Impenetrable: Should Apple backdoor the iPhone?

Ben Wolfson

Computing Ethics

Laura Levy

July 28th, 2020

Abstract

Apple's refusal to comply with 2016 FBI-mandated court orders to decrypt a terrorist's phone sparked a seemingly inconsolable clash between principles of national security and individual rights. It has also led to debate over what a tech giant's corporate social responsibility is in the modern world, where data has become increasingly commodified. The FBI argues that Apple is acting against the nation's best interests—and illegally. Apple's position is that their obligation to customers' privacy is stronger than the law, arguing that the move would not only create undue burden, but also would introduce a deadly example for future cases and foreign governments. They also argue against compelled speech since code is recognized by the courts as a form of personal expression. Some critics say that Apple's stance is motivated by marketing, and that the company is being unnecessarily difficult. Others push for the protections of the first amendment in these types of conditions, citing the previous surveillance by the NSA as reasoning for why the government cannot be trusted with the potential power that would come with such a legal precedent. This paper will examine the evolution of encryption and communication standards, discuss the arguments on both sides of Apple v. FBI, and finally explore the hypothesis of extended cognition as it relates to our classifications of smartphone usage—both legal and ideological—ultimately supporting the ethical basis for maintaining device privacy in spite of the legal validity of the FBI's claim.

Introduction

The struggle of government to get its hands on private civilian communications has been a persistent issue over the past several decades. In 1987, Congress passed the Computer Security Act, intending to limit the NSA's involvement in the development of civilian communication standards (Congressional Research Service, 1988). However, in 1993, the NSA released the Clipper Chip, a cryptographic device designed to encrypt private communications with a built-in back door for government access. The intention behind this chip was for mass implementation by telecommunications companies, thereby giving the government direct access to cellphone communication channels (Froomkin, 1995). This move was met with great controversy, and in 1994 researchers determined that the chip was extremely vulnerable to being hacked (Froomkin, 1995). Finally, later in 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to allow law enforcement to wiretap digital communication networks for use in criminal investigations (Congressional Research Service, 1994). In 2006, 12 years later, CALEA was amended to include Voice over Internet Protocol (VoIP) services like Skype. After this point, the bureaucratic crawl of legislation could not keep pace with the constantly changing internet landscape, and significant divergence between the two began to emerge.

The events of September 11th, 2001 precipitated a cascade of government referendums as part of the War on Terror. Mass civilian surveillance became legal under the premise of strengthening national security, but set in motion a series of events that would eventually fracture the public trust in government. Most notable among these changes was the Patriot Act, enacted 45 days

after 9/11, which allowed the government to access private phone and email communications, bank and credit reporting records, and track web activity of regular citizens (Cornell Law School, n.d.). Additionally, secret intelligence activities were initiated under the President's Surveillance Program (PSP) (Electronic Frontier Foundation, 2014). The public first became aware of these secret actions as a result of the Snowden leaks in June 2013, when the NSA was exposed to have been secretly collecting the internet data of innocent citizens through PRISM, a remnant of PSP, which involved the NSA collecting data directly from the databases of tech giants like Google, for example (Kelley, 2013).

The manifestation of the quickly increasing public concern in the private sphere was almost immediate. Customers demanded more privacy—and even some foreign countries started engaging in preliminary discussions to establish their own secure networks (Taylor, 2013). American tech companies heeded their customers' calls. Just over a year later, in September 2014, Apple stopped their policy of unlocking iPhones for use in criminal investigations. This decision coincided with the release of the iPhone 6 and iOS 8—when Apple started marketing their phones as the only fully secure ones in the market, backed by a virtually uncrackable, proprietary encryption (Apple, Inc., 2015). Apple had been iteratively improving their device security for years, releasing Touch ID only a year before in 2013—a major step towards increased protection—but this unprecedented leap forward seemed to have uncanny timing. Regardless, consumer expectations for privacy skyrocketed, and smartphone security took a huge step forward as a result.

