Apple argued that if it were to create the software for this case, it would be providing a way for hackers to unlock other Apple devices (Crovitz, 2016).

February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

[Answers to your questions about privacy and security >](#)

(Source: Apple, 2016)



This case is relevant to multiple corporate communication areas including data privacy, government relations and issues management. Because Apple is such a well-known company, when it declined to decrypt the iPhone its decision and justification was extremely public and put the company at risk for alienating certain stakeholder groups. As a result, Apple had to figure out how to navigate and explain the ethical and legal ramifications of its decision to all its stakeholders as its decision was heavily debated within the court of public opinion. Furthermore, this public battle between the FBI and Apple brought the tension between national security and individual and corporations' rights to the forefront. It raised issues of privacy and national security, of freedom of speech, and even foreign policy considerations with respect to repressive regimes and those governments hoping to track journalists' sources. Lastly, this case is an important milestone in the evolution of the digital world and technology. Apple's argument about potential government misuse or criminal appropriation, and the government's counter that the tradeoff with privacy in certain cases is needed to fight terrorists, will help decide how *all* companies balance safety and security in the future against a suspicion about government intrusion into peoples' daily lives.

Company Background: Getting "Siri"ous

History of Apple

Founded by Steve Jobs, Steve Wozniak and Ronald Wayne in 1976, Apple has been at the forefront of technological innovation for the last four decades. Apple is the world's largest technological company in terms of total assets, and the largest information technology company in terms of revenue (Chen, 2015). Since its genesis, Apple has set the standard for functional, innovative and user-friendly consumer software and electronics. The company has had its ups and downs, including the death of Steve Jobs in 2011. Through it all, one thing that has been consistent is Apple's authority in the technology industry. Apple has been called groundbreaking, brilliant and a company that leads by example (Bajarin, 2012).

Although Apple has a strict customer privacy policy, the 2016 incident is not the first time the company has faced privacy concerns. The initiation of the iCloud in 2011 caused



consumer concern amongst Apple's customers. Speculations were made that iCloud played a part in the leaking of private celebrity photos. This caused Apple to work on its security issues and protect its customer's privacy (Timberg, 2014). Now Apple has a strong customer privacy policy that it refuses to compromise.

Mission Statement

Apple has never formally published a mission statement, however, the statement found at the bottom of all of its most recent press releases, is viewed by many as Apple's version of a "Mission Statement". The statement is as follows:

"Apple revolutionized personal technology with the introduction of the Macintosh in 1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch and Apple TV. Apple's four software platforms — iOS, macOS, watchOS and tvOS — provide seamless experiences across all Apple devices and empower people with breakthrough services including the App Store, Apple Music, Apple Pay and iCloud. Apple's 100,000 employees are dedicated to making the best products on earth, and to leaving the world better than we found it."

"Core" Values

Although Apple does not expressly publish a mission statement, it lists six core company values on its website. Each value is discussed in detail and Apple's site provides multiple examples of how it incorporates its values into everything they do and create as a company.

Apple's Values:

- **Accessibility**
- **Education**
- **Environment**
- **Inclusion and Diversity**
- **Supplier Responsibility**
- **Privacy:** Apple knows the importance of consumer trust. Privacy is one of Apple's core values, taken into consideration when creating Apple products. Because the company respects its customer's privacy, Apple products have been designed to provide



maximum security to its customers' data (Apple Inc., 2016). The software, hardware and services of an iOS device are built to work together to encrypt data and keep it safe on the iCloud server. Apple does not have a backdoor for this server and no one other than Apple has access to this server (Apple Inc., 2016). These stringent security policies are the reason that Syed Farook's iPhone could not be unlocked. The data on Farook's phone had not synchronized with iCloud and incorrect passcode attempts would have completely erased it.

