SMARTPHONE ENCRYPTION: APPLE VS THE FBI

Michael Molenda

IST 594B mpm325@psu.edu

Table of Contents

Abstract

The issue of smartphone encryption is complex. Encryption has always been a part of smartphone operating systems. However, the encryption schemes have become much better and thus the phones have become harder to break into by law enforcement. As with all complex issues, there are two sides to this issue: law enforcement and consumers. The central research question that this paper covers is whether or not consumers need smartphone encryption.

In some cases, consumers are unaware that their phones are encrypted and what that even means. In other cases, the consumers are high-level technology experts and know exactly what it means and what the implications are if this encryption is broken. I asked these questions to both types of consumers to learn more about their attitudes toward smartphone encryption including do they need it, attitudes towards encryption and law enforcement, and personal privacy.

I distributed a survey to my friends, friends-of-friends, and classmates. I received a plethora of information back from the respondents to my survey. I have assessed the responses and analyzed the results and have presented their results in this paper. In short, the major finding of my research is that consumers believe that their data should be protected from so-called “bad guys” (e.g. criminals). At the same time, the respondents suggested their data should be accessible to law enforcement officials, even if it means that Apple, Google, and Microsoft have to create tools or special versions of their operating systems specifically for law enforcement. They agreed that these tools could also fall into the hands of “bad guys”.

However, in order to understand this topic, we must understand some of the history behind it.

Introduction

In today's highly electronic world, people are constantly using their phones for communication of all types including: phone, text, social networking, and chat. In 2014, Apple was the first smartphone maker to embrace full device encryption in iOS 8. There had been prior encryption used in iOS, however, not to the extent that was used in iOS 8 (and future iOS versions). Poulsen (2014) puts it bluntly, "For the first time, all the important data on your phone—photos, messages, contacts, reminders, call history—are encrypted by default." This means that everything that you do on your phone cannot be accessed by any other means than unlocking the phone with the owner's PIN or passcode. There are no hidden backdoors or ways that hackers or law enforcement can obtain consumers' private data. Poulsen (2014) also gives us a glimpse into what the law enforcement community thinks about this encryption issue: "They warn that without the ability to crack the security on seized smartphones, police will be hamstrung in critical investigations. John Escalante, chief of detectives for Chicago's police department, predicts the iPhone will become "the phone of choice for the pedophile."

The reason that law enforcement is against this type of encryption technology and the way that Apple has implemented it can be summed up by this one quote, "Apple itself can't access your files, which means, unlike in the past, the company can't help law enforcement officials access your files, even if presented with a valid search warrant." (Poulsen, 2014) On the one hand, "The technology firms, while pledging to honor search warrants in other situations, say they simply won't possess the ability to unlock the smartphones. Only the owner of the phone, who set up the encryption, will be able to do that." ("Compromise needed", 2014, para 3) However, this is not purely about mass surveillance. What law enforcement is asking for is a

way to access the data on phones where the court has issued a search warrant. In these cases, this is not intrusive but a very reasonable request.

President Obama made a keynote address at the South by Southwest Conference [SXSW] in March 2016. At the end of the keynote, he took questions. The question of encryption naturally came up and Obama was political with his answer. While, he does side with the law enforcement agencies, he also believes in strong encryption. His answer tried to satisfy both sides of the argument. However, this seems to be contradictory in terms. However, the President did give this as part of his answer about balancing national security concerns and encryption: “As to how to balance these things Obama said we'll have to figure out "how do we have encryption as strong as possible, the key as secure as possible and accessible by the smallest pool of people possible, for a subset of issues that we agree is important."” (as cited in Ingraham, 2016)

With all of the issues surrounding national security, do consumers need full-phone encryption? The U.S. Congress and the FBI certainly do not think they do. Those consumers who carry an iPhone (particularly the iPhone 5s and later) have some very sophisticated encryption methods in their phones.

However, in most instances, consumer may be aware their phones are fully encrypted, nor do they know if they need it or not. Although, there are some polls that have confirmed that an overwhelming majority of American voters support some type of encryption. According to a survey conducted in April 2016, “93 percent of respondents said it’s important that the photos, health data or financial information they store on their phones and apps, or share online, stay secure and private.” (Wyckoff 2016)

Another interesting finding in this particular survey, 54 percent of those surveyed, believe that their data is safer with Apple, Google, and Facebook than with the FBI. Although, this is not directly related to my research, it is very thought-provoking that American voters do not appear to trust their own government with their data.

Literature Review

I submit that journalists and bloggers have written about the phone encryption. Most of the authors seem to be focused the reasons they think that consumers need phone encryption, because it is a privacy issue. On our phones, it means that our messages and email should be private (in this case, via encryption). Interestingly enough, for most, our desktops and laptops are not encrypted by default whereas our phones are encrypted by default. Why is that? It is simple: our phones are mobile and are easily stolen. The question really is 'Do consumers need full phone encryption?' Since there are multiple sides to this issue, I will take them one by one.