In 2016, the topic of device privacy was yet again brought to the forefront of the public's attention, this time through the very publicized dispute between Apple and the FBI. The FBI asked Apple to implement a backdoor into future phones and to develop software to brute force their way into the iPhone of Syed Farook, a suspect of the 2015 San Bernardino shooting. Apple declined, the core of their reasoning being that such an action would eventually result in more harm than good for most citizens, and also criticized the FBI for attempting to use such a high-profile case to strong-arm their way into the secure Apple ecosystem (Etzioni, 2016). Tim Cook, Craig Federighi, and many other Silicon Valley executives voiced their concerns to the media of the importance of maintaining individual device integrity (Etzioni, 2016). The FBI argued that Apple was acting illegally in their choice under the All Writs Act, legislation which allows federal courts to compel third parties to act in certain ways when deemed necessary (28 U.S.C. § 1651). The dispute seemingly vanished overnight in March 2016 when the FBI dropped its case against Apple, having paid $900,000 to an anonymous third party to access the phone in question (Hosenball, 2016). However, the underlying tension between private technological security and national security remains, and the question still remains unanswered: to what extent can the government compel private corporations to act in what it deems to be the interest of public good?

Ethical Analysis: Apple v. FBI

During the San Bernardino shooting, the perpetrators attempted to smash all of their personal devices, presumably to erase any digital traces about potential future planned incidents or leads to other parties involved in the shooting (ABC News, 2015). The iPhone 5C left by Farook was

actually a work phone, but still could have contained some of this type of information (Young, 2016). By not unlocking the device, the FBI argues Apple was directly interfering with matters of national security.

Apple's rebuttal to this is quite simple: maintaining personal privacy is actually *mor*e in the interest of national security. Craig Federighi, who oversees the development of Apple's suite of operating systems as vice president of software engineering, was quoted as saying the following: "...the threat to our personal information is just the tip of the iceberg… Criminals and terrorists who want to infiltrate systems and disrupt sensitive networks may start their attacks through access to just one person's smartphone" (2016). Essentially, he argues that since phones are not self-contained objects, ensuring their individual security protects the vital systems to which they are connected, thereby resulting in a more encompassing mission for national security.

Essentially, we have an ideological battle between national security and personal privacy. The following section will analyze the ethical ramifications of the two perspectives through multiple ethical frameworks.

Act Utilitarianism

Act utilitarianism argues that the ethical action in a given scenario is the one that maximizes the net utility of that scenario's outcome, using some form of a cost-benefit analysis (Quinn, 2020). To analyze Apple's decision, we need to define 'bestness' in terms of some variable. Let us count the number of people who will be positively and negatively affected—the classical example, and one that most readily comes to mind in this case. If Apple complies with the FBI's request, they have a positive influence on the people who would otherwise be harmed by the

potential information that is on the FBI-supplied phones. We can reasonably assume that this would amount to no more than one hundred thousand people yearly. This value is deterministic for this analysis. However, the next component hinges on hypotheticals, so we can only calculate an expected value; one that varies as a result of probabilities. By introducing a backdoor, Apple is increasing the likelihood that a black hat hacker figures out how to break through their encryption. The probability of this event is greater than 0, but most certainly very small. This would most certainly undermine the security of the more than 718 million iPhone users globally (O'Dea, 2020). Additionally, it would arm the government with another tool for potentially spying on Americans, which adds another layer of negative net utility. There is overwhelmingly more downside to complying than not.

Kantianism

In contrast to the consequentialist nature of utilitarianism, Kant's deontological approach to ethics completely disregards consequences. He attempts to use logic in establishing morality, and under the first formulation of the Categorical Imperative, argues that people should only follow rules that can be universally applied without resulting in fallacy (Quinn, 2020). Kant would argue in favor of Apple's decision to not introduce a backdoor into their devices, since if every device has a backdoor, then the very notion of privacy itself would become undone, resulting in contradiction. The company is also concerned that the government would take advantage of the backdoor to improve their surveillance capabilities on innocent civilians. Kant would disagree with this. Under the second formulation of the Categorical Imperative, he argues that people are never to be treated as means to an end, and only as ends in themselves (Quinn, 2020). Certainly,

using a backdoor to acquire personal information is using people as a means to acquire their data, which goes against Kant's principles.

Literature and Arguments Review

While analyzing the broad ethicality of both sides of national security and personal privacy is useful, there are other important considerations that, when applied to ethical analysis would make the situation too complex to analyze in a reasonable amount of time. This section will examine the other legal and practical rebuttals offered by Apple and their analysis by other notable peer-reviewed literature: Etzioni's "Apple: Good Business, Poor Citizen?" and Nielsen's "Ethical and Legal First Amendment Implications of FBI v. Apple: A commentary on Etzioni's 'Apple: Good business, Poor Citizen?'".