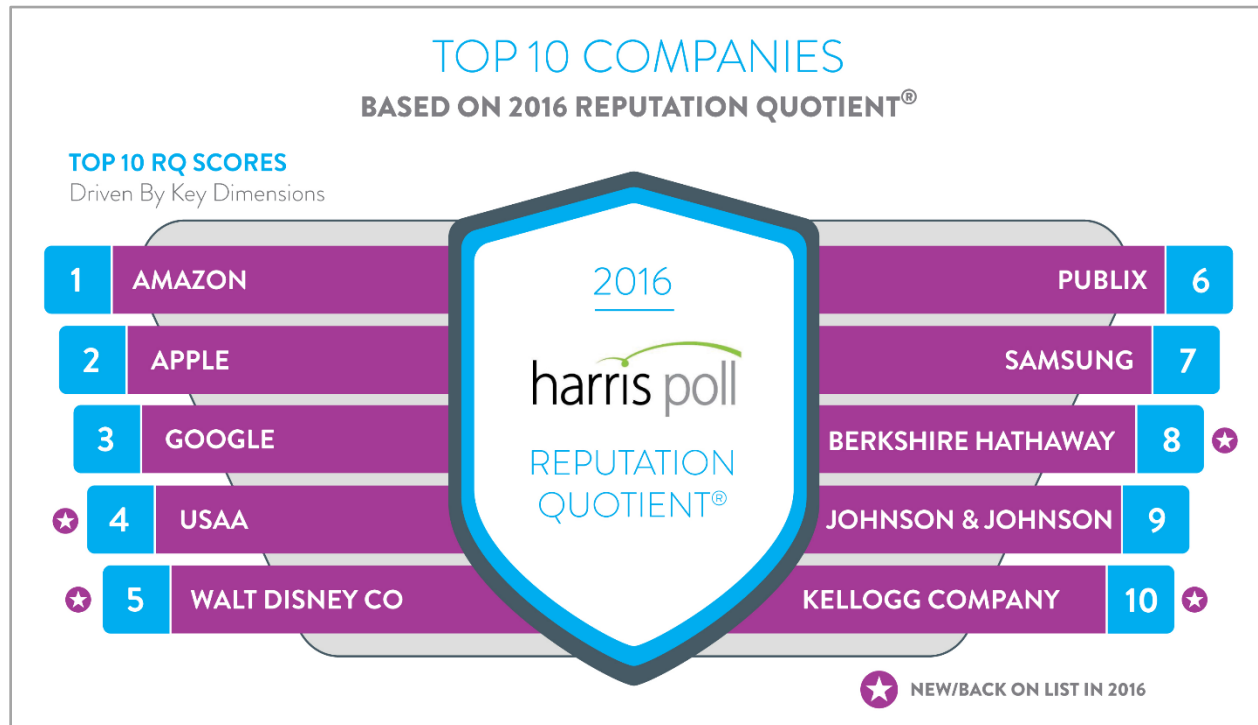
Corporate Reputation

According to the Arthur W. Page Society, all actions of an organization are a reflection of its defined character. The beliefs and the actions of the company towards its stakeholders help in building its character. The perception of this character is the measure of its reputation. Thus, reputation is the non-financial component of a company on which the other financial factors depend (Ragas & Culp, 2014, p. 28). A successful organization with a good reputation is reflected not only by its profits but also by its services towards its stakeholders (Arthur W. Page Society, 2012).

Apple has worked hard to establish and maintain strong relationships and trust with its customers. This effort, combined with Apple's high quality products, has established a very strong corporate reputation. A poll, conducted by Morning Consult, of 1,935 Americans on February 24 and 25, 2016, showed that 54% of respondents trusted Apple with their data and personal information. In the same poll question, Apple was more trusted by respondents than other technology companies, including Uber, Facebook and Google (O'Neill, 2016). Apple earned a reputation quotient of 83.03 from The 2016 Harris Poll RQ[®] (Reputation Quotient), which was the second highest reputation score among the general public (Harris Poll, 2016).



Finally, Apple has held the number one spot on Fortune's *World's Most Admired Companies Top 50 All-Stars* list for the past nine years (Fortune, 2016).



(Source: Harris Poll RQ®, 2016)

Corporate Character

A company defines its Corporate Character on the basis of its “mission, purpose, values, culture, business model, strategy, operations, and brand”. This creates a company’s brand identity which is relatable to its customers and is represented consistently through all its communications (Arthur W. Page Society, 2012, p. 5). A company should maintain this corporate character all throughout its hierarchy levels by adhering to its core purpose, values, and culture, leading to a consistent message of corporate character to all the stakeholders.

As indicated by its high reputation rankings, Apple generally communicates its corporate character effectively to its customers. The message is that Apple is innovative, high quality and trustworthy. These values have created something that many companies want, but few achieve



such a high degree of brand loyalty (Smith, 2014). This case served as a high-profile test of Apple's corporate character and reputation during a complex, high-profile situation.

Situation Analysis

Over the years, Apple has become a leader in the technology world. The company is credited with redefining product categories, such as the MP3 player and smartphone, and forging new territory with technological innovation and exceptional design. Each time Apple introduced a new product, both consumers and other tech manufacturers followed, embracing Apple's vision of each new device and the software that accompanied it (Bolluyt, 2015).

Furthermore, Apple and its CEO, Tim Cook, have become more outspoken on their stance regarding societal issues, making Apple and Cook leaders not just in business, but also in terms of corporate social responsibility. After Steve Jobs stepped down as CEO, Cook began making Apple more transparent publishing an annual report on suppliers and working conditions for more than a million factory workers. Speaking on behalf of Apple, he has also taken aggressive positions on social and legal issues, pushing a once secretive company into the center spotlight of some highly charged issues (Benner & Perloth, 2016).

More specifically, privacy has been a priority for Apple and Tim Cook for a long time. At a tech conference in 2010, he said Apple "has always had a very different view of privacy than some of our colleagues in the Valley." (Benner & Perloth, 2016). Those views on privacy toughened over the years as customers globally began entrusting more personal data to Apple's iPhones and the number of requests from government officials worldwide asking the company to unlock smartphones rose.

After a while, Cook and other Apple executives committed not only to lock up customer data, but to do so in a way that would put the keys into the hands of the customer, not the company. By the time Apple released a new mobile operating system, iOS7, in September 2013, the company was encrypting all third-party data stored on customers' phones by default (Benner & Perloth, 2016).



Legal Precedence and Implications

Apple's stance on privacy and security comes from a long-held, business-based decision to protect its brand with customers who prize the data protection built into iPhones. In a New York legal dispute with prosecutors in 2015, Apple argued, "forcing Apple to extract data... absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand," (Harris, Shane 2016).

The 2016 court's order to create a new technological method that would allow government officials to override login safeguards built into Apple's latest phones was completely unprecedented. Not only had something of this magnitude never been requested of a technology company by the U.S. government, no government had ever made a demand of such substance. Furthermore, if Apple obliged to this order, it would have set a legal standard for the U.S. government and other foreign governments to make similar requests of Apple and other technology companies and in future legal cases.

Timeline

- **December 2, 2015:** Shooting occurs in San Bernardino, California killing 14 and wounding 22.
- **February 16, 2016:** The Federal Bureau of Investigation (FBI) issues a court order to Apple to unlock the phone of Syed Farook, the terrorist involved in the shooting attacks in San Bernardino (Source: Weise, 2016).
Apple responds to the FBI's request by issuing a statement on their website saying they "oppose this order, which has implications far beyond the legal case at hand," (Source: Apple, 2016).
- **February 17, 2016:** Josh Earnst, a spokesperson for the White House, responds to Apple claiming that the FBI was not asking them to create this backdoor encryption but merely have them open the single phone of the terrorist (Source: Apple vs FBI, 2016).
- **February 18, 2016:** Apple is told they have until February 26, 2016 to reply to the court order to unlock the phone.