Governmental Attempts at Regulating Encryption

It is understandable why the law enforcement community would detest encryption would like a way around it (i.e. backdoor) because criminals use encryption for their benefit. However, what price do all consumers have to pay to assist the law enforcement community in their battle against cybercriminals?

in reaction to the Apple vs FBI court encryption-related battle, a couple of bills that have been introduced since the end of 2015. (Buttar, 2016) During the 2015-2016 legislative session, a new bill was introduced into the New York Senate. New York State Senate Bill 8093 (June 8, 2015) proposed a law to ban the sales of phones in these states that do not come with "backdoors". Bill 8093 states, "Simply stated, passcode-protected devices render lawful court orders meaningless and encourage criminals to act with impunity." (Fitzgerald, 2016) However, as students of cybersecurity, we have learned throughout our studies in Information Assurance is any backdoor left open for law enforcement can be found and exploited by people who may use this for nefarious reasons. This is why privacy advocates oppose backdoors.

On April 7, 2016, Senator Burr (R-North Carolina) and Dianne Feinstein (D-California) introduced a new bill in the United States Senate, named “Compliance with Court Orders Act of 2016”. That bill would essentially stop the end-to-end encryption within the United States. (Greenberg, 2016) This encryption is used by Apple as part of its iMessage service as well as chat app, WhatsApp. Additionally, there are dozens of other apps on smartphones that reply on encryption. “This basically outlaws end-to-end encryption,” says Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology. “It’s effectively the most anti-crypto bill of all anti-crypto bills.” (Greenberg, 2016) This sums up the reaction of the bill in the technology community. While this bill does not call for backdoors specifically, the language of the bill suggests a backdoor. It states that all ‘communication’ firms should be able to unencrypt the data or give law enforcement the means to decrypt. This would essentially be a backdoor.

Some in the United States Congress do see this a something that would make Americans less safe, such as Oregon Senator Ron Wyden. Wyden has vowed to do everything in his power to prevent something like this. Others in Congress are not so sure. "If there is another attack in the United States," said Indiana's Coats "the American people will be saying, 'Did you do everything you possibly could to prevent this?' " (Wellna, 2016)

FBI (Law Enforcement)

Since the beginning of this case, the FBI has been hinting at a backdoor. It seems as if James Comey, Director of the FBI, is also asking for the major information technology (IT) companies to not adopt ‘end-to-end encryption’. This was from a Senate hearing on December 9, 2015 following the Paris attacks and the San Bernardino attacks (Khandelwal, 2015) James

Comey told the Senate that tech companies should reconsider their business model and stop doing end-to-end encryption. In addition, the FBI is asking these companies to retain a "readable" version of the initial data. (Khandelwal, 2015)

However, instead of companies complying with this request, more and more of their mobile devices and apps are becoming even more encrypted. Apple's iMessage and as of this week, Facebook owned, Whatsapp, and Viber (messaging app) both provide end-to-end encryption messaging services (Wagner, 2016).

The FBI wants the leading IT companies to stop the encryption practice because they can neither intercept nor decrypt these messages. The FBI is worried that terrorists or other people with ill intent can use these services and nobody can intercept and/or decrypt their communications. The FBI would like these companies to be able to comply with the court orders. However, as McGoogle (2015) pointed out, many technology companies are keeping and even strengthening their encryption because they believe that is what their customers want.

The San Bernardino attacks and the Paris attacks prompted fifty-six technology companies to call for encryption protections under the banner of the Information Technology Industry Council (ITIC). They spoke against any plans to make it possible to access end-to-end encryption. "But weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys," wrote the president of the ITIC. (Burgess, 2015)

The Media

I read a three-part series of articles in the Washington Post by Orin Kerr. He begins his first article by telling the readers how dangerous and troubling iOS 8 is for him: "In general, cryptography is an awesome thing" (Kerr, 2014). Most technologists would agree that cryptography is awesome, especially those who have studied cryptography in the Cybersecurity program at the Pennsylvania State University. He continues his article by arguing that the encryption as implanted by Apple in iOS 8 will impede law enforcement from doing their jobs. He states, "If officers lawfully come into possession of a target's unlocked phone, the data may effectively disappear as soon as the phone locks." (Kerr, 2014) Nowhere in this article does he consider the consumer. What about the consumer?

In the second article in the series, the author reflects on the feedback that he received from his readership. What his readership taught him was to look at the more than just the law enforcement angle of phone encryption. One of his readers replied with this: "Although it's unfortunate that Apple's new approach will thwart lawful search warrants, the benefit to the public outweighs that loss." (Kerr, 2014) This is the essential argument for encryption for the consumer as written by a consumer. Of course, without knowing the person who wrote this, I am sure it is somebody involved with the world of technology. I am sure consumers would love to know this, but most of them do not know or may not want to know. Again, why do consumers need full phone encryption?