All Writs Act

While the FBI's core argument is that having backdoor access to phones is in the public's best interest, even if this position can be ethically justified, the government's authority to compel a private corporation needs to first be lawfully established, since without it there is no basis for their argument. The All Writs Act allows federal courts to compel private entities and other third parties to perform certain actions—as described previously—however, these actions are not without limits (28 U.S.C. § 1651). Somewhat ironically, in *United States v. New York Telephone*, the Supreme Court amended the extent of the All Writs Act, stating that "unreasonable burdens may not be imposed" (*United States v. New York Telephone*, 1977).

In October 2015, the Brooklyn Attorney's office attempted to use court order under the All Writs Act to compel Apple to unlock a suspected drug dealer's phone. New York Magistrate Judge James Orenstein denied this request, stating that the justification provided by the government was insufficient (Orenstein, 2015). Shortly thereafter, Apple countered the initial request, claiming that such a request was technically impossible and subsequently "unreasonably burdensome", thereby negating the scope of the All Writs Act.

In the 2016 case, however, the courts were not on Apple's side. The FBI asked Apple to create a backdoor key to brute force into Farook's phone. This time, California Magistrate Judge Sheri Pym ordered Apple to offer the FBI "reasonable technical assistance" (Etzioni, 2016). Again, Apple argued that this was too burdensome. Etzioni disagrees, arguing that, by their own admission, Apple estimates that in order to do so would probably only require 6 employees working for only 2 weeks (Government's Reply Brief, 2016, p. 2).

According to crowdsourced data from LinkedIn's search function, the company has in excess of 21,000 US-based software engineers, many of whom are among the best and brightest talent in the industry. This supports the idea that having some of them come up with a novel solution to solve this issue does not seem particularly *unreasonable*—especially for a company that regularly maintains a cash reserve in excess of 200 billion dollars.

First Amendment

Perhaps the strongest legal argument that Apple has is protection under the First Amendment, which, of course, allows for freedom of speech. In the landmark case of *Bernstein v. Department of Justice*, the Ninth Circuit Court of Appeals ruled that software source code was speech, and therefore protected under the First Amendment (*Bernstein v. Department of Justice*, 1996) . Bernstein was a graduate student at the University of California at Berkeley when he discovered an encryption algorithm 'Snuffle' (Columbia University, 2019). Naturally, he sought to publish his findings along with source code of its implementation. However, the Arms Export Control Act and International Traffic in Arms Regulation first required him to submit this work to the government for approval and additionally apply for a specific license (Columbia University, 2019). When the courts ruled in favor of him, we assume their reasoning was to establish the precedent of having the freedom to share novel ideas in computing. However, it should be noted that, in the 90s, there was much confusion surrounding these kinds of topics, since technology was not nearly as widespread as it is today—for perspective, the Internet had only first become commercialized in 1995, one year prior to the case.

One of Nielsen's core arguments is that, historically, First Amendment protections have been voided in favor of national security. This concept—that free speech is not an absolute right when it comes to matters of national security—is most certainly in the best interests of the public. Both Etzioni and Nielsen cite a popular quote by Supreme Court Justice Holmes during the proceedings of *Schenck v. United States,* which involved political naysayers to US involvement in WWI and opposed the draft: "the most stringent protection of free speech would not protect a

man in falsely shouting ‘fire’ in a theater and causing panic” (*Schenck v. United States*, 1919). Nielsen also references the more recent 2010 Supreme Court decision in *Holder v. Humanitarian Law Project* in which the court decided that speech advocating for “material support” of terrorist organizations is unlawful (*Holder v. Humanitarian Law Project*, 2010). He then goes on to discuss First Amendment protections under social media communications, since the US Judiciary has historically given leeway to cases involving government intrusion of social media sites. Finally, he explores the possibility of Apple being classified as a social media company. However, this is somewhat trivial, since Apple does not claim to be one and does not offer such services in their product portfolio, with the potential exception of Apple Music.