Twitter founder, Jack Dorsey, tweets from his account in support of Tim Cook, Apple's CEO, on his decision to not unlock the phone. Facebook also releases a statement supporting Apple (Source: Apple vs FBI, 2016).

- **February 19, 2016:** Donald Trump gives his opinion on the Apple vs. FBI case during a campaign rally in South Carolina. Trump urges his supporters to boycott Apple until they help unlock the phone.

The Department of Justice files a motion against Apple asking them to comply with the FBI and unlock the phone (Source: Apple vs FBI, 2016).

- **February 24, 2016:** Apple CEO Tim Cook is interviewed by ABC's David Muir. Cook speaks of his concerns for safety and privacy involving a backdoor access to the iPhone. Cook reiterates that Apple has cooperated with the FBI but will continue to put its customers' safety first (Source: Apple vs FBI, 2016).



(Source: ABC News, 2016)

- **February 25, 2016:** Apple files a motion to vacate the previously issued court order, stating that the FBI is "attempting to expand the use of All Rights Act" (Source: Apple vs FBI, 2016).
- **February 26, 2016:** Major tech companies, including Google, Facebook, and Twitter, issue statements saying they will file friend of the court briefs in support of Apple (Source: Weise, 2016).



- **February 29, 2016:** Judge James Orenstein of the US District Court of the Eastern District of New York rules against the Department of Justice’s request to sidestep a passcode on the iPhone of a criminal involved in a drug case (Source: Apple vs FBI, 2016).
- **March 1, 2016:** A court hearing labeled “The Encryption Tightrope: Balancing Americans’ Security and Privacy,” is held in front of the House Judiciary committee involving representatives from both Apple and the FBI (Source: Tepper, 2016).
- **March 3, 2016:** 17 major tech companies publicize their support for Apple in their decision. Some big names providing support are Amazon, Facebook, Cisco, Microsoft, Mozilla, Yahoo and Google (Source: Weise, 2016).

March 3, 2016

Facebook and Industry Peers Support Apple in Amicus Brief

“Forcing engineers to build security vulnerabilities into products to allow extraordinary government access is an unprecedented legal step that would weaken security for everyone. We are proud to join our peers today in urging the court to reject the government’s demands,” – Colin Stretch, Facebook General Counsel

(Source: Facebook, 2016)

- **March 10, 2016:** The Justice Department replies to Apple’s motion to vacate the court order stating that the FBI’s request was “modest” as they only wanted to open the phone of the terrorist and that was it (Source: Weise, 2016).
- **March 15, 2016:** Apple responds to Justice Department comment stating that the government is forcing Apple to assist them without having the official authority to do so (Source: Weise, 2016).
- **March 21, 2016:** While at a launch event for the new iPhone SE, CEO Tim Cook speaks out about Apple’s stance on privacy with regards to their dispute with the FBI. Cook states, “We



owe it to our customers and we owe it to our country. This is an issue that affects all of us and we will not shrink from our responsibility,” (Source: Apple vs FBI, 2016).



(Source: Goldman, 2016)

- **March 28, 2016:** The Justice Department announces they have unlocked the terrorist’s iPhone using a third party. The Justice Department says it will not release how this was accomplished (Source: Weise, 2016).
- **March 29, 2016:** At 4:44pm Pacific time, Judge Sheri Pym withdraws the case against Apple that began on February 16, 2016 and the case comes to an end (Source: Weise, 2016).

Response: How the (Apple) Pie was Sliced

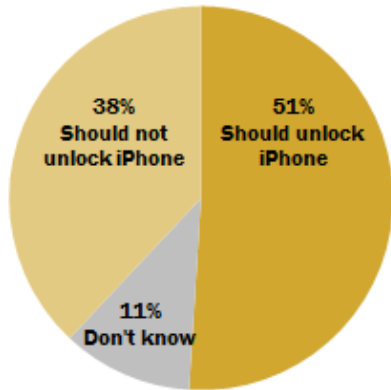
Public Response

When the news broke, the public immediately began to take sides. The Pew Research Center surveyed the general American public and asked their opinions of the case. The results indicate that, of those surveyed, 51% believe Apple should help the FBI unlock the phone, while 38% support Apple’s stance of not unlocking the phone (Maniam, 2016). In a national online poll conducted by Reuters/Ipsos, results showed again that the public was pretty divided on who’s side to take with about 45% agreeing with Apple’s opposition and 35% disagreeing.



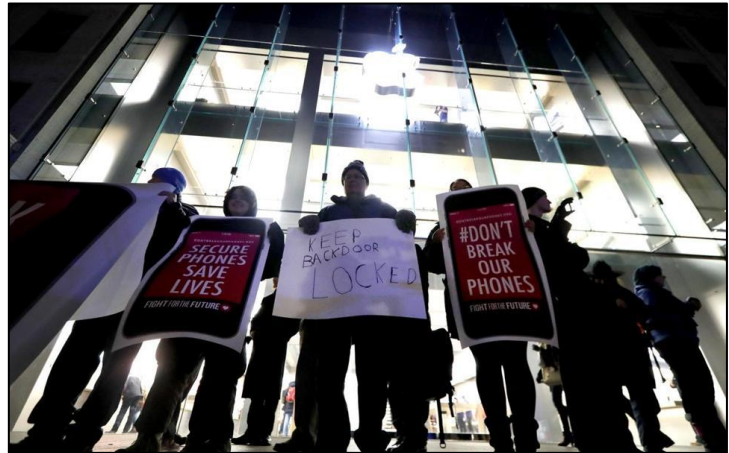
About half say Apple should unlock terror suspect's iPhone; 38% disagree

In response to court order tied to ongoing FBI investigation of San Bernardino attacks, Apple ...