In the last of his series of articles, the author is seeking the answers to questions that concern most of us. His questions are: "where would you draw the line?" and "what is the privacy tradeoff?" (Kerr, 2014).

Although I was not seeking answers to the same questions, the answers that I got in my research should also be informative.

Technology Community

The technology community in many ways is the voice of the consumers. Bruce Schneier is a well-respected authority on information security and is often quoted by technologists. In defending the rights of consumers, he wrote an article that both established the fear that law enforcement exhibits with facts that refute many of their claims. He understands that opening a backdoor for good guys likewise opens a backdoor for bad guys as well. "Backdoor access built for the good guys is routinely used by the bad guys. In 2005, some unknown group surreptitiously used the lawful-intercept capabilities built into the Greek cell phone system." (Schneier, 2014)

Schneier makes another valid point in the fight for the consumers' right to have full-phone encryption:

> We need to fight this. Strong encryption protects us from a panoply of threats. It protects us from hackers and criminals. It protects our businesses from competitors and foreign spies. It protects people in totalitarian governments from arrest and detention. This isn't just me talking: The FBI also recommends you encrypt your data for security. (Schneier, 2014)

The Electronic Frontier Foundation ("EFF") which is an organization designed to defend civil liberties in the "electronic" age has also given their opinion on this subject. They give reasons why a backdoor is essentially a very bad idea. The EFF supports the idea that if such a

tool were made available that not only could it be used for legitimate purposes, but it could also fall into the hands of those who might use it for nefarious purposes.

Johnathan Zdziarski, forensic scientist, wrote a blog post on why backdoors are a bad idea entitled, “Open Letter to Congress on Encryption Backdoors”. Mr. Zdzairski spends time examining the current state of law enforcement and the state of backdoors. He argues that putting in a backdoor to a mobile device (or any device) is an invasion of privacy. “I urge you to protect the rights of Americans to keep their most intimate thoughts secret.” (Zdzairski, 2016)

Tim Cook, CEO of Apple, Inc., published a letter to customers on the Apple website in February 2016 explaining the company’s position regarding encryption and their opposition to the FBI in the San Bernardino case. He reminds customers of the types of information that is now stored on our phones: photos, music, health information, text communication, and location data. Tim makes the most poignant statement on encryption (and against backdoors) that sums up what those in the technology community have been saying. “All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission.” (Cook, 2016)

Presented here are two very valid examples of members of the security community, the CEO of Apple, Tim Cook, and a consumer privacy protection agency as advocates for encryption and the stance against backdoors that circumvent and weaken security and weaken privacy. This confirms that full-phone encryption is needed. The phone encryption is not about keeping the good guys out but about keeping the bad guys out. Does the average consumer know this? Do consumers need full-phone encryption?

San Bernardino

In my review, I found several articles that reference the mass shooting in San Bernardino in December 2015. These articles discuss the fact that the FBI is having difficulties unlocking the phones that belonged to the perpetrators of the crime. The FBI feels that the key to unlocking the motives and movements leading up to the crime are encrypted on these devices. They cannot unlock or decrypt these phones. "The encrypted data could shed light on why Farook left a bag with several homemade pipe bombs in the conference room, whether they considered additional attacks, or whether the couple was in communication with anyone about their plans before the attack." (Bennett, 2016)

Tim Cook also weighed in on the San Bernardino case. Cook referenced that in other cases, Apple has complied with the FBI requests, if the data was in their possession. This particular case, however, is different than the rest. The FBI request for this case is seeking a new version of the iOS system that would compromise some of the security features. Cook also puts the dangers of this type of custom software in a very plain language: "In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession" (Cook, 2016).

The FBI enlisted the help of a group of "researchers" who specialize in finding vulnerabilities in software and selling them, sometimes to the U.S. Government. The FBI ended up unlocking the phone through an exploit found by these "researchers". The FBI paid a one-time fee for the exploit (Contantin, 2016; Nakashima, 2016). The FBI subsequently dropped the case against Apple.

Conclusion

It is a slippery slope now. Some articles in the mainstream news media (e.g., Bennett, 2016) could influence consumers in favor of the law enforcement side with regard to their stance against phone encryption. Now, my research project becomes muddied. If the consumer were to be asked about phone encryption before reading such articles, they could have had a different opinion. Everybody can agree that there should be something the law and/or the technology companies be able to do. Nobody can agree on the how to do it. More importantly, nobody will be able to answer this seemingly simple question: Do consumers need full-phone encryption?

Methodology

For my research design, I intended to use a quantitative research design. I sought to find out as much about my sample demographic as I could. My research question was: "Do consumers need smartphone encryption?" I intended to get opinions from people inside the technology community (such as my classmates) and outside the technology community (such as many of my Facebook friends and co-workers). Thus, I distributed a survey questionnaire to my classmates, family, and co-workers.