A stronger deficiency against Apple’s claim for First Amendment protections is the notion that code always constitutes speech. Applying the Bernstein ruling to other cases should be done with caution, as it was for a very specific set of circumstances. The *Bernstein v. DOJ* case conclusion states that “because the prepublication licensing regime challenged by Bernstein applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, we hold that it constitutes an impermissible prior restraint on speech”. This type of language suggests that the ruling extends to methods of information dissemination, and not necessarily source code as it applies to non-distributional instances. A more palatable situation to illustrate the application of this law: a software engineer is compelled by his employer to code a specific function that he does not want to program. Imagine the engineer sues his employer for compelled speech—such a case would be disregarded almost immediately in the courtroom. The idea that code contains inherent expressional value is a fallacy, since

sometimes code is merely functional, whereas expression generally constitutes an idea or a particular sentiment. The ruling of Bernstein applied to "scientific expression", i.e. *scientific idea*—and dismantled the systematic barriers to *publishing* those *ideas*. The Apple case only concerns the implementation of functional code—not the publishing of expressive code. Here we have the key distinctions between the two cases: type of code and the nature of its usage. Both Etzioni and Nielsen fail to consider this in their criticisms.

International Precedent

Although we generally consider Apple to be an American company, more than half (55%) of their revenues are actually generated outside of the United States (Apple, Inc., 2019). Apple argues that implementing a backdoor in their phones for the FBI will set a precedent for the foreign governments who want them to do the same thing—forcing them to potentially comply with authoritarian-leaning regimes, like China. Outside of the US, China is the greatest consumer of Apple products, generating slightly under 25% of their total annual sales (Apple, Inc., 2019). This gives them an enormous amount of economic leverage over the company. Interestingly, China also has twice as many iPhone users as the United States (O'Dea, 2020).

Etzioni believes that this argument is void. He points to the fact that the lack of international legalities has never stopped the Chinese government hesitant to act out previously, and that "precedence is a legalistic, Anglo Saxon notion" (2016). He further argues that refraining from establishing important legislation in fear of the ramifications of other nations is extremely dangerous. He points to the counter example: "[Should the US stop censoring] child pornography

just because China may point to this American limit on the right to free speech and use it as an excuse to further limit the free speech rights of their citizens?" (Etzioni, 2016). Finally, he points to the fact that Apple has already complied with Chinese government in the past through censorship of the CNN News app (2016). Apple's hypocrisy in this area severely undermines their claim, especially considering the numerous official accounts of providing chinese client account information, even after the release of iOS 8 in 2014 (Privacy and Security in the Digital Age, 2016).

Discussion

Cell phones have evolved rapidly since the days of the Motorola DynaTAC. Before the emergence of smartphones, the actual process of texting was extremely cumbersome, with most phones forcing users to use a 9-key keypad to type out messages. The awkwardness of this mechanism made calling the de facto standard for communication, as it was significantly difficult to get across complex or even multi-sentence ideas through finicky finger presses. Although BlackBerry was the first phone manufacturer to come out with a full feature keyboard, Apple was the first company to do it right. The iPhone, with its multi-touch capability, took the smartphone world by storm and made it possible for a new modality of communication to flourish: texting.

Now, over a decade later, smartphones have become the hearth of our digital homes, storing the information most sensitive to us—from credit cards and Internet search history to text exchanges with loved ones. Naturally, the courts have struggled in keeping pace with these developments.

In particular, the topic of warrantless cell phone searches incident to arrest commanded great controversy over the course of the mid 2000s to early 2010s, with states having mixed policies on its legality during this time. In the 2014 landmark case of *Riley v. California*, the Supreme Court ruled that "police generally may not [subject to exigent circumstances] without a warrant, search digital information on a cell phone seized from an individual who has been arrested" and further establishing that "the fact that technology now allows an individual to carry such [personal] information in his hand does not make their information worthy of protection for which the Founders fought" (*Riley v. California*, 2014).

The field of philosophy, on the other hand, has not been stifled by the rapid technological advancements. Some philosophers are exploring the concept of reclassification of smartphones under the hypothesis of extended cognition (HEC), which argues that the mind extends beyond the body, spilling into objects in the environment around us, in "intimate feedback with our thought processes" (Carter & Palermos, 2016). Essentially, under this hypothesis, external objects can be considered as part of our cognitive model.