Source: Survey conducted Feb. 18-21, 2016.
Figures may not add to 100% because of rounding.

PEW RESEARCH CENTER



(Sources: Maniam, 2016 & Bedford, 2016)

People also responded online via social media with their opinions about the case and showed up at Apple stores across the country to show support for Apple's stance and protest the FBI's demand.

Lastly, one of the most notable public responses came from Salihin Kondoker, a Muslim man and the husband of one of the San Bernardino shooting victims. Kondoker submitted a letter to the judge in support of Apple's position. In the letter, he says, "I believe privacy is important and Apple should stay firm in their decision. Neither I, nor my wife, want to raise our children in a world where privacy is the tradeoff for security. I believe this case will have a huge impact all over the world" (Kondoker, 2016).

Social Media Response

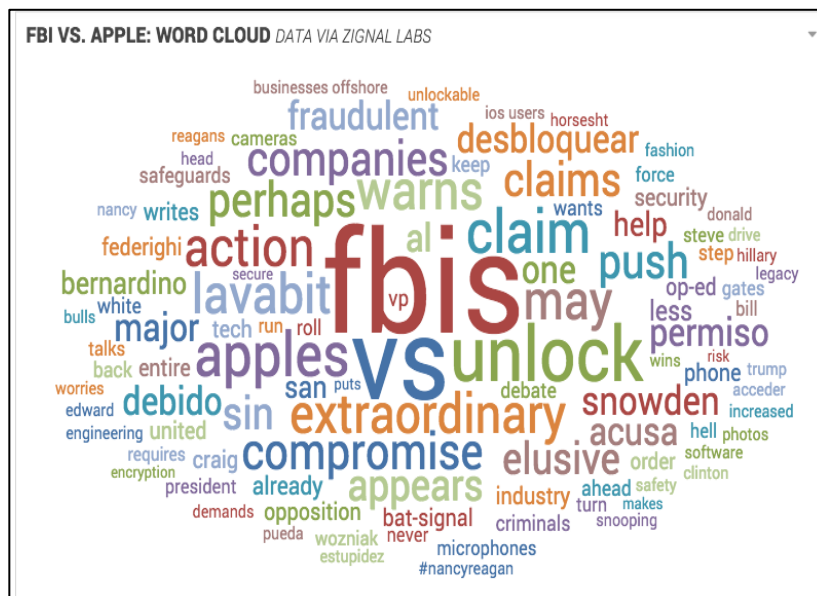
The story trended on multiple social media channels throughout its duration. Signal Labs, a social media analytics company, measured and tracked the online chatter at multiple points during the case. Signal Labs took a 24-hour snapshot of the conversation on Twitter after



Tim Cook responded to the court's demand with his public letter. During this time, the case's mention volume averaged in at around 7,115 mentions an hour, with nearly 172,000 per day. They also created a word cloud to visually represent what people were talking about most in regards to the case (Dietrich, 2016).



(Source: Hughes, 2016)



(Source: Dietrich, 2016)



News Media Response

News media and blogs around the world immediately began covering the Apple v. FBI case as soon as the federal court ordered Apple to assist in unlocking the iPhone. Every major news outlet and news blog seemed to be covering the story including, *BBC*, *TechCrunch*, *The Washington Post*, *New York Times*, *CNBC*, *NPR*, *TIME Magazine*, *Last Week Tonight with John Oliver* and *Wired*, to name a few. Steady media coverage continued to analyze the FBI's demand and Apple's response through September 2016, long after the FBI could unlock the iPhone, through an unnamed third-party, and after they dropped their demand on March 28, 2016.

The New York Times

TECHNOLOGY

Explaining Apple's Fight With the F.B.I.

By **MIKE ISAAC** FEB. 17, 2016

    | 

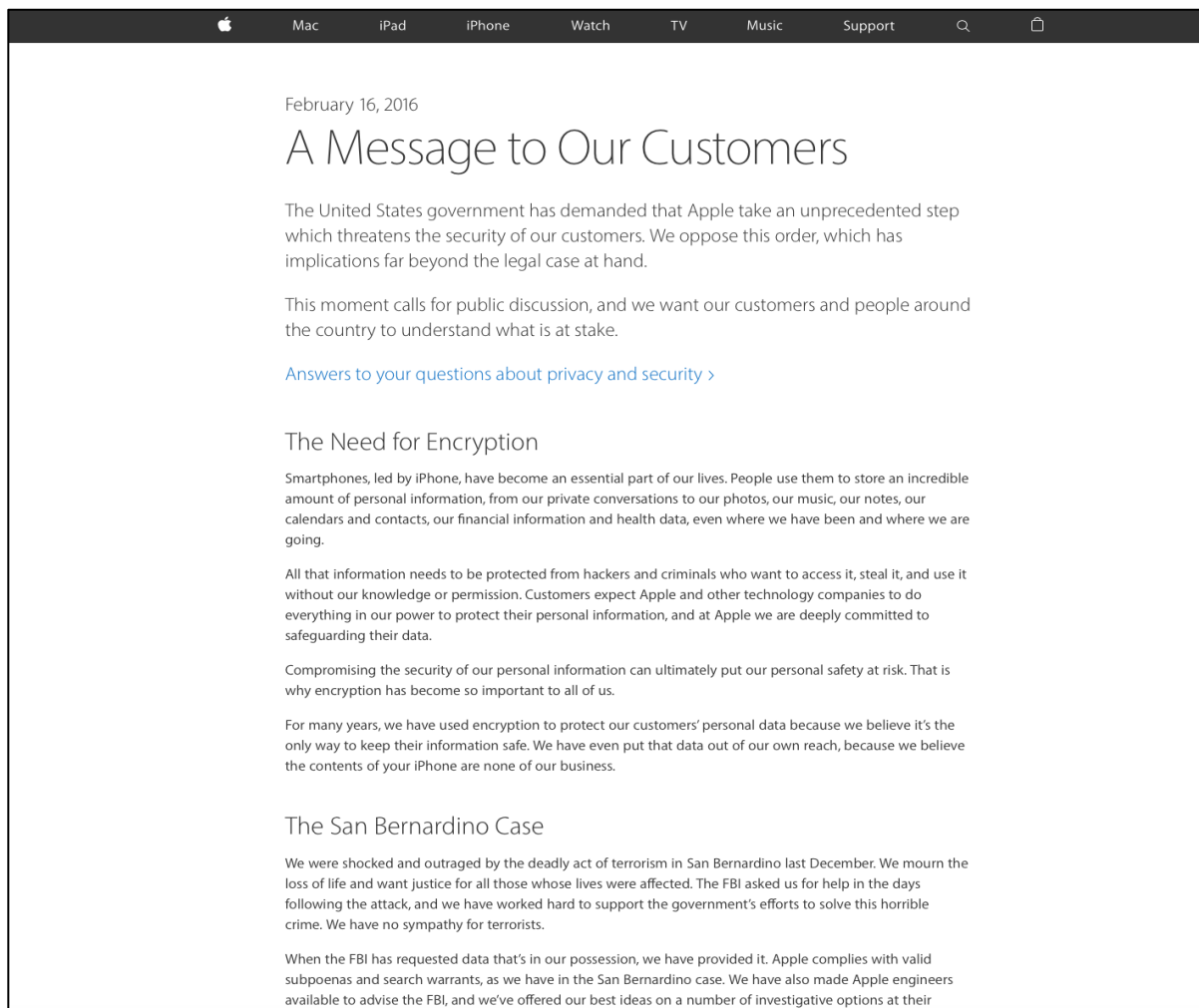
(Source: Isaac, 2016)