The survey was divided into two parts. The first part was a true-false section that intended to get some background information regarding the respondent's knowledge of the subject. This section included questions about the respondent's age, type of smartphone (iPhone, Android, Windows Phone, and even Blackberry), and occupation.

The second section of the survey was used to reveal the respondent's attitudes on several different topics including law enforcement, government involvement and the role of smartphone manufacturers. I had the subjects answer in one of five possible answers, which I assigned numeric values to for statistical breakdowns: Strongly Disagree (-2), Disagree (=1), Neutral (0), Agree (1), Strongly Agree (2). I used these to get an overall picture of all of my subjects or break it down by subject. For instance, "Do you know what smartphone encryption is?" The answers would be: Strongly Disagree (-2), Disagree (=1), Neutral (0), Agree (1), Strongly Agree (2). I used several methods to show the data.

I used a simple random sampling in order to obtain responses to my survey. I understood that the attitudes among different groups were most likely to be consistent. Therefore, I wanted to get the attitudes of as many and as random of respondents as possible.

In my analysis, I was able to get the picture of the attitudes among different groups though the collection of data in the survey, both in the quantitative questions and the demographic questions.

I collected the data though the use of SurveyMonkey.com. This free online survey software has a very good reputation in the industry. Unfortunately, the free service only allowed for 10 questions with 100 responses. SurveyMonkey.com did not allow me to export the data. Therefore, I had to read the data and manually collect it from their site.

I distributed the link to the survey via e-mail, Facebook status post (for my "normal" customers), and, possibly, Twitter because my posts there are public. I assumed that using the right hashtag could get me more responses from people that I may not necessarily know. In addition, SurveyMonkey has a service called "SurveyMonkey Audience" that promotes academic research to an audience for free.

I believed that 100 responses were enough to get the data I needed for this research project, as opposed to the "real-world" surveys that do require many more responses. I also used social networking to get my survey link out to as many people as I could.

I planned to use Excel to analyze the numeric data and to pull the data I needed. I have working knowledge of Visual Basic for Applications (aka VBA), so that I could create macros that capable of doing the analysis for me. From this, reports and graphs could be created to give the results of data analysis a good visual.

Results

For my survey, I published the survey on June 29, 2016 and allowed two weeks for responses and closed the survey on July 17, 2016. The survey was distributed though Facebook status message posting and was shared by at least two of my Facebook friends. It was posted at the beginning of each week the survey was open for responses. I also sent out the link to all of my classmates in this course (IST 594) through the Canvas messaging application. As I estimate, there were approximately 300 perspective respondents to my survey. I had hoped for at least 50 respondents out of the approximately 300 perspectives. I managed to only garner a total of 38 responses. This is a low rate of response at approximately 13 percent and a fairly low number of responses.

However, the responses that I did get were very honest and did come from a wide variety of respondents. I had a fairly even number of responses among smart phone owners (with the exception of the one Windows Phone User) and a very wide age range. The respondents to my survey also had a wide range of occupations. All respondents answered all questions because I did not setup the survey to allow any questions (other than a couple of demographic questions) to be skipped. Skipping of any of the questions of this survey would have been detrimental to the spirit of the survey.

In the end, the results of my survey are very much in line with what I had expected going into the analysis for the most part. Some results were surprising and some results were not. I have anonymized the data and removed anything that could identify a respondent. I have broken down my respondents by age range and by type of phones used. I have shown the breakdowns in the following charts:

Age Group	20 to 29	30 to 39	40 to 49	50 to 59	60 plus
Percentage of Respondents	13.16%	23.68%	36.84%	18.42%	7.89%

Figure 1. Age Group Breakdown

Type of Phone	Android	iPhone	Windows 10 Phone
Percentage of Respondents	45%	53%	3%

Figure 2. Type of Phones Used Breakdown

I will go over each question and the results overall including a deeper analysis of the responses by age group and by the respondent's phone type.

Question 2a: Have you been following the Apple vs FBI case?

Overall, 66 percent of the respondents said that they had been following the case. Of those, 70 percent of iPhone users said they were following the case, whereas only 59 percent of Android users said they had been following the case. In addition, 100% of my Windows phone respondents said they were following the case. The age range breakdown has almost all age ranges that said that they were following the case with the exception of the 20 – 29 age range where only 20 percent of respondents said they were following the case.

Question 2b: Do you understand what smartphone encryption entails?

Overall, only 55 percent of my respondents to the survey said that they understood what smartphone encryption entailled. The percentage of respondents for both iPhone and Android were almost equal with iPhone users at 55 percent and Android users at 53 percent, with 100 percent of Windows phone users saying that they understand what smartphone encryption entails. The age breakdown is fairly even with all age groups at the 60 percent mark. The exception is the 20 – 29 and 40 – 49 age groups clocking in at about 40 percent.