In Carter & Palermos' "Is Having Your Computer Compromised a Personal Assault? The Ethics of Extended Cognition", they pose the following question: "What makes the difference between whether I've intended to use force against your person as opposed to merely your property?". Assault has always lawfully been considered a separate violation to property damage. The UK has established the following precedent: "The body of the victim includes all parts of his body, including his organs, his nervous system and his brain. Bodily injury therefore may include

injury to any of those parts of his body responsible for his mental and other faculties (Carter & Palermos, 2016). The authors point to the fact that, in this definition, there are actually two subtly distinctive ideas: while the first clause takes a reductive interpretation of the body, the second takes a functionalist interpretation—allowing us to detach from traditionalist notion of establishing an individual's faculties as a result of "organismic parts" (2016).

At last we arrive at Carter & Palermos' justification for Extended Assault, which they arrive at through the following syllogism:

(1) Intentional harm to a part of a person responsible for the person's mental and other faculties constitutes personal assault. (Definition)
(2) Our mental faculties can be partly constituted by external artifacts so long as these artifacts have been appropriately integrated into our overall cognitive system. (From HEC)
(3) Therefore, having our integrated epistemic artifacts intentionally compromised plausibly qualifies as a case of personal assault. (From 1 and 2) (p. 8)

In *Ladner v. United States*, the US courts established that apprehension of harm alone is sufficient in constituting assault (*Ladner v. United States*, 1958). Incorporating this with HEC, would the ever-present threat of having one's phone being able to be accessed by the government create 'apprehension of harm'? While the concept that compromises to our phones by a third party constitute personal assault is most certainly unorthodox, it has interesting applications to

the issue of *Apple v. FBI*, for it brings the following question into focus: what is the likelihood of the courts to change their interpretation of phones yet again? While the US Judiciary may never integrate HEC with the law, as we have seen with the recent case of *Riley v. California*, it has been shown to consider more progressive interpretations of the technology. Moreover, if the nature of our relationship with phones continues to change, what kind of effect would the precedent of introducing backdoors now have in the future? We can reasonably assume that, given more advancements, smartphones have the very likely potential to become more intertwined with our cognitive models, increasing our personal exposure and the potential magnitude of extended assault under HEC. Would having a backdoor to our phones prove too much temptation for the US government to handle? It certainly has not treaded lightly in the past.

Conclusion

The case for privacy is clear, in spite of the flimsy legal basis for Apple's claims. The ethical basis for maintaining personal privacy over an alternative reality is validated from a consequentialist and deontological perspective. War is the mother of invention—and modern cryptography. The parity between black hats, law enforcement, and phone manufacturers will always exist. Introducing a backdoor into the iPhone security simply creates the potential for too much downside to account for minor improvements in national security. Surely there are other methods that the FBI can use to unlock these phones through fingerprint verification or making a 3D mold of a suspect's head to use the iris scanner. Even still, maybe there does exist a way for Apple to access data on a case-by-case basis without compromising the security of other users. Devoting a team of internal engineers to solving the problem could prove to be a worthy cause

for the company, as they may find new security encryption breakthroughs along the way. The rapidly changing pace of technology almost guarantees the further integration of smartphones into our lives. Maybe instead of dismantling the encryption that protects our personal information, we should focus on strengthening it, thereby improving national security. After all, a chain is only as strong as its weakest link.

References

ABC News. (2015, December 3). *San Bernardino Shooters Tried to Destroy Phones, Hard Drives, Sources Say.* https://abcnews.go.com/US/san-bernardino-shooters-destroy-phones-hard-drives-sources/story?id=35570286

Apple, Inc. (2015). iOS Security - iOS 8.3 or later. https://www.apple.com/ph/privacy/docs/iOS_Security_Guide.pdf

Apple, Inc. (2019). *Form 10-K.* Retrieved from http://d18rn0p25nwr6d.cloudfront.net/CIK-0000320193/1a919118-a594-44f3-92f0-4ecca47b1a7d.pdf

Bernstein v. United States Department of Justice, No. 97-16686 (9th Cir. Apr. 15, 1996). Retrieved from https://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.html

Carter, J.A. & Palermos, S.O. (2016). Is having your computer compromised a personal assault? The ethics of extended cognition. *Journal of the American Philosophical Association, 2*(4), 542-560. https://doi.org/10.1017/apa.2016.28

Columbia University. (2019, November 20). *Bernstein v. Department of Justice.* Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/cases/bernstein-v-department-of-justice/