Many news outlets remained neutral in their reporting and attempted to explain the nuances of the FBI's demand and why Apple was opposing it. As the case developed, media also reported on who was taking whose side from influential opinion makers, to large corporations, like Amazon, to the 2016 Presidential candidates. Multiple news outlets also published op-ed articles with authors either siding with the FBI or Apple and political cartoons depicting the situation.

On February 18, 2016, *The Washington Post* published an op-ed article written by Bruce Schneier, a security technologist and lecturer at the Kennedy School of Government at Harvard University, titled: "Why You Should Side with Apple, not the FBI, in the San Bernardino iPhone Case." Finally, many media outlets polled readers to see which party readers sided with to gauge public opinion on topics including privacy rights, security and government access.



At the start of this incident, Apple CEO, Tim Cook, did not hold a formal press conference, but rather wrote a personal response to the motion, via a message to Apple customers which was posted on its website, about his stance on the case and explaining why Apple would not create the “backdoor” the FBI requested of them. At the same time that Apple posted the customer letter, it created an FAQ section on its website that addressed privacy and security questions more in depth. (Apple, 2016)



(Source: Apple, 2016)

As far as speaking directly with the media, Tim Cook sat down with David Muir from *ABC World News* for his first exclusive press interview regarding the case. Only a small portion of the interview aired on TV on February 24, 2016. However, the full-length interview was made available online the same day and picked up and shared by multiple news outlets and blogs. On



March 10, Tim Cook sat down with *TIME*'s Nancy Gibbs and Lev Grossman to discuss Apple's rapidly escalating fight with the FBI over encryption. That interview transcript was made available on *TIME*'s website March 17, 2016 and finally, on March 28, 2016, the same day the FBI dropped its demand, *TIME Magazine* released a cover story about the interview and the case in its entirety. Also just before the court dropped its demand, on March 21, 2016, Apple held a press conference. During the conference, Cook talked about the ongoing conflict with the FBI by saying, "We have a responsibility to protect your data and your privacy. We will not shrink from this responsibility." (Dillet, 2016).



(Source: *TIME*, 2016)

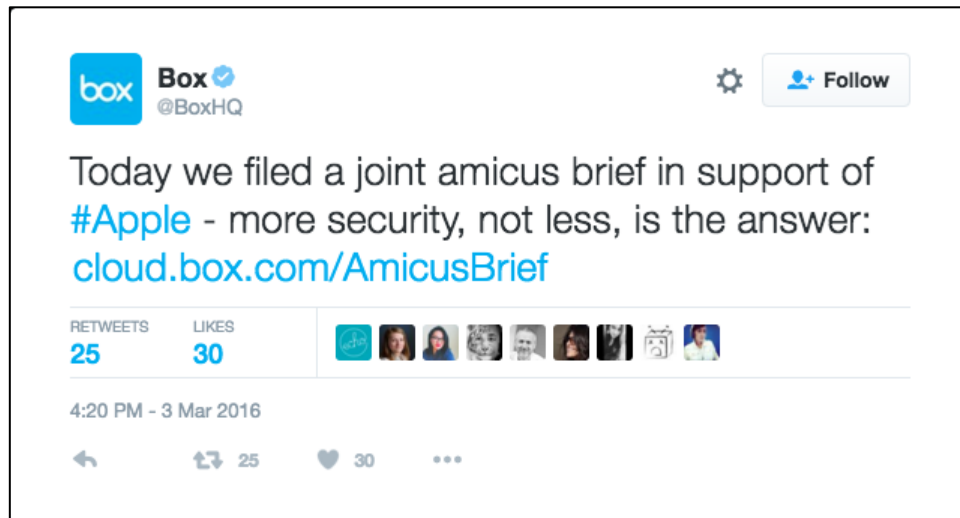
Response by Silicon Valley

Much like the rest of the country, technology companies were divided on the issue. Technology giants Amazon, Box, Cisco Systems, Evernote, Nest, Pinterest, Snapchat, Whatsapp, Yahoo, Mozilla, Dropbox, Facebook, Google and Microsoft backed Apple, submitting amicus briefs supporting Apple's decision.