Question 2c: Did you know that your smartphone could be encrypted by default? (This is only true for Google Nexus devices and iPhones with iOS 8 and later. Some other phones offer encryption, but it is not on by default)

Overall, only 53 percent of respondents knew that their smartphone could be encrypted by default. This is only true of certain models of iPhone with iOS 8 or higher and only select Android phones. It appears that the Android users are more aware of this fact than iPhone users. 59 percent of Android users said they were aware that their phone could be encrypted whereas, only 60 percent of iPhone users said they did. Again, 100 percent of Windows phone users said they knew this fact. The age breakdown is fairly even with all age groups at the 60 percent mark. The exception is the 20 – 29 and 40 – 49 age groups. The 20 – 29 age group is about 40 percent, but the 40 – 49 age group is a measly 29 percent.

Question 2d: Do you understand the concept of a "backdoor"?

Overall, a nice 68 percent of respondents said they understood the concept of "backdoor". Again here, Android users had the higher percentage of respondents. For this question, 76 percent of Android users said they understood the concept of a "backdoor" with only 60 percent of iPhone users responding that they also understood this concept. Again, my Windows phone users had a 100 percent understanding of this concept. All age groups responded positively except for the 20 – 29 age group.

Question 3: In today's world, our smartphones keep all types of personal information such as contracts, photos, calendar entries, voice memos, and reminders. This information is encrypted in a way that Law Enforcement cannot retrieve from you without your consent. Should data be encrypted where Law Enforcement cannot retrieve this information?

Overall, the majority of respondents were either neutral or agreed with this question. Only 16 of respondents disagreed with this statement. Owners of all phone types and ages were either neutral or agreed with this statement. Only the 50 – 59 age group did not agree with this question.

Question 4: In the case of the recent tragedies, such as the San Bernardino attack where the owner/user of the phone is deceased, do you think that phone manufacturers (such as Apple, Samsung, Microsoft) be compelled to decrypt a phone containing that person's personal information?

Overall, a majority of respondents were neutral or agreed with this statement. 34 percent of respondents disagreed with this statement. There is a contrast here between Android and iPhone users regarding this question. A 70 percent majority of Android users agreed with this question contrasting the 45 percent of iPhone users who agree with this question. 55 percent of iPhone users were neutral or disagreed with this question. That is a sharp contrast to the only 30 percent of Android users that answered the same. In addition, 100 percent of Windows phone users agreed with this question. The only age range that disagreed with this question was the 60 plus age range. All other age ranges were neutral or agreed with this question.

Question 5: Following up on the previous question, would this set a precedent allowing the government to get the manufacturers to bypass the encryption on demand for persons that are not deceased that refuse to unlock (decrypt) their smartphone?

Again, a majority of respondents were either neutral or agreed with this question with only 21 percent of respondents that disagreed with the question. Android users and iPhone

users were almost equal on this question at around 75 percent that were neutral or agreed with the question. Most age ranges agree with this question with the exception of the 60 plus age range where 67 percent of the respondents disagreed with the question.

Question 6: Do believe that if the government can compel a private company to devote resources to creating custom software to bypass encryption for anybody that your data is safe?

Overall, the majority of respondents were either neutral or disagreed with this question. Only 18 percent of respondents agreed with this question. The only phone usage group to agree with this question is the Windows Phone users. All other users were only around 20 percent who agreed with this question. All age ranges seemed to be either neutral or disagree with this question.

Question 7: Do you believe that the government can compel a private company to provide a "backdoor" into a phone that Law Enforcement can use to get data from a phone without your consent?

Overall, this question is split very much right down the middle. 50 percent were either neutral or disagreed and 50 percent were either neutral or agreed with this statement. Android users disagreed with this question while iPhone users were split. Windows phone users tended to agree with this question as well. The age ranges differed greatly on this question. The 20 – 29 and the 50 – 59 age groups agreed with the question. The 30 – 39 and the 60 plus age groups disagreed with the question. The 40 – 49 age group was split on this question.

Question 8: Do you believe that any tampering with or creation of tools that can bypass a phone's encryption can fall into the hands of criminals?

Overall, all respondents agreed with this statement regardless of the phone type they owned or the age group. This question did not even have a neutral answer. Very compelling.

The numbers on this survey were very wide and varying in their nature. There are quite a few varying attitudes among smartphone users. There were questions where iPhone and Android users agreed and there were times they were far apart in their attitudes. Attitudes among the age groups were fairly equal most of the time. What does all of this really mean?

Questions 2b – 2d were designed to get the overall understanding of the respondent's technical knowledge. The numbers bear out that about half of the respondents have some technical knowledge. Some of this knowledge could come from personal or business training or even from some of the articles that have been written about the case. A small majority of the respondents have been following the case, so some of them may have picked up some of the technical knowledge from following the case.