Congressional Research Service. (1988, January 8). Summary: H.R.145 - Computer Security Act of 1987. https://www.congress.gov/bill/100th-congress/house-bill/145

Congressional Research Service. (1994, October 25). Summary: H.R.4922 - Communications Assistance for Law Enforcement Act. https://www.congress.gov/bill/103rd-congress/house-bill/4922

Cornell Law School. (n.d.) *Patriot Act.* Legal Information Institute. Retrieved from https://www.law.cornell.edu/wex/patriot_act

Electronic Frontier Foundation. (2014, August 10). *How the NSA's Domestic Spying Program Works.* https://www.eff.org/nsa-spying/how-it-works

Froomkin, A. M. (1995). The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. *University of Pennsylvania Law Review, 143*(3), 709. https://doi.org/10.2307/23312529

Etzioni, A. (2016). Apple: Good Business, Poor Citizen? *Journal of Business Ethics, 151*(1), 1-11. https://doi.org/10.1007/s10551-016-3233-4

Federighi, C. (2016, March 6). *Apple VP: The FBI wants to roll back safeguards that keep us a step ahead of criminals.* Washington Post. https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fopinions%2fapple-vp-the-fbi-wants-to-roll-back-safeguards-that-keep-us-a-step-ahead-of-criminals%2f2016%2f03%2f06%2fcceb0622-e3d1-11e5-a6f3-21ccdbc5f74e_story.html

Government's Reply in Support of Motion to Compel and Opposition to Apple Inc's Motion to Vacate Order. *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 #5KGD203,* ED No. CM 16-10 (SP). Retrieved from https://www.justice.gov/usao-cdca/file/832166/download

Holder v. Humanitarian Law Project, 561 U.S. 1 (2010). Retrieved from https://www.law.cornell.edu/supremecourt/text/08-1498

Hosenball, M. (2016, May 4). *FBI paid under $1 million to unlock San Bernardino iPhone: sources.* Reuters. https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032

Orenstein, J. (2015, Oct. 9) *In Re Order Requiring Apple, Inc.*, 15-MC-1902(JO) Retrieved from https://epic.org/amicus/crypto/apple/Orenstein-Order-Apple-iPhone-02292016.pdf

Kelley, M. (2013, June 15). *The Best Explanation Yet of How the NSA's PRISM Surveillance Program Works.* Business Insider. https://www.businessinsider.com/how-prism-surveillance-works-2013-6?international=true&r=US&IR=T

Ladner v. United States, 358 U.S 169 (1958). Retrieved from https://www.law.cornell.edu/supremecourt/text/358/169

Nielsen, R.P. (2017). "Ethical and Legal First Amendment Implications of FBI v. Apple: A commentary on Etzioni's 'Apple: Good Business, Poor Citizen?'". *Journal of Business Ethics*, *151*(1), 17-28. https://doi.org/10.1007/s10551-017-3437-2

O'Dea, S. (2020, February 26). *iPhones in use worldwide.* Statista. https://www.statista.com/statistics/755625/iphones-in-use-in-us-china-and-rest-of-the-world/

Privacy and Security in a Digital Age. (2016). Council on Foreign Relations. Retrieved from https://www.cfr.org/event/privacy-and-security-digital-age

Quinn, M. J. (2020). *Ethics for the Information Age* (8th ed.). Pearson.

Raso, F. (2016, March 29). *Federal Court Orders Apple to Unlock iPhone. Apple Refuses.* Harvard Journal of Law & Technology. http://jolt.law.harvard.edu/digest/federal-court-orders-apple-to-unlock-iphone-apple-refuses

Riley v. California, 573 U.S. 373 (2014). Retrieved from https://www.law.cornell.edu/supremecourt/text/13-132

Schenck v. United States, 249 U.S. 47 (1919). Retrieved from https://www.law.cornell.edu/supremecourt/text/249/47

Taylor, M. (2013, November 1). *NSA surveillance may cause breakup of internet, warn experts.* The Guardian. https://theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden

United States v. New York Telephone, 434 U.S. 159 (1977). Retrieved from https://www.law.cornell.edu/supremecourt/text/434/159

Young, L. J. (2016, March 19). *San Bernardino iPhone 5C: Everything We Know.* Inverse. https://www.inverse.com/article/13053-san-bernardino-iphone-5c-everything-we-know