On the other end of the issue, tech companies AirBnB, Atlassian PTY, Ltd., Automattic Inc., CloudFlare Inc., Ebay Inc., GitHub Inc., Kickstarter, PBC, LinkedIn Corporation, MapBox Inc., A Medium Corporation, Meetup Inc., Squarespace Inc., Twilio Inc., Twitter Inc., and Wickr Inc. sided with the government, submitting amicus briefs opposing Apple's decision (Roth, 2016).



Some companies also wrote blog posts and took to social media to express opinions on the controversial topic. For example, Box tweeted about its joint amicus brief.



(Source: Box, 2016)

Although these companies publicly opposed Apple’s decision, the briefs voiced the idea that the All Writs Act, under which the government had requested information from Apple, was unbound by legal limits (Deluca, 2016). Ultimately, these opposing companies believe that Apple should have accepted the FBI’s request, while still acknowledging that the government could have used a better strategy to request this information.

Business Performance: Will One Bad Apple Spoil the Whole Bunch?

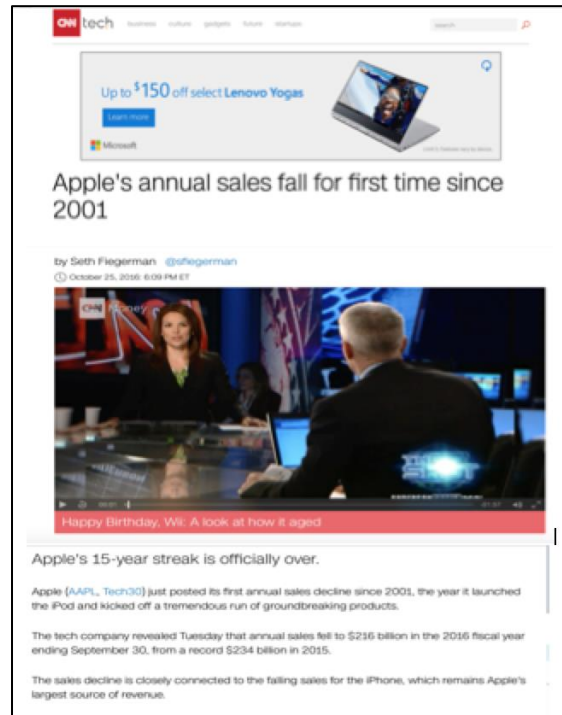
Financial Impact

Prior to the San Bernardino shooting, Apple’s stock had been sufficiently lower than previous years (Source: Thielman, Neate, Hern, 2016). 2016 was the first year that Apple had seen a sufficient dip in its stock in years. While this case affected Apple and its customers, many other factors came into play during 2016 that affected Apple’s stock price.

According to Apple’s second quarter 2016 financial report, quarterly revenue was \$50.6 billion, which was down from the prior year’s revenue of \$58 billion (Source: Apple Reports Second Quarter Earnings, 2016). Apple briefed investors prior to releasing its quarterly report that revenue and sales would be down. iPhone sales were down from the previous year and



Apple attributed this to no new iPhone releases in 2015 and customers purchasing their phones at that time rather than in 2016. “The total tally for the device was \$32.9 billion from 51.2 million phones sold; the previous year Apple brought in \$40.3 billion from 61.2 million phones” (Source: Thielman, Neate, Hern, 2016). Apple did not make as much money on the iPhone in 2016, resulting in a decline in revenue.



(Source: Fiegerman, 2016)

While the sales of the iPhone declined in 2016, there is no clear evidence to indicate that it was directly correlated to the ongoing FBI case. Before the San Bernardino shooting, Apple had been struggling to generate revenue growth in the face of maturing product lines, such as the iPhone.

When the case first began on February 16, 2016 and Tim Cook released his statement online about why Apple would not help, Apple's stock closed the day at \$96.64 per share. When the FBI and Apple met on March 1, 2016, to discuss the case in front of the House Judiciary Committee, Apple shares closed at \$100.53 per share. This was an increase from February 16th when the case began. On March 29, 2016, the case officially closed after the FBI was able to



unlock the phone the day before. On this day, Apple's stock closed at \$107.68 per share making it its highest close since the case began (Source: Apple Reports Second Quarter Earnings, 2016).

Throughout the case, Apple's stock continued to rise, further showing that this issue cannot directly correlate to the lower than normal stock prices seen in early 2016. This dip could be correlated to a mix of different factors, such as a new iPhone release the year prior, international sales lower than normal, etc. With many factors impacting the company's stock price, we cannot attribute causation to just one. After the case, Apple shares continued to rise (New York Times, 2016).



(Source: Yahoo Finance, 2016)

Reputation Impact

Although the iPhone was ultimately unlocked by an unknown third-party, the fact that Apple stuck to its core value of privacy in all of its responses throughout the 43 days strengthens Apple's reputation as a defender of privacy, and its claim that strong encryption isn't a security disaster (Grossman, 2016).

Over the past couple of decades, Apple has become one of the most admired and valuable companies in the world. Even though much of the public was split over Apple's decision of whether Apple should comply with the FBI's orders to unlock the iPhone or not, Apple has long ranked among the most reputable companies worldwide (Harris Poll Reputation



Quotient, 2016). Reputation rankings for 2017 (post this incident) seem likely to continue this trend.

Looking Ahead: Apple-y Ever After

As we move further into the age of big data, customer data privacy and security will be a challenge for all companies. Cybersecurity, hacks, breaches and requests by government entities is the new reality that all companies, and, by extension all Chief Communications Officers and Corporate Communication Departments, must be prepared to address and expertly navigate.