Question 2d asks if the respondent if they are aware of what a "backdoor" is. An analysis of the numbers between this and the follow up question 7 results in the following conclusion. Although, a majority of respondents know what a backdoor is, they are split on whether or not the government can compel a private company to install a backdoor. This backdoor can be used by anyone including Law Enforcement and even hackers (or the "bad guys"). However, all respondents agreed that these tools could fall into the hands of criminals (or the "bad guys"). I am not sure what to make of this outcome. It is clear that the question on whether or not the government can compel a private company to install a backdoor should have been preceded by a slightly different question. That question should have been stated as

following: Should there be “backdoors” installed on consumer phones. The results of that question combined with the restated question would have proven more informative.

From a wider view, it seems as if the respondents feel that the government should play a larger role in these types of cases. For example, question 4 asks the respondent if the government should be able to compel a private company (such as Apple, Google, Microsoft) to decrypt a phone if the person is deceased. The overwhelming majority agreed that this should be the case and so far as agreed that this would set a precedent if this were done. Of course, it would set a precedent. If the government can compel Apple to decrypt an iPhone for this case, then certainly it could in the case of, say, a drug dealer.

In an earlier survey conducted by ACT, 93 percent of the respondents claimed that data on their smartphones should be held secure and private (Wyckoff, 2016). This is in line with the 84 percent of respondents to my survey who said their data should remain secured.

The majority also seems to worry about tools that may decrypt or unlock phones and thus compromise the safety of their data. That attitude appears to coincide with the responses to question 8 in my survey. If the tools designed to decrypt a phone exist, of course, they can fall into the hand of criminals. Criminals by their nature will use the power of these tools to obtain personal information from these phones. This is the same information that the same respondents said should be encrypted in a way that law enforcement agencies could not obtain without their consent. Of course, there are easy ways for law enforcement to get to your data if you so choose. You just unlock your phone. However, if the law enforcement professionals can get to this data through a backdoor, then so could do a criminal.

In the Pew research survey (Otto 2016), fifty-one percent of respondents said that Apple should comply with the FBI request to unlock the San Bernardino phones. However, in my survey, a much higher number of respondents (i.e., at 66 percent) said that phone manufactures should be compelled to decrypt phone such as the phones in the San Bernardino case.

In conclusion, there are some trends here. Respondents to my survey want government intervention in the case the owner of the phone is deceased (as in the San Bernardino case) but also when it comes to decrypting the phone for other Law Enforcement purposes. They understand that the backdoor (or other decryption tools) can fall into the hands of criminals, but the majority believes that the government should compel companies to install these backdoors. This is interesting to me because a backdoor is not something to take lightly as it will affect every phone that is running that particular software version.

There is some good that came out of this study, as I now understand how people feel about encryption and law enforcement. This is significant, as we move forward into a world where even more of our personal lives and information lives on our smartphones. Do we feel safe having this data on our phones if it is unencrypted or in a state where it can be easily obtained? The respondents said 'No.' This data should be kept away from prying eyes and those who wish to do us ill. However, they also said they want law enforcement to have some method to obtain the data when there is a need for it.

My study was limited to a small network of friends and friends-of-friends. This is a great method to find out what those around you think and their opinions on this subject matter. I, perhaps, did not do enough in promoting the survey. That is why it only garnered the number

of responses that it did. It did not get the reach that I had planned. The biggest issue is that I did not take it to Twitter as I first planned. I became somewhat weary of the type of respondents that it might garner or it might have not garnered any. I also was unable to get my survey in the academic section of SurveyMonkey.com, and thus lost out on an opportunity there as well.

This survey could be of more importance if someone took it to the next level and perhaps refined a few of the questions and brought it to a wider audience. There are quite a number of things that can be learned here and perhaps, if taken to a wider audience, the survey results could potentially exert influence on lawmakers and law enforcement officials. There were some real honest responses and tentative trends found in the data that I collected, and, if given the chance, it could have been even greater.

References

Bennett, B. (2016, February 9). FBI can't figure out how to unlock encrypted phone in San Bernardino investigation. Retrieved February 15, 2016, from http://www.latimes.com/nation/la-na-san-bernardino-phone-locked-20160209-story.html

Buttar, S. (2016, February 20). Apple, Americans, and Security vs. FBI. Retrieved April 24, 2016, from https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi

Burgess, M. (2015, November 23). Apple, Facebook, Google and Twitter call for encryption protections (Wired UK). Retrieved April 25, 2016, from http://www.wired.co.uk/news/archive/2015-11/23/apple-google-twitter-encryption-weaken

Cook, T. (2016, February 16). Customer Letter - Apple. Retrieved April 24, 2016, from https://www.apple.com/customer-letter/

Compromise needed on smartphone encryption. (2014, October 3). *Washington Post*, Retrieved January 24, 2016, from https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html

Constantin, L. (2016, April 13). FBI bought exploit from hackers to access San Bernardino iPhone. Retrieved April 24, 2016, from http://www.computerworld.com/article/3055486/security/fbi-bought-exploit-from-hackers-to-access-san-bernardino-iphone.html

Greenberg, A. (2016, April 8). The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'. Retrieved August 08, 2016, from https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/

Fitzgerald, S. (2016, January 15). New York Bill Could Force Backdoors for Phone Encryption. Retrieved January 24, 2016, from https://www.nextpowerup.com/news/25737/new-york-bill-could-force-backdoors-for-phone-encryption/

Kerr, O. (2014, September 19). Apple's dangerous game. Retrieved February 15, 2016, from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/

Kerr, O. (2014, September 22). Apple's dangerous game, part 2: The strongest counterargument. Retrieved February 15, 2016, from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-2-the-strongest-counterargument/?tid=a_inl

Kerr, O. (2014, September 22). Apple's dangerous game, part 3: Where do you draw the line, and what's the privacy tradeoff? Retrieved February 15, 2016, from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-3-where-do-you-draw-the-line-and-whats-the-privacy-tradeoff/?tid=a_inl

Kerr, O. (2014, September 24). Julian Sanchez on encryption, law enforcement, and the balance of power. Retrieved February 15, 2016, from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/24/julian-sanchez-on-encryption-law-enforcement-and-the-balance-of-power/?tid=a_inl

Khandelwal, S. (2015, December 9). FBI Director Asks Tech Companies to At least Don't Offer End-to-End Encryption. Retrieved April 24, 2016, from http://thehackernews.com/2015/12/fbi-end-to-end-encryption.html

McGoogan, C. (2015, December 10). The FBI director wants to stop end-to-end encryption (Wired UK). Retrieved April 25, 2016, from http://www.wired.co.uk/news/archive/2015-12/10/fbi-director-calls-for-encryption-end

Nakashima, E. (2016, April 12). FBI paid professional hackers one-time fee to crack San Bernardino iPhone. Retrieved July 31, 2016, from https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

Otto, G. (2016, February 22). Half of Americans side with FBI in iPhone unlocking case. Retrieved July 31, 2016, from http://fedscoop.com/apple-fbi-iphone-unlock-pew-survey-201

Poulsen, K. (2014, October 10). Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It. Retrieved January 24, 2016, from http://www.wired.com/2014/10/golden-key/

Schneier, B. (2014, October 6). IPhone Encryption and the Return of the Crypto Wars. Retrieved February 15, 2016, from https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html

Wagner, K. (2016, April 19). Viber Joins WhatsApp, Apple With End-to-End Encryption. Retrieved April 24, 2016, from http://recode.net/2016/04/19/viber-end-to-end-encryption-security-update/

Wellna, D. (2016, April 14). The Next Encryption Battleground: Congress. Retrieved April 24, 2016, from http://www.npr.org/sections/alltechconsidered/2016/04/14/474113249/the-next-encryption-battleground-congress

Wyckoff, W. B. (2016, April 18). Poll: American voters overwhelmingly want privacy, encryption. Retrieved May 29, 2016, from http://fedscoop.com/survey-most-americans-want-data-on-their-phone-to-stay-private

Zaziarski, J. (2016, April 20). Open Letter to Congress on Encryption Backdoors. Retrieved April 24, 2016, from http://www.zdziarski.com/blog/?p=6058

Appendix A

Invitation to Participate

Participants,

Welcome to the survey on smartphone encryption. My name is Michael Molenda. I am a graduate student at the Pennsylvania State University World Wide Campus Online. I am conducting a survey that will only take a moment of your time.

Smartphone encryption is a very sensitive and complex subject that I am asking for your participation in conducting. There are no right or wrong answers here as I am looking how you feel about each question that is presented.

The answers that you give will be only seen by me and my professor. However, the data will be anonymized and analyzed. The data will be used to help me form a hypothesis of consumer attitudes towards smartphone encryption. For those who wish to view the results of the survey, I can provide the data along with my hypothesis at the end of my summer semester. Taking the survey is easy, especially if you have taken a survey via SurveyMonkey in the past. SurveyMonkey surveys have easy navigation through the survey and again, should only take a moment of your time.

Sincerely,
Michael Molenda
mpm325@psu.edu

Appendix B:

Survey Questionnaire

The answers for questions 1-4 will be Yes (1) and No (0).

1. Have you been following the Apple vs FBI case?
2. Do you understand what smartphone encryption entails?
3. Did you know that your smartphone could be encrypted by default? (This is only true for Google Nexus devices and iPhones with iOS 8 and later. Some other phones offer encryption, but it is not on by default)
4. Do you understand the concept of a "backdoor"?

The answers will be: Strongly Disagree (-2); Disagree (-1); Neutral (0); Agree (1); Strongly Agree (2) for Questions 5-10.