When pushed, Apple reverted to its core principal of privacy to create a strong, clear message on where it stands in this broader discussion. On June 13, 2016, Apple reaffirmed its commitment to encryption by announcing it was applying “differential privacy” research to keep users’ information private, a move that bolster’s the company’s standing as a leader in digital privacy. Executives at Apple’s annual developer conference in San Francisco also emphasized the company’s commitment to using encryption by default to protect customer’s data. Furthermore, privacy researcher Aaron Roth said the move reaffirmed Apple’s status as the “clear privacy leader among technology companies today” (Drange, 2016).



References: Isn't There an App for That?

Apple Inc. (n.d.). *Apple Values*. Retrieved from: <https://www.apple.com>

Apple Inc. (2016, May). iOS Security. Retrieved from: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Apple Inc. (n.d.). *Privacy*. Retrieved from: <http://www.apple.com/privacy/government-information-requests/>

Apple Inc. (2016) *Supplier Responsibility 2016 Progress Report*. Retrieved from http://images.apple.com/supplier-responsibility/pdf/Apple_SR_2016_Progress_Report.pdf

Apple Reports Second Quarter Results. (2016, April 26). Retrieved from <http://www.apple.com/pr/library/2016/04/26Apple-Reports-Second-Quarter-Results.html>

Apple vs. FBI: A Timeline of the Legal Battle. (2016, March 28). Retrieved from https://www.graphiq.com/vlp/DW36cJUvtj?utm_source=viz&utm_medium=viz.referral&utm_campaign=viz.ref&utm_viz_id=DW36cJUvtj&utm_pubreferrer=www.foxnews.com/tech/2016/03/29/fbi-breaks-into-san-bernardino-gunmans-iphone-without-apples-help-ending-court-case.html&vlp_ver=2#0-Apple-vs-FBI-a-Timeline-of-the-Legal-Battle

Arthur W. Page Society (2012). *Building belief: A new model for activating corporate culture & authentic advocacy*. Retrieved from: <http://www.awpagesociety.com/wpcontent/uploads/2012/03/Building-BeliefNew-Model-for-Corp-Comms-2012.pdf>

Bajarin, T. (2012, May 7). 6 Reasons Why Apple Is Successful. Retrieved January 09, 2017, from <http://techland.time.com/2012/05/07/six-reasons-why-apple-is-successful/>

Bedford, K. (2016, February 24). *Demonstrators rally outside Apple store in Boston* [Photograph found in Boston, MA]. In *Boston Globe*. Retrieved November 20, 2016, from <https://www.bostonglobe.com/metro/2016/02/23/demonstrators-rally-outside-apple-store-boston/fyy2bsnMjxuyszSShr9xaP/story.html> (Originally photographed 2016, February 24)

Benner, K., & Perloth, N. (2016, February 18). How Tim Cook, in iPhone Battle, Became a Bulwark for Digital Privacy. Retrieved November 20, 2016, from <http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html>



Bolluyt, J. (2015, June 20). Apple: 5 Ways It's Gone From Industry Leader to Follower. Retrieved November 20, 2016, from <http://www.cheatsheet.com/technology/apple/apple-5-ways-its-gone-from-industry-leader-to-follower.html/?a=viewall>

Chen, L. (2015, May 11). The World's Largest Tech Companies: Apple Beats Samsung, Microsoft, Google. Retrieved October 17, 2016, from <http://www.forbes.com/sites/liyanchen/2015/05/11/the-worlds-largest-tech-companies-apple-beats-samsung-microsoft-google/#77efae0c415a>

Coldewey, D. (2016, April 15). Apple tells NY judge FBI has 'utterly failed' to prove it needs help unlocking iPhones. Retrieved November 06, 2016, from <https://techcrunch.com/2016/04/15/apple-tells-ny-judge-fbi-has-utterly-failed-to-prove-it-needs-help-unlocking-iphones/>

Cook, T. (2016, February 16). A Message to Our Customers [Letter written February 16, 2016 to Apple Customers]. In *Apple*. Retrieved November 6, 2016, from <http://www.apple.com/customer-letter/>

Cook, T. (2016, February 24). Exclusive: Apple CEO Tim Cook Sits Down With David Muir (Extended Interview) [Interview by D. Muir]. In *ABC News*. Retrieved November 6, 2016, from <http://abcnews.go.com/WNT/video/exclusive-apple-ceo-tim-cook-sits-david-muir-37174976>

Cook, T. (2016, March 17). Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook [Interview by N. Gibbs & L. Grossman]. In *TIME*. Retrieved November 6, 2016, from <http://time.com/4261796/tim-cook-transcript/>

Crovitz, L. G. (2016, February 19). The FBI vs. Apple - WSJ - <http://www.wsj.com/articles/the-fbi-vs-apple-1455840721>. Retrieved November 06, 2016, from <http://grabpage.info/t/www.wsj.com/articles/the-fbi-vs-apple-1455840721>

Customer Letter - FAQ - Apple. (2016, February 16). Retrieved November 06, 2016, from <http://www.apple.com/customer-letter/answers/>

Deluca, M. (2016, March 03). Tech vs. the Feds: Apple Allies Rally in Flurry of New Court Filings. Retrieved November 06, 2016, from <http://www.nbcnews.com/tech/tech-news/apple-allies-expected-form-ranks-flurry-court-filings-n530987>

Dietrich, G. (2016, March 10). Privacy, Security, Transparency, and Crisis Management. Retrieved November 20, 2016, from <http://explore.zignallabs.com/h/i/222559635-privacy-security-transparency-and-crisis-management/239301>

Dillet, R. (2016, March 21). Apple's Tim Cook on iPhone unlocking case: 'We will not shrink from this responsibility' Retrieved November 06, 2016, from <https://techcrunch.com/2016/03/21/apples-tim-cook-on-iphone-unlocking-case-we-will-not-shrink-from-this-responsibility/>



Encryption: Last Week Tonight with John Oliver [Television series episode]. (2016, March 13). In *Last Week Tonight with John Oliver*. New York City, NY: HBO.