5. In today's world, our smartphones keep all types of personal information such as contracts, photos, calendar entries, voice memos, and reminders. This information is encrypted in a way that Law Enforcement cannot retrieve from you without your consent. Should data be encrypted where Law Enforcement cannot retrieve this information?
6. In the case of the recent tragedies, such as the San Bernardino attack where the owner/user of the phone is deceased, do you think that phone manufacturers (such as Apple, Samsung, Microsoft) be compelled to decrypt a phone containing that person's personal information?
7. Following up on the previous question, would this set a precedent allowing the government to get the manufacturers to bypass the encryption on demand for persons that are not deceased that refuse to unlock (decrypt) their smartphone?
8. Do believe that if the government can compel a private company to devote resources to creating custom software to bypass encryption for anybody that your data is safe?
9. Do you believe that the government can compel a private company to provide a "backdoor" into a phone that Law Enforcement can use to get data from a phone without your consent?
10. Do you believe that any tampering with or creation of tools that can bypass a phone's encryption can fall into the hands of criminals?

Appendix C:
The Numbers

Overall Numbers

Questions	2a	2b	2c	2d
Yes	66%	55%	53%	68%
No	34%	45%	47%	32%

Questions	3	4	5	6	7	8
Strongly Disagree	8%	16%	5%	37%	18%	0%
Disagree	8%	18%	16%	34%	32%	0%
Neutral	24%	8%	16%	11%	5%	0%
Agree	24%	34%	42%	18%	37%	37%
Strongly Agree	37%	24%	21%	0%	8%	63%

By Phone Type

iPhone

	2a	2b	2c	2d
Yes	70%	55%	55%	60%
No	30%	45%	45%	40%

Android

	2a	2b	2c	2d
Yes	59%	53%	59%	76%
No	41%	47%	41%	24%

Windows Phone

	2a	2b	2c	2d
Yes	100%	100%	100%	100%
No	0%	0%	0%	0%

iPhone

	3	4	5	6	7	8
Strongly Disagree	0%	25%	0%	35%	20%	0%
Disagree	10%	25%	15%	30%	25%	0%
Neutral	20%	5%	15%	15%	5%	0%

Agree	30%	30%	40%	20%	45%	40%
Strongly Agree	40%	15%	30%	0%	5%	60%

Android

	3	4	5	6	7	8
Strongly Disagree	18%	6%	12%	41%	18%	0%
Disagree	6%	12%	18%	41%	41%	0%
Neutral	24%	12%	18%	6%	6%	0%
Agree	18%	35%	41%	12%	24%	29%
Strongly Agree	35%	35%	12%	0%	12%	71%

Windows Phone

	3	4	5	6	7	8
Strongly Disagree	0%	0%	0%	0%	0%	0%
Disagree	0%	0%	0%	0%	0%	0%
Neutral	100%	0%	0%	0%	0%	0%
Agree	0%	100%	100%	100%	100%	100%
Strongly Agree	0%	0%	0%	0%	0%	0%

By Age Group

20-29

	2a	2b	2c	2d
Yes	20%	40%	40%	40%
No	80%	60%	60%	60%

30-39

	2a	2b	2c	2d
Yes	67%	67%	67%	78%
No	33%	33%	33%	22%

40-49

	2a	2b	2c	2d
Yes	64%	43%	29%	64%
No	36%	57%	71%	36%

50-59

	2a	2b	2c	2d

Yes	86%	71%	86%	86%
No	14%	29%	14%	14%

60 plus

	2a	2b	2c	2d
Yes	0%	67%	67%	67%
No	100%	33%	33%	33%

20-29

	3	4	5	6	7	8
Strongly Disagree	0%	20%	0%	40%	0%	0%
Disagree	20%	0%	40%	0%	0%	0%
Neutral	40%	0%	40%	20%	20%	0%
Agree	0%	20%	0%	40%	40%	60%
Strongly Agree	40%	60%	20%	0%	40%	40%

30-39

	3	4	5	6	7	8
Strongly Disagree	0%	22%	22%	56%	22%	0%
Disagree	0%	22%	0%	44%	67%	0%
Neutral	11%	0%	22%	0%	0%	0%
Agree	33%	33%	33%	0%	11%	0%
Strongly Agree	56%	22%	22%	0%	0%	100%

40-49

	3	4	5	6	7	8
Strongly Disagree	7%	21%	0%	36%	29%	0%
Disagree	0%	14%	7%	36%	21%	0%
Neutral	21%	7%	7%	14%	0%	0%
Agree	21%	29%	57%	14%	50%	43%
Strongly Agree	50%	29%	29%	0%	0%	57%

50-59

	3	4	5	6	7	8
Strongly Disagree	29%	0%	0%	29%	14%	0%
Disagree	29%	24%	14%	29%	14%	0%

Neutral	14%	29%	14%	14%	14%	0%
Agree	29%	57%	57%	29%	43%	43%
Strongly Agree	0%	0%	14%	0%	14%	57%

60 plus

	3	4	5	6	7	8
Strongly Disagree	0%	0%	0%	0%	0%	0%
Disagree	0%	67%	67%	67%	67%	0%
Neutral	67%	0%	0%	0%	0%	0%
Agree	33%	33%	33%	33%	33%	67%
Strongly Agree	0%	0%	0%	0%	0%	33%