Facebook and Industry Peers Support Apple in Amicus Brief | Facebook Newsroom. (2016, March 3). Retrieved November 20, 2016, from <http://newsroom.fb.com/news/h/facebook-and-industry-peers-support-apple-in-amicus-brief/>

Drange, M. (2016, June 13). Apple Reaffirms Commitment To Encryption. Retrieved November 21, 2016, from <http://www.forbes.com/sites/mattdrange/2016/06/13/apple-to-strengthen-privacy/#b8292b36b075>

Fiegerman, S. (2016, October 25). Apple's annual sales fall for first time since 2001 - Oct. 25, 2016 - <http://money.cnn.com/2016/10/25/technology/apple-earnings-decline/index.html>. Retrieved November 20, 2016, from <http://grabpage.info/t/money.cnn.com/2016/10/25/technology/apple-earnings-decline/index.html>

Finkle, J. (2016, February 24). Solid support for Apple in iPhone encryption fight: Poll. Retrieved November 6, 2016, from Solid support for Apple in iPhone encryption fight: poll

Goldman, D. (2016, February 16). Tim Cook says the FBI wants Apple to 'hack' your iPhone. Retrieved November 20, 2016, from <http://money.cnn.com/2016/02/17/technology/fbi-apple-hack-iphone/index.html>

Grossman, L. (2016, March 28). Inside Apple CEO Tim Cook's Fight With the FBI. *TIME*, 187(11). Retrieved November 6, 2016, from <http://time.com/4262480/tim-cook-apple-fbi-2/>

Harris, Shane. "Apple Unlocked iPhones for the Feds 70 Times Before." *The Daily Beast*. The Daily Beast Company, 17 Feb. 2016. Web. 20 Nov. 2016.

Harris Poll. (2016, February) *The Harris Poll Releases Annual Reputation Rankings for The 100 Most Visible Companies in the U.S.* Retrieved from: <http://www.theharrispoll.com/business/Reputation-Rankings-Most-Visible-Companies.html>

Hughes, G. (2016, February 22). Social Media's Response to Apple vs. The FBI. Retrieved November 20, 2016, from <http://www.convinceandconvert.com/realtime-today/social-medias-response-to-apple-vs-the-fbi/>

Isaac, M. (2016, February 17). Explaining Apple's Fight With the F.B.I. - The New York Times. Retrieved November 6, 2016, from <http://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html>



Kharpal, A. (2016, March 29). Apple vs FBI: All you need to know. Retrieved November 06, 2016, from <http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html>

Kokalitcheva, K. (2016, March 22). Apple's Fight With the FBI Isn't Keeping People From Wanting an iPhone. Retrieved November 20, 2016, from <http://fortune.com/2016/03/22/poll-apple-fbi-iphone/>

Kondoker, S. (n.d.). [Letter to Honorable Judge Sheri Pym]. In *Apple*. Retrieved November 20, 2016, from http://images.apple.com/pr/pdf/Letter_from_Salihin_Kondoker.pdf

La Monica, P. (2016, February 24). Apple's stock has worms but FBI isn't one of them. Retrieved November 20, 2016, from <http://money.cnn.com/2016/02/24/investing/apple-stock-fbi-iphone/index.htm>

Lee, D. (2016, February 18). Apple v the FBI - a plain English guide. Retrieved November 6, 2016, from <http://www.bbc.com/news/technology-35601035>

Madigan, M. (2016, March 22). Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google ... Retrieved November 6, 2016, from http://images.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Google_Microsoft_Mozilla_Nest_Pinterest_Slack_Snapchat_WhatsApp_and_Yahoo.pdf

Maniam, S. (2016, February 22). More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone. Retrieved November 20, 2016, from <http://www.peoplepress.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/>

Mozingo, J. (2015, December 09). San Bernardino Shooting Update. Retrieved November 06, 2016, from <http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html>

Newseum: San Bernardino Shooting. (2015, December 3). Retrieved from http://www.newseum.org/todaysfrontpages/?tfp_display=archive-summary

O'Neill, P. H. (2016, February 26). Americans trust Apple but remain divided on unlocking iPhone for FBI, new poll finds. Retrieved November 06, 2016, from <http://www.dailydot.com/layer8/apple-tim-cook-fbi-iphone-unlock-encryption-morning-consult-poll/>

Ragas, M. W., & Culp, R. (2014). Business essentials for strategic communicators: Creating shared value for the organization and its stakeholders. New York: Palgrave Macmillan.



Thielman, S., Neate, R., & Hern, A. (2016). Decline in iPhone sales leads to first revenue decline in 13 years for Apple. Retrieved November 20, 2016, from <https://www.theguardian.com/technology/2016/apr/26/apple-iphone-first-revenue-decline-13-years>

Timberg, C. (2014, November 04). Apple users raise privacy concerns after hard-drive files uploaded to servers. Retrieved November 06, 2016, from <https://www.theguardian.com/technology/2014/nov/04/apple-data-privacy-icloud>

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

Welch, C. (2016, February 24). Watch Tim Cook's full 30-minute interview on Apple's fight with the FBI. Retrieved November 06, 2016, from <http://www.theverge.com/2016/2/24/11110802/apple-tim-cook-full-interview-fbi-iphone-encryption>

Zetter, K. (2016, February 19). DOJ Files Motion to Force Apple to Hack iPhone in San Bernardino Case. Retrieved November 06, 2016